Regulatory Reference Texts

FTC · GDPR · HIPAA · TCPA: sample summaries and official full texts

Generated 2026-11-10

About this document

Part 1 contains short plain-language SUMMARIES written for testing the screening engine. They are not the law. Part 2 reproduces the official texts as retrieved from the sources named with each section. Formatting has been simplified (tables and footnotes may be flattened), so this is not an official version. Always rely on the official publication linked under each section.

Sources and reuse

United States Code and Code of Federal Regulations: works of the U.S. Government, public domain (17 U.S.C. 105); retrieved from eCFR (ecfr.gov), GovInfo (govinfo.gov) or the Office of the Law Revision Counsel (uscode.house.gov). GDPR: (c) European Union, https://eur-lex.europa.eu. Only the European Union legislation published in paper editions of the Official Journal of the European Union, or in its electronic edition on EUR-Lex, is deemed authentic.

Not legal advice

This compilation is provided for reference only and is not legal advice. Consult qualified counsel.

Part 1: Sample summaries (not the law)

Federal Trade Commission (FTC)

16 CFR 255.2

Advertisements featuring consumer endorsements that convey a product's performance are treated as claims the advertiser must substantiate; atypical results must not be presented as typical.

Official text: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-B/part-255

16 CFR 255.5

When there is a material connection between an endorser and the seller (payment, free product, employment, family or business relationship) that consumers would not expect, the connection must be clearly and conspicuously disclosed.

Official text: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-B/part-255

16 CFR 318 (Health Breach Notification Rule)

Vendors of personal health records not covered by HIPAA must notify consumers, the FTC and in some cases the media after a breach of security, which includes unauthorized disclosure of identifiable health information such as sharing with advertisers without authorization.

Official text: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318

FTC Act s.5 (15 U.S.C. 45)

Unfair or deceptive acts or practices in commerce are unlawful, including misrepresenting how consumer personal data is collected, used or shared, and making health or efficacy claims without competent and reliable evidence.

Official text: https://www.law.cornell.edu/uscode/text/15/45

EU General Data Protection Regulation (GDPR)

GDPR Art. 13

When collecting personal data, the controller must inform the data subject of its identity, purposes and legal basis, recipients, international transfers, retention period, and their rights including access, erasure and complaint to a supervisory authority.

Official text: https://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR Art. 28

Controllers may use only processors that give sufficient guarantees, under a binding contract setting out the subject matter, duration, purpose, data types and processor obligations.

Official text: https://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR Art. 6

Processing of personal data is lawful only with a legal basis: consent, contract, legal obligation, vital interests, public task, or legitimate interests not overridden by the data subject's rights.

Official text: https://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR Art. 7

Where processing relies on consent, the controller must be able to demonstrate consent; requests must be clearly distinguishable, in plain language, and consent must be as easy to withdraw as to give.

Official text: https://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR Art. 9

Processing of special categories of data, including health, genetic and biometric data, is prohibited unless an exception applies, such as explicit consent for specified purposes.

Official text: https://eur-lex.europa.eu/eli/reg/2016/679/oj

HIPAA Privacy, Security and Breach Notification Rules

45 CFR 164.502

A covered entity or business associate may not use or disclose protected health information except as permitted or required

by the Privacy Rule, and must limit uses and disclosures to the minimum necessary.
Official text: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

45 CFR 164.504(e)

A covered entity may disclose protected health information to a business associate only under a business associate agreement that limits use and requires safeguards.
Official text: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

45 CFR 164.508

A valid written authorization from the individual is required for most uses and disclosures of protected health information for marketing, and for any sale of protected health information.
Official text: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

45 CFR 164.520

Individuals have a right to adequate notice of privacy practices describing how their protected health information may be used and disclosed and their rights.
Official text: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

Telephone Consumer Protection Act (TCPA)

47 CFR 64.1200(a)(10)

Consumers may revoke consent to autodialed or prerecorded calls and texts by any reasonable means, and callers must honor revocation promptly.
Official text: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-L/section-64.1200

47 CFR 64.1200(a)(2)

Telemarketing calls or texts using an autodialer or artificial or prerecorded voice to wireless numbers require the called party's prior express written consent.
Official text: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-L/section-64.1200

47 CFR 64.1200(c)

Telephone solicitations to numbers on the National Do Not Call Registry, or outside 8 a.m. to 9 p.m. local time, are prohibited absent an exception.
Official text: https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-L/section-64.1200

Part 2: Federal Trade Commission (FTC), official text

§ 255.0 Purpose and definitions.

16 CFR 255.0 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.0

(a) The Guides in this part represent administrative interpretations of laws enforced by the Federal Trade Commission for the guidance of the public in conducting its affairs in conformity with legal requirements. Specifically, the Guides address the application of section 5 of the FTC Act, 15 U.S.C. 45, to the use of endorsements and testimonials in advertising. The Guides provide the basis for voluntary compliance with the law by advertisers and endorsers. Practices inconsistent with these Guides may result in corrective action by the Commission under section 5 if, after investigation, the Commission has reason to believe that the practices fall within the scope of conduct declared unlawful by the statute. The Guides set forth the general principles that the Commission will use in evaluating endorsements and testimonials, together with examples illustrating the application of those principles. The examples in each section apply the principles of that section to particular factual scenarios but do not address every possible issue that the facts or principles might implicate. Nor do the Guides purport to cover every possible use of endorsements in advertising.

1

Whether a particular endorsement or testimonial is deceptive will depend on the specific factual circumstances of the advertisement at issue.

1 Staff business guidance applying section 5 of the FTC Act to endorsements and testimonials in advertising is available on the FTC website. Such staff guidance addresses details not covered in these Guides and is updated periodically but is not approved by or binding upon the Commission.

(b) For purposes of this part, an “endorsement” means any advertising, marketing, or promotional message for a product that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser. Verbal statements, tags in social media posts, demonstrations, depictions of the name, signature, likeness or other identifying personal characteristics of an individual, and the name or seal of an organization can be endorsements. The party whose opinions, beliefs, findings, or experience the message appears to reflect will be called the “endorser” and could be or appear to be an individual, group, or institution.

(c) The Commission intends to treat endorsements and testimonials identically in the context of its enforcement of the Federal Trade Commission Act and for purposes of this part. The term endorsements is therefore generally used hereinafter to cover both terms and situations.

(d) For purposes of this part, the term “product” includes any product, service, brand, company, or industry.

(e) For purposes of this part, an “expert” is an individual, group, or institution possessing, as a result of experience, study, or training, knowledge of a particular subject, which knowledge is superior to what ordinary individuals generally acquire.

(f) For purposes of this part, “clear and conspicuous” means that a disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers. If a communication's representation necessitating a disclosure is made through visual means, the disclosure should be made in at least the communication's visual portion; if the representation is made through audible means, the disclosure should be made in at least the communication's audible portion; and if the representation is made through both visual and audible means, the disclosure should be made in the communication's visual and audible portions. A disclosure presented simultaneously in both the visual and audible portions of a communication is more likely to be clear and conspicuous. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, should stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood. An audible disclosure should be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it. In any communication using an interactive electronic medium, such as social media or the internet, the disclosure should be unavoidable. The disclosure should not be contradicted or mitigated by, or inconsistent with, anything else in the communication. When an endorsement targets a specific audience, such as older adults, “ordinary consumers” includes members of that group.

(g) Examples:

(1) Example 1. A film critic's review of a movie is excerpted in an advertisement placed by the film's producer. The critic's review

is not an endorsement, but when the excerpt from the review is used in the producer's advertisement, the excerpt becomes an endorsement. Readers would view it as a statement of the critic's own opinions and not those of the producer. If the excerpt alters or quotes from the text of the review in a way that does not fairly reflect its substance, the advertisement would be deceptive because it distorts the endorser's opinion. (See § 255.1(b))

(2) Example 2. A television commercial depicts two unidentified shoppers in a supermarket buying a laundry detergent. One comments to the other how clean the advertised brand makes the shopper's clothes. The other shopper then replies, “I will try it because I have not been fully satisfied with my own brand.” This obviously fictional dramatization would not be an endorsement.

(3) Example 3. In an advertisement for a pain remedy, an announcer unfamiliar to consumers except as a spokesperson for the advertising drug company praises the drug's ability to deliver fast and lasting pain relief. The spokesperson does not purport to speak from personal experience, nor on the basis of their own opinions, but rather in the place of and on behalf of the drug company. The announcer's statements would not be considered an endorsement.

(4) Example 4. A manufacturer of automobile tires hires a well-known professional automobile racing driver to deliver its advertising message in television commercials. In these commercials, the driver speaks of the smooth ride, strength, and long life of the tires. Many consumers are likely to believe this message reflects the driver's personal views, even if the driver does not say so, because consumers recognize the speaker primarily as a racing driver and not merely as a product spokesperson. Accordingly, many consumers would likely believe the driver would not speak for an automotive product without actually believing in the product and having personal knowledge sufficient to form the beliefs expressed. The likely attribution of these beliefs to the driver makes this message an endorsement under the Guides.

(5) Example 5. (i) A television advertisement for a brand of golf balls includes a video of a prominent and well-recognized professional golfer practicing numerous drives off the tee. The video would be an endorsement even though the golfer makes no verbal statement in the advertisement.

(ii) The golfer is also hired to post the video to their social media account. The paid post is an endorsement if viewers can readily identify the golf ball brand, either because it is apparent from the video or because it is tagged or otherwise mentioned in the post.

(6) Example 6. (i) An infomercial for a home fitness system is hosted by a well-known actor. During the infomercial, the actor demonstrates the machine and states, “This is the most effective and easy-to-use home exercise machine that I have ever tried.” Even if the actor is reading from a script, the statement would be an endorsement, because consumers are likely to believe it reflects the actor's personal views.

(ii) Assume that, rather than speaking about their experience with or opinion of the machine, the actor says that the machine was designed by exercise physiologists at a leading university, that it isolates each of five major muscle groups, and that it is meant to be used for fifteen minutes a day. After demonstrating various exercises using the machine, the actor finally says how much the machine costs and how to order it. As the actor does not say or do anything during the infomercial that would lead viewers to believe that the actor is expressing their own views about the machine, there is no endorsement.

(7) Example 7. (i) A consumer who regularly purchases a particular brand of dog food decides one day to purchase a new, more expensive brand made by the same manufacturer with their own money. The purchaser posts to their social media account that the change in diet has made their dog's fur noticeably softer and shinier, and that in their opinion, the new dog food definitely is worth the extra money. Because the consumer has no connection to the manufacturer beyond being an ordinary purchaser, their message cannot be attributed to the manufacturer and the post would not be deemed an endorsement under the Guides. The same would be true if the purchaser writes a consumer product review on an independent review website. But, if the consumer submits the review to the review section of the manufacturer's website and the manufacturer chooses to highlight the review on the homepage of its website, then the review as featured is an endorsement even though there is no connection between the consumer and the manufacturer.

(ii) Assume that rather than purchase the dog food with their own money, the consumer receives it for free because the store routinely tracks purchases and the dog food manufacturer arranged for the store to provide a coupon for a free trial bag of its new brand to all purchasers of its existing brand. The manufacturer does not ask coupon recipients for product reviews and recipients likely would not assume that the manufacturer expects them to post reviews. The consumer's post would not be deemed an endorsement under the Guides because this unsolicited review cannot be attributed to the manufacturer.

(iii) Assume now that the consumer joins a marketing program under which participants agree to periodically receive free products from various manufacturers and write reviews of them. If the consumer receives a free bag of the new dog food through this program, their positive review would be considered an endorsement under the Guides because of their connection to the manufacturer through the marketing program.

(iv) Assume that the consumer is the owner of a “dog influencer” (a dog with a social media account and a large number of followers). If the manufacturer sends the consumer coupons for a year's worth of dog food and asks the consumer to feature the brand in their dog's social media feed, any resulting posts that feature the brand would be considered endorsements even though the owner could have chosen not to endorse the product.

(8) Example 8. A college student, who has earned a reputation as an excellent video game player, live streams their game play. The developer of a new video game pays the student to play and live stream its new game. The student plays the game and appears to enjoy it. Even though the college student does not expressly recommend the game, the game play is considered an endorsement because the apparent enjoyment is implicitly a recommendation.

(9) Example 9. (i) An influencer who is paid to endorse a vitamin product in their social media posts discloses their connection to the product's manufacturer only on the profile pages of their social media accounts. The disclosure is not clear and conspicuous because people seeing their paid posts could easily miss the disclosure.

(ii) Assume now that the influencer discloses their connection to the manufacturer but that, in order to see the disclosures, consumers have to click on a link in the posts labeled simply “more.” If the endorsement is visible without having to click on the link labeled “more,” but the disclosure is not visible without doing so, then the disclosure is not unavoidable and thus is not clear and conspicuous.

(iii) Assume now that the influencer relies solely upon a social media platform's built-in disclosure tool for one of these posts. The disclosure appears in small white text, it is set against the light background of the image that the influencer posted, it competes with unrelated text that the influencer superimposed on the image, and the post appears for only five seconds. The disclosure is easy to miss and thus not clear and conspicuous.

(10) Example 10. A television advertisement promotes a smartphone app that purportedly halts cognitive decline. The ad presents multiple endorsements by older senior citizens who are represented as actual consumers who used the app. The advertisement discloses via both audio and visual means that the persons featured are actors. Because the advertisement is targeted at older consumers, whether the disclosure is clear and conspicuous will be evaluated from the perspective of older consumers, including those with diminished auditory, visual, or cognitive processing abilities.

(11) Example 11. (i) A social media advertisement promoting a cholesterol-lowering product features a testimonialist who says by how much their serum cholesterol went down. The claimed reduction greatly exceeds what is typically experienced by users of the product and a disclosure of typical results is required. The marketer has been able to identify from online data collection individuals with high cholesterol levels who speak a particular foreign language and are unable to understand English. It microtargets a foreign-language version of the ad to them, disclosing users' typical results only in English. The adequacy of the disclosure will be evaluated from the perspective of the microtargeted individuals, and the disclosure must be in the same language as the ad.

(ii) Assume now that the ad has a disclosure that is clear and conspicuous when viewed on a computer browser but that it is not clear and conspicuous when the ad is rendered on a smartphone. Because some consumers will view the ad on their smartphones, the disclosure is inadequate.

(12) Example 12. An exterminator purchases fake negative reviews of competing exterminators. A paid or otherwise incentivized negative statement about a competitor's service is not an endorsement, as that term is used in the Guides. Nevertheless, such statements, e.g., a paid negative review of a competing product, can be deceptive in violation of section 5. (See § 255.2.(e)(4)(v) regarding the purchase of a fake positive review for a product.) Fake positive reviews that are used to promote a product are “endorsements.”

(13) Example 13. A motivational speaker buys fake social media followers to impress potential clients. The use by endorsers of

fake indicators of social media influence, such as fake social media followers, is not itself an endorsement issue. The Commission notes, however, that it is a deceptive practice for users of social media platforms to purchase or create indicators of social media influence and then use them to misrepresent such influence to potential clients, purchasers, investors, partners, or employees or to anyone else for a commercial purpose. It is also a deceptive practice to sell or distribute such indicators to such users.

§ 255.1 General considerations.

16 CFR 255.1 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.1

(a) Endorsements must reflect the honest opinions, findings, beliefs, or experience of the endorser. Furthermore, an endorsement may not convey any express or implied representation that would be deceptive if made directly by the advertiser. (See § 255.2(a) and (b) regarding substantiation of representations conveyed by consumer endorsements.)

(b) An advertisement need not present an endorser's message in the exact words of the endorser unless the advertisement represents that it is presenting the endorser's exact words, such as through the use of quotation marks. However, the endorsement may not be presented out of context or reworded so as to distort in any way the endorser's opinion or experience with the product. An advertiser may use an endorsement of an expert or celebrity only so long as it has good reason to believe that the endorser continues to subscribe to the views presented. An advertiser may satisfy this obligation by securing the endorser's views at reasonable intervals where reasonableness will be determined by such factors as new information about the performance or effectiveness of the product, a material alteration in the product, changes in the performance of competitors' products, and the advertiser's contract commitments.

(c) When the advertisement represents that the endorser uses the endorsed product, the endorser must have been a bona fide user of it at the time the endorsement was given. Additionally, the advertiser may continue to run the advertisement only so long as it has good reason to believe that the endorser remains a bona fide user of the product. (See paragraph (b) of this section regarding the “good reason to believe” requirement.)

(d) Advertisers are subject to liability for misleading or unsubstantiated statements made through endorsements or for failing to disclose unexpected material connections between themselves and their endorsers. (See § 255.5.) An advertiser may be liable for a deceptive endorsement even when the endorser is not liable. Advertisers should:

(1) Provide guidance to their endorsers on the need to ensure that their statements are not misleading and to disclose unexpected material connections;

(2) Monitor their endorsers' compliance; and

(3) Take action sufficient to remedy non-compliance and prevent future non-compliance. While not a safe harbor, good faith and effective guidance, monitoring, and remedial action should reduce the incidence of deceptive claims and reduce an advertiser's odds of facing a Commission enforcement action.

(e) Endorsers may be liable for statements made in the course of their endorsements, such as when an endorser makes a representation that the endorser knows or should know to be deceptive, including when an endorser falsely represents that they personally used a product. Also, an endorser who is not an expert may be liable for misleading or unsubstantiated representations regarding a product's performance or effectiveness, such as when the representations are inconsistent with the endorser's personal experience or were not made or approved by the advertiser and go beyond the scope of the endorser's personal experience. (For the responsibilities of an endorser who is an expert, see § 255.3.) Endorsers may also be liable for failing to disclose unexpected material connections between themselves and an advertiser, such as when an endorser creates and disseminates endorsements without such disclosures.

(f) Advertising agencies, public relations firms, review brokers, reputation management companies, and other similar intermediaries may be liable for their roles in creating or disseminating endorsements containing representations that they know or should know are deceptive. They may also be liable for their roles with respect to endorsements that fail to disclose unexpected material connections, whether by disseminating advertisements without necessary disclosures or by hiring and directing endorsers who fail to make necessary disclosures.

(g) The use of an endorsement with the image or likeness of a person other than the actual endorser is deceptive if it misrepresents

a material attribute of the endorser.

(h) Examples:

(1) Example 1. (i) A building contractor states in an advertisement disseminated by a paint manufacturer, “I use XYZ exterior house paint because of its remarkable quick drying properties and durability.” This endorsement must comply with the pertinent requirements of § 255.3. Subsequently, the advertiser reformulates its paint to enable it to cover exterior surfaces with only one coat. Prior to continued use of the contractor's endorsement, the advertiser must contact the contractor in order to determine whether the contractor would continue to use the paint as reformulated and to subscribe to the views presented previously.

(ii) Assume that, before the reformulation, the contractor had posted an endorsement of the paint to their social media account. Even if the contractor would not use or recommend the reformulated paint, there is no obligation for the contractor or the manufacturer to modify or delete a historic post containing the endorsement as long as the date of that post is clear and conspicuous to viewers. If the contractor reposts or the advertiser shares the contractor's original endorsement after the reformulation, consumers would expect that the contractor holds the views expressed in the original post with respect to the reformulated product and the advertiser would need to confirm that with the contractor.

(2) Example 2. In a radio advertisement played during commercial breaks, a well-known DJ talks about how much they enjoy making coffee with a particular coffee maker in the morning. The DJ's comments likely communicate that they regularly use the coffee maker. If, instead, they used it only during a demonstration by its manufacturer, the ad would be deceptive.

(3) Example 3. (i) A dermatologist is a paid advisor to a pharmaceutical company and is asked by the company to post about its products on their professional social media account. The dermatologist posts that the company's newest acne treatment product is “clinically proven” to work. Before giving the endorsement, the dermatologist received a write-up of the clinical study in question, which indicates flaws in the design and conduct of the study that are so serious that they preclude any conclusions about the efficacy of the product. Given their medical expertise, the dermatologist should have recognized the study's flaws and is subject to liability for their false statements made in the advertisement. The advertiser is also liable for the misrepresentation made through the endorsement. (See § 255.3 regarding the product evaluation that an expert endorser must conduct.) Even if the study was sufficient to establish the product's proven efficacy, the pharmaceutical company and the dermatologist are both potentially liable if the endorser fails to disclose their relationship to the company. (See § 255.5 regarding the disclosure of unexpected material connections.)

(ii) Assume that the expert had asked the pharmaceutical company for the evidence supporting its claims and there were no apparent design or execution flaws in the study shown to the expert, but that the pharmaceutical company had withheld a larger and better controlled, non-published proprietary study of the acne treatment that failed to find any statistically significant improvement in acne. The expert's “clinically proven” to work claim would be deceptive and the company would be liable for the claim, but because the dermatologist did not have a reason to know that the claim was deceptive, the expert would not be liable.

(4) Example 4. A well-known celebrity appears in an infomercial for a hot air roaster that purportedly cooks a chicken perfectly in twenty minutes. During the shooting of the infomercial, the celebrity watches five attempts to cook chickens using the roaster. In each attempt, the chicken is undercooked after twenty minutes and requires forty-five minutes of cooking time. In the commercial, the celebrity places an uncooked chicken in the roaster. The celebrity then takes from a second roaster what appears to be a perfectly cooked chicken, tastes the chicken, and says that if you want perfect chicken every time, in just twenty minutes, this is the product you need. A significant percentage of consumers are likely to believe the statement represents the celebrity's own view and experience even though the celebrity is reading from a script. Because the celebrity knows that their statement is untrue, the endorser is subject to liability. The advertiser is also liable for misrepresentations made through the endorsement.

(5) Example 5. A skin care products advertiser hires an influencer to promote its products on the influencer's social media account. The advertiser requests that the influencer try a new body lotion and post a video review of it. The advertiser does not provide the influencer with any materials stating that the lotion cures skin conditions and the influencer does not ask the advertiser if it does. However, believing that the lotion cleared up their eczema, the influencer says in their review, “This lotion cures eczema. All of my followers suffering from eczema should use it.” The influencer, who did not limit their statements to their personal experience using the product and did not have a reasonable basis for their claim that the lotion cures eczema, is subject to liability for the misleading or unsubstantiated representation in the endorsement. If the advertiser lacked adequate substantiation for the implied claims that the lotion cures eczema, it would be liable regardless of the liability of the endorser. The influencer and the advertiser

may also be liable if the influencer fails to disclose clearly and conspicuously being paid for the endorsement. (See § 255.5.) In order to limit its potential liability, the advertiser should provide guidance to its influencers concerning the need to ensure that statements they make are truthful and substantiated and the need to disclose unexpected material connections and take other steps to discourage or prevent non-compliance. The advertiser should also monitor its influencers' compliance and take steps necessary to remove and halt the continued publication of deceptive representations when they are discovered and to ensure the disclosure of unexpected material connections. (See paragraph (d) of this section and § 255.5.)

(6) Example 6. (i) The website for an acne treatment features accurate testimonials of users who say that the product improved their acne quickly and with no side effects. Instead of using images of the actual endorsers, the website accompanies the testimonials with stock photos the advertiser purchased of individuals with near perfect skin. The images misrepresent the improvements to the endorsers' complexions.

(ii) The same website also sells QRS Weight-Loss shakes and features a truthful testimonial from an individual who says, “I lost 50 pounds by just drinking the shakes.” Instead of accompanying the testimonial with a picture of the actual endorser, who went from 300 pounds to 250 pounds, the website shows a picture of an individual who appears to weigh about 100 pounds. By suggesting that QRS Weight-Loss shakes caused the endorser to lose one-third of their original body weight (going from 150 pounds to 100 pounds), the image misrepresents the product's effectiveness. Even if it is accompanied by a picture of the actual endorser, the testimonial could still communicate a deceptive typicality claim.

(7) Example 7. A learn-to-read program disseminates a sponsored social media post by a parent saying that the program helped their child learn to read. The picture accompanying the post is not of the endorser and their child. The testimonial is from the parent of a 7-year-old, but the post shows an image of a child who appears to be only 4 years old. By suggesting that the program taught a 4-year-old to read, the image misrepresents the effectiveness of the program.

§ 255.2 Consumer endorsements.

16 CFR 255.2 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.2

(a) An advertisement employing endorsements by one or more consumers about the performance of an advertised product will be interpreted as representing that the product is effective for the purpose depicted in the advertisement. Therefore, the advertiser must possess and rely upon adequate substantiation, including, when appropriate, competent and reliable scientific evidence, to support express and implied claims made through endorsements in the same manner the advertiser would be required to do if it had made the representation directly, i.e., without using endorsements. Consumer endorsements themselves are not competent and reliable scientific evidence.

(b) An advertisement containing an endorsement relating the experience of one or more consumers on a central or key attribute of the product will likely be interpreted as representing that the endorser's experience is representative of what consumers will generally achieve with the advertised product in actual, albeit variable, conditions of use. Therefore, an advertiser should possess and rely upon adequate substantiation for this representation. If the advertiser does not have substantiation that the endorser's experience is representative of what consumers will generally achieve, the advertisement should clearly and conspicuously disclose the generally expected performance in the depicted circumstances, and the advertiser must possess and rely on adequate substantiation for that representation. The disclosure of the generally expected performance should be presented in a manner that does not itself misrepresent what consumers can expect. To be effective, such disclosure must alter the net impression of the advertisement so that it is not misleading.

(c) Advertisements presenting endorsements by what are represented, expressly or by implication, to be “actual consumers” should utilize actual consumers in both the audio and video, or clearly and conspicuously disclose that the persons in such advertisements are not actual consumers of the advertised product.

(d) In procuring, suppressing, boosting, organizing, publishing, upvoting, downvoting, reporting, or editing consumer reviews of their products, advertisers should not take actions that have the effect of distorting or otherwise misrepresenting what consumers think of their products, regardless of whether the reviews are considered endorsements under the Guides.

(e) Examples:

(1) Example 1. (i) A web page for a baldness treatment consists entirely of testimonials from satisfied customers who say that after

using the product, they had amazing hair growth and their hair is as thick and strong as it was when they were teenagers. The advertiser must have competent and reliable scientific evidence that its product is effective in producing new hair growth.

(ii) The web page will also likely communicate that the endorsers' experiences are representative of what new users of the product can generally expect. Therefore, even if the advertiser includes a disclaimer such as, “Notice: These testimonials do not prove our product works. You should not expect to have similar results,” the ad is likely to be deceptive unless the advertiser has adequate substantiation that new users typically will experience results similar to those experienced by the testimonialists.

(2) Example 2. (i) An advertisement disseminated by a company that sells heat pumps presents endorsements from three individuals who state that after installing the company's heat pump in their homes, their monthly utility bills went down by $100, $125, and $150, respectively. The ad will likely be interpreted as conveying that such savings are representative of what consumers who buy the heat pump can generally expect. The advertiser does not have substantiation for that representation because, in fact, fewer than 20% of purchasers will save $100 or more. A disclosure such as, “Results not typical” or “These testimonials are based on the experiences of a few people and you are not likely to have similar results” is insufficient to prevent this ad from being deceptive because consumers will still interpret the ad as conveying that the specified savings are representative of what consumers can generally expect.

(A) In another context, the Commission tested the communication of advertisements containing testimonials that clearly and prominently disclosed either “Results not typical” or the stronger “These testimonials are based on the experiences of a few people and you are not likely to have similar results.” Neither disclosure adequately reduced the communication that the experiences depicted are generally representative. Based upon this research, the Commission believes that similar disclaimers regarding the limited applicability of an endorser's experience to what consumers may generally expect to achieve are unlikely to be effective. Although the Commission would have the burden of proof in a law enforcement action, the Commission notes that an advertiser possessing reliable empirical testing demonstrating that the net impression of its advertisement with such a disclaimer is non-deceptive will avoid the risk of the initiation of such an action in the first instance.

(B) The advertiser should clearly and conspicuously disclose the generally expected savings and have adequate substantiation that homeowners can achieve those results. There are multiple ways that such a disclosure could be phrased, e.g., “the average homeowner saves $35 per month,” “the typical family saves $50 per month during cold months and $20 per month in warm months,” or “most families save 10% on their utility bills.”

(ii) Disclosures like those in this Example 2, specifically paragraph (e)(2)(i)(B) of this section, could still be misleading, however, if they only apply to limited circumstances that are not described in the advertisement. For example, if the advertisement does not limit its claims by geography, it would be misleading if the disclosure of expected results in a nationally disseminated advertisement was based on the experiences of customers in a southern climate and the experiences of those customers was much better than could be expected by heat pump users in a northern climate.

(3) Example 3. An advertisement for a cholesterol-lowering product features individuals who claim that their serum cholesterol went down by 120 points and 130 points, respectively; the ad does not mention the endorsers having made any lifestyle changes. A well-conducted clinical study shows that the product reduces the cholesterol levels of individuals with elevated cholesterol by an average of 15% and the advertisement clearly and conspicuously discloses this fact. Despite the presence of this disclosure, the advertisement would be deceptive if the advertiser does not have competent and reliable scientific evidence that the product can produce the specific results claimed by the endorsers (i.e., a 130-point drop in serum cholesterol without any lifestyle changes).

(4) Example 4. (i) An advertisement for a weight-loss product features an endorsement by a formerly obese person who says, “Every day, I drank 2 QRS Weight-Loss shakes, ate only raw vegetables, and exercised vigorously for six hours at the gym. By the end of six months, I had gone from 250 pounds to 140 pounds.” The advertisement accurately describes the endorser's experience, and such a result is within the range that would be generally experienced by an extremely overweight individual who consumed QRS Weight-Loss shakes, only ate raw vegetables, and exercised as the endorser did. Because the endorser clearly describes the limited and truly exceptional circumstances under which they achieved the claimed results, the ad is not likely to convey that consumers who weigh substantially less or use QRS Weight-Loss under less extreme circumstances will lose 110 pounds in six months. If the advertisement simply says that the endorser lost 110 pounds in six months using QRS Weight-Loss together with diet and exercise, however, this description would not adequately alert consumers to the truly remarkable circumstances leading to the endorser's weight loss. The advertiser must have substantiation, however, for any performance claims conveyed by the endorsement (e.g., that QRS Weight-Loss is an effective weight-loss product and that the endorser's weight loss was not caused

solely by their dietary restrictions and exercise regimen).

(ii) If, in the alternative, the advertisement simply features “before” and “after” pictures of a woman who says, “I lost 50 pounds in 6 months with QRS Weight-Loss,” the ad is likely to convey that the endorser's experience is representative of what consumers will generally achieve. Therefore, if consumers cannot generally expect to achieve such results, the ad would be deceptive. Instead, the ad should clearly and conspicuously disclose what they can expect to lose in the depicted circumstances (e.g., “women who use QRS Weight-Loss for six months typically lose 15 pounds”). A disclosure such as “Average weight loss is 1-2 pounds per week” is inadequate because it does not effectively communicate the expected weight loss over six months. Furthermore, that disclosure likely implies that weight loss continues at that rate over six months, which would not be true if, for example, the average weekly weight loss over six months is .57 pounds.

(iii) If the ad features the same pictures but the testimonialist simply says, “I lost 50 pounds with QRS Weight-Loss,” and QRS Weight-Loss users generally do not lose 50 pounds, the ad should disclose what results they do generally achieve (e.g., “women who use QRS Weight-Loss lose 15 pounds on average”). A disclosure such as “most women who use QRS Weight-Loss lose between 10 and 50 pounds” is inadequate because the range specified is so broad that it does not sufficiently communicate what users can generally expect.

(iv) Assume that a QRS Weight-Loss advertisement contains a disclosure of generally expected results that is based upon the mean weight loss of users. If the mean is substantially affected by outliers, then the disclosure would be misleading. For example, if the mean weight loss is 15 pounds, but the median weight loss is 8 pounds, it would be misleading to say that the average weight loss was 15 pounds. In such cases, the disclosure's use of median weight loss instead could help avoid deception, e.g., “most users lose 8 pounds” or “the typical user loses 8 pounds.”

(v) Assume that QRS Weight-Loss's manufacturer procured a fake consumer review, reading “I lost 50 pounds with QRS Weight-Loss,” and had it published on a third-party review website. This endorsement is deceptive because it was not written by a bona fide user of the product (see § 255.1(c)) and because it does not reflect the honest opinions, findings, beliefs, or experience of the endorser (see § 255.1(a)). Moreover, the manufacturer would need competent and reliable scientific evidence that QRS Weight-Loss is capable of causing 50-pound weight loss.

(vi) Assume that QRS Weight-Loss is a diet and exercise program and a person appearing in a QRS Weight-Loss ad says, “I lost 50 pounds in 6 months with QRS Weight-Loss.” Very few QRS Weight-Loss users lose 50 pounds in 6 months and the ad truthfully discloses, “The typical weight loss of QRS Weight-Loss users who stick with the program for 6 months is 35 pounds.” In fact, only one-fifth of those who start the QRS Weight-Loss program stick with it for 6 months. The disclosure is inadequate because it does not communicate what the typical outcome is for users who start the program. In other words, even with the disclosure, the ad does not communicate what people who join the QRS Weight-Loss program can generally expect.

(vii) Assume that QRS Weight-Loss's manufacturer forwards reviews for its product to a third-party review website. If it forwards only favorable reviews or omits unfavorable reviews, it is engaging in a misleading practice.

(5) Example 5. An advertisement presents the results of a poll of consumers who have used the advertiser's cake mixes as well as their own recipes. The results purport to show that the majority believed that their families could not tell the difference between the advertised mix and their own cakes baked from scratch. Many of the consumers are pictured in the advertisement along with relevant, quoted portions of their statements endorsing the product. This use of the results of a poll or survey of consumers represents that this is the typical result that ordinary consumers can expect from the advertiser's cake mix.

(6) Example 6. An advertisement appears to show a “hidden camera” situation in a crowded cafeteria at breakfast time. A spokesperson for the advertiser asks a series of patrons of the cafeteria for their spontaneous, honest opinions of the advertiser's recently introduced breakfast cereal. Even though none of the patrons is specifically identified during the advertisement, the net impression conveyed to consumers may well be that these are actual customers. If actors have been employed, this fact should be clearly and conspicuously disclosed.

(7) Example 7. (i) An advertisement for a recently released motion picture shows three individuals coming out of a theater, each of whom gives a positive statement about the movie. These individuals are actual consumers expressing their personal views about the movie. The advertiser does not need to have substantiation that their views are representative of the opinions that most consumers will have about the movie. Because the consumers' statements would be understood to be the subjective opinions of only three

people, this advertisement is not likely to convey a typicality message.

(ii) If the motion picture studio had approached these individuals outside the theater and offered them free tickets if they would talk about the movie on camera afterwards or post about it on social media, that arrangement should be clearly and conspicuously disclosed. (See § 255.5.)

(8) Example 8. (i) A camping goods retailer's website has various product pages. Each product page provides consumers with the opportunity to review the product and rate it on a five-star scale. Each such page displays the product's average star rating and a breakdown of the number of reviews with each star rating, followed by individual consumers' reviews and ratings. As such, the website is representing that it is providing an accurate reflection of the views of the purchasers who submitted product reviews to the website. If the retailer chose to suppress or otherwise not publish any reviews with fewer than four stars or reviews that contain negative sentiments, the product pages would be misleading as to purchasers' actual opinions of the products.

(ii) If the retailer chose not to post reviews containing profanity, that would not be unfair or deceptive even if reviews containing profanity tend to be negative reviews. However, it would be misleading if the retailer blocked negative reviews containing profanity, but posted positive reviews containing profanity. It would be acceptable for the retailer to have a policy against posting reviews unrelated to the product at issue or related services, for example reviews complaining about the owner's policy positions. But it would be misleading if the retailer chose to filter reviews based on other factors that are only a pretext for filtering them based on negativity. Sellers are not required to display customer reviews that contain unlawful, harassing, abusive, obscene, vulgar, or sexually explicit content; the personal information or likeness of another person; content that is inappropriate with respect to race, gender, sexuality, or ethnicity; or reviews that the seller reasonably believes are fake, so long as the criteria for withholding reviews are applied uniformly to all reviews submitted. Neither are sellers required to display reviews that are unrelated to their products or services. A particular seller's customer service, delivery, returns, and exchanges are related to its products and services.

(iii) Assume now that each product page starts with a glowing five-star review that is labeled as “the most helpful review.” Labeling the review as the most helpful suggests it was voted most helpful by consumers visiting the website. If the initial review on each such page was selected by the retailer and was not selected as the most helpful review by other consumers, labeling it as the most helpful would be deceptive.

(9) Example 9. A manufacturer offers to pay genuine purchasers $20 each to write positive reviews of its products on third-party review websites. Such reviews are deceptive even if the payment is disclosed because their positive nature is required by, rather than being merely influenced by, the payment. If, however, the manufacturer did not require the reviews to be positive and the reviewers understood that there were no negative consequences from writing negative reviews, a clear and conspicuous disclosure of the material connection would be appropriate. (See Example 6).

(10) Example 10. (i) In an attempt to coerce them to delete their reviews, a manufacturer threatens consumers who post negative reviews of its products to third-party review websites, with physical threats, with the disclosure of embarrassing information, with baseless lawsuits (such as actions for defamation that challenge truthful speech or matters of opinion), or with lawsuits it actually does not intend to file. Such threats amount to an unfair or deceptive practice because other consumers would likely be deprived of information relevant to their decision to purchase or use the products, or be misled as to purchasers' actual opinions of the product. [2]

2 The Consumer Review Fairness Act makes it illegal for companies to include standardized contract provisions that threaten or penalize people for posting honest reviews. 15 U.S.C. 45b.

(ii) Assume now that one of the third-party review websites has a reporting mechanism that allows businesses to flag suspected fake reviews. The manufacturer routinely flags negative reviews of its products as fake without a reasonable basis for believing that they actually are fake, resulting in truthful reviews being removed from the website. This misuse of the reporting option is an unfair or deceptive practice.

(11) Example 11. A marketer contacts recent online, mail-order, and in-store purchasers of its products and asks them to provide feedback to the marketer. The marketer then invites purchasers who give very positive feedback to post online reviews of the products on third-party websites. Less pleased and unhappy purchasers are simply thanked for their feedback. Such a practice may be an unfair or deceptive practice if it results in the posted reviews being substantially more positive than if the marketer had not engaged in the practice. If, in the alternative, the marketer had simply invited all recent purchasers to provide feedback on

third-party websites, the solicitation would not have been unfair or deceptive, even if it had expressed its hope for positive reviews.

§ 255.3 Expert endorsements.

16 CFR 255.3 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.3

(a) Whenever an advertisement represents, expressly or by implication, that the endorser is an expert with respect to the endorsement message, then the endorser's qualifications must in fact give the endorser the expertise that the endorser is represented as possessing with respect to the endorsement.

(b) Although an expert may, in endorsing a product, take into account factors not within the endorser's expertise (such as taste or price), the endorsement must be supported by an actual exercise of the expertise that the expert is represented as possessing in evaluating product features or characteristics which are relevant to an ordinary consumer's use of or experience with the product. This evaluation must have included an examination or testing of the product at least as extensive as someone with the same degree of represented expertise would normally need to conduct in order to support the conclusions presented in the endorsement. To the extent that the advertisement implies that the endorsement was based upon a comparison to another product or other products, such comparison must have been included in the expert's evaluation; and as a result of such comparison, the expert must have concluded that, with respect to those features on which the endorser is represented to be an expert and which are relevant and available to an ordinary consumer, the endorsed product is at least equal overall to the competitors' products. Moreover, where the net impression created by the endorsement is that the advertised product is superior to other products with respect to any such feature or features, then the expert must in fact have found such superiority. (See § 255.1(e) regarding the liability of endorsers.)

(c) Examples:

(1) Example 1. An endorsement of a particular automobile by one described as an “engineer” implies that the endorser's professional training and experience are such that the endorser is well acquainted with the design and performance of automobiles. If the endorser's field is, for example, chemical engineering, the endorsement would be deceptive.

(2) Example 2. An endorser of a hearing aid is simply referred to as a doctor during the course of an advertisement. The ad likely implies that the endorser has expertise in the area of hearing, as would be the case if the endorser is a medical doctor with substantial experience in audiology or a non-medical doctor with a Ph.D. or Au.D. in audiology. A doctor without substantial experience in the area of hearing might be able to endorse the product if the advertisement clearly and conspicuously discloses the nature and limits of the endorser's expertise.

(3) Example 3. A manufacturer of automobile parts advertises that its products are approved by the “American Institute of Science.” From its name, consumers would infer that the “American Institute of Science” is a bona fide independent testing organization with expertise in judging automobile parts and that, as such, it would not approve any automobile part without first testing its performance by means of valid scientific methods. If the American Institute of Science is not such a bona fide independent testing organization (e.g., if it was established and operated by an automotive parts manufacturer), the endorsement would be deceptive. Even if the American Institute of Science is an independent bona fide expert testing organization, the endorsement may nevertheless be deceptive unless the Institute has conducted valid scientific tests of the advertised products and the test results support the endorsement message.

(4) Example 4. A manufacturer of a non-prescription drug product represents that its product has been selected over competing products by a large metropolitan hospital. The hospital has selected the product because the manufacturer, unlike its competitors, has packaged each dose of the product separately. This package form is not generally available to the public. Under the circumstances, the endorsement would be deceptive because the basis for the hospital's choice—convenience of packaging—is neither relevant nor available to consumers, and the basis for the hospital's decision is not disclosed to consumers.

(5) Example 5. A person who is identified as the president of a commercial “home cleaning service” states in a television advertisement for a particular brand of cleanser that the service uses that brand instead of its leading competitors because of its performance. Because cleaning services extensively use cleansers in the course of their business, the ad likely conveys that the president has knowledge superior to that of ordinary consumers. Accordingly, the president's statement will be deemed to be an expert endorsement. The service must, of course, actually use the endorsed cleanser. In addition, because the advertisement implies that the cleaning service has experience with a reasonable number of leading competitors' brands available to consumers, the service must, in fact, have such experience, and have determined, based on its expertise, that the endorsed product's cleaning ability

is at least equal (or superior, if such is the net impression conveyed by the advertisement) to that of the leading competitors' products available to consumers. Because in this example the cleaning service's president makes no mention that the endorsed cleanser was “chosen,” “selected,” or otherwise evaluated in side-by-side comparisons against its competitors, it is sufficient if the service has relied solely upon its accumulated experience in evaluating cleansers without having performed side-by-side or scientific comparisons.

(6) Example 6. A medical doctor states in an advertisement for a drug that the product will safely allow consumers to lower their cholesterol by 50 points. If the materials the doctor reviewed were merely letters from satisfied consumers or the results of a rodent study, the endorsement would likely be deceptive because those materials are not the type of scientific evidence that others with the represented degree of expertise would consider adequate to support this conclusion about the product's safety and efficacy. Under such circumstances, both the advertiser and the doctor would be liable for the doctor's misleading representation. (See § 255.1(d) and (e)).

§ 255.4 Endorsements by organizations.

16 CFR 255.4 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.4

(a) Endorsements by organizations, especially expert ones, are viewed as representing the judgment of a group whose collective experience exceeds that of any individual member, and whose judgments are generally free of the sort of subjective factors that vary from individual to individual. Therefore, an organization's endorsement must be reached by a process sufficient to ensure that the endorsement fairly reflects the collective judgment of the organization. Moreover, if an organization is represented as being expert, then, in conjunction with a proper exercise of its expertise in evaluating the product under § 255.3, it must utilize an expert or experts recognized as such by the organization or standards previously adopted by the organization and suitable for judging the relevant merits of such products. (See § 255.1(e) regarding the liability of endorsers.)

(b) Examples:

(1) Example 1. A mattress manufacturer advertises that its product is endorsed by a chiropractic association. Because the association would be regarded as expert with respect to judging mattresses, its endorsement must be supported by an evaluation by an expert or experts recognized as such by the organization, or by compliance with standards previously adopted by the organization and aimed at measuring the performance of mattresses in general and not designed with the unique features of the advertised mattress in mind.

(2) Example 2. A trampoline manufacturer sets up and operates what appears to be a trampoline review website operated by an independent trampoline institute. The site reviews the manufacturer's trampolines, as well as those of competing manufacturers. Because the website falsely appears to be independent, it is deceptive. (See § 255.5.)

(3) Example 3. (i) A third-party company operates a wireless headphone review website that provides rankings of different manufacturers' wireless headphones from most recommended to least recommended. The website operator accepts money from manufacturers in exchange for higher rankings of their products. Regardless of whether the website makes express claims of objectivity or independence, such paid-for rankings are deceptive and the website operator is liable for the deception. A headphone manufacturer who pays for a higher ranking on the website may also be held liable for the deception. A disclosure that the website operator receives payments from headphone manufacturers would be inadequate because the payments actually determine the headphones' relative rankings. If, however, the review website does not take payments for higher rankings, but receives payments from some of the headphone manufacturers, such as for affiliate link referrals, it should clearly and conspicuously disclose that it receives such payments. (See § 255.5(k)(11))

(ii) Assume that the headphone review website operator uses a ranking methodology that results in higher rankings for products whose sellers have a relationship to the operator because of those relationships. The use of such a methodology is also misleading.

§ 255.5 Disclosure of material connections.

16 CFR 255.5 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.5

(a) When there exists a connection between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement, and that connection is not reasonably expected by the audience, such connection must be disclosed clearly and conspicuously. Material connections can include a business, family, or personal relationship. They can include monetary payment or the provision of free or discounted products (including products unrelated to the endorsed product) to

an endorser, regardless of whether the advertiser requires an endorsement in return. Material connections can also include other benefits to the endorser, such as early access to a product or the possibility of being paid, of winning a prize, or of appearing on television or in other media promotions. Some connections may be immaterial because they are too insignificant to affect the weight or credibility given to endorsements. A material connection needs to be disclosed when a significant minority of the audience for an endorsement does not understand or expect the connection. A disclosure of a material connection does not require the complete details of the connection, but it must clearly communicate the nature of the connection sufficiently for consumers to evaluate its significance.

(b) Examples:

(1) Example 1. A drug company commissions research on its product by an outside organization. The drug company determines the overall subject of the research (e.g., to test the efficacy of a newly developed product) and pays a substantial share of the expenses of the research project, but the research organization determines the protocol for the study and is responsible for conducting it. A subsequent advertisement by the drug company mentions the research results as the “findings” of that research organization. Although the design and conduct of the research project are controlled by the outside research organization, the weight consumers place on the reported results could be materially affected by knowing that the advertiser had funded the project. Therefore, the advertiser's payment of expenses to the research organization should be disclosed in the advertisement.

(2) Example 2. A film star endorses a particular food product in a television commercial. The endorsement regards only points of taste and individual preference. This endorsement must, of course, comply with § 255.1; but, regardless of whether the star's compensation for the commercial is a $1 million cash payment or a royalty for each product sold by the advertiser during the next year, no disclosure is required because such payments likely are ordinarily expected by viewers.

(3) Example 3. (i) During an appearance by a well-known professional tennis player on a television talk show, the host comments that the past few months have been the best of the player's career and during this time the player has risen to their highest level ever in the rankings. The player responds by attributing that improvement to seeing the ball better ever since having laser vision correction surgery at a specific identified clinic. The athlete continues talking about the ease of the procedure, the kindness of the clinic's doctors, the short recovery time, and now being able to engage in a variety of activities without glasses, including driving at night. The athlete does not disclose having a contractual relationship with the clinic that includes payment for speaking publicly about the surgery. Consumers might not realize that a celebrity discussing a medical procedure in a television interview has been paid for doing so, and knowledge of such payments would likely affect the weight or credibility consumers give to the celebrity's endorsement. Without a clear and conspicuous disclosure during the interview that the athlete has been engaged as a spokesperson for the clinic, this endorsement is likely to be deceptive. A disclosure during the show's closing credits would not be clear and conspicuous. Furthermore, if consumers are likely to take away from the interview that the athlete's experience is typical of those who undergo the same procedure at the clinic, the advertiser must have substantiation for that claim.

(ii) Assume that the tennis player instead touts the results of the surgery—mentioning the clinic by name—in the player's social media post. Consumers might not realize that the athlete is a paid endorser, and because that information might affect the weight consumers give to the tennis player's endorsement, the relationship with the clinic should be disclosed—regardless of whether the clinic paid the athlete for that particular post. It should be disclosed even if the relationship involves no payments but only the tennis player getting the laser correction surgery for free or at a significantly reduced cost.

(iii)(A) Assume that the clinic reposts the tennis player's social media post to its own social media account and that the player's original post either—

(1) Did not have a clear and conspicuous disclosure, or

(2) Had such a disclosure that does not appear clearly and conspicuously in the repost.

(B) Given the nature of the endorsement (i.e., a personally created statement from the tennis player's social media account), the viewing audience of the clinic's social media account would likely reasonably not expect the tennis player to be compensated. The clinic should clearly and conspicuously disclose its relationship to the athlete in its repost.

(iv) Assume that during the appearance on the television talk show, the tennis player is wearing clothes bearing the insignia of an athletic wear company with which the athlete also has an endorsement contract. Although this contract requires wearing the

company's clothes not only on the court but also in public appearances, when possible, the athlete does not mention the clothes or the company during the appearance on the show. No disclosure is required because no representation is being made about the clothes in this context.

(4) Example 4. (i) A television ad for an anti-snoring product features a physician who says, “I have seen dozens of products come on the market over the years, and in my opinion, this is the best ever.” Consumers would expect the physician to be reasonably compensated for appearing in the ad. Consumers are unlikely, however, to expect that an expert endorser like the physician receives a percentage of gross product sales or owns part of the company, and either of these facts would likely materially affect the credibility that consumers attach to the endorsement. Accordingly, the advertisement should clearly and conspicuously disclose such a connection between the company and the physician.

(ii) Assume that the physician is instead paid to post about the product on social media. In that context, consumers might not expect that the physician was compensated and might be more likely than in a television ad to expect that the physician is expressing an independent, professional opinion. Accordingly, the post should clearly and conspicuously disclose the doctor's connection with the company.

(5) Example 5. (i) In a television advertisement, an actual patron of a restaurant, who is neither known to the public nor presented as an expert, is shown seated at the counter. The diner is asked for a “spontaneous” opinion of a new food product served in the restaurant. Assume, first, that the advertiser had posted a sign on the door of the restaurant informing all who entered that day that patrons would be interviewed by the advertiser as part of its television promotion of its new “meat-alternative” burger. A patron seeing such a sign might be more inclined to give a positive review of that item in order to appear on television. The advertisement should thus clearly and conspicuously inform viewers that the patrons on screen knew in advance that they might appear in a television advertisement because that information may materially affect the weight or credibility of the endorsement.

(ii) Assume, in the alternative, that the advertiser had not posted the sign and that patrons asked for their opinions about the burger did not know or have reason to believe until after their response that they were being recorded for use in an advertisement. No disclosure is required here, even if patrons were also told, after the interview, that they would be paid for allowing the use of their opinions in advertising.

(6) Example 6. (i) An infomercial producer wants to include consumer endorsements in an infomercial for an automotive additive product not yet on the market. The producer's staff selects several people who work as “extras” in commercials and asks them to use the product and report back, telling them that they will be paid a small amount if selected to endorse the product in the infomercial. Viewers would not expect that these “consumer endorsers” are actors who used the product in the hope of appearing in the commercial and receiving compensation. Because the advertisement fails to disclose these facts, it is deceptive.

(ii) Assume that the additive's marketer wants to have more consumer reviews appear on its retail website, which sells a variety of its automotive products. The marketer recruits ordinary consumers to get a free product (e.g., a set of jumper cables or a portable air compressor for car tires) and a $30 payment in exchange for posting a consumer review of the free product on the marketer's website. The marketer makes clear and the reviewers understand that they are free to write negative reviews and that there are no negative consequences of doing so. Any resulting review that fails to clearly and conspicuously disclose the incentives provided to that reviewer is likely deceptive. When the resulting reviews must be positive or reviewers believe they might face negative consequences from posting negative reviews, a disclosure would be insufficient. (See §§ 255.2(d) and (e)(9).) Even if adequate disclosures appear in each incentivized review, the practice could still be deceptive if the solicited reviews contain star ratings that are included in an average star rating for the product and including the incentivized reviews materially increases that average star rating. If such a material increase occurs, the marketer likely would need to provide a clear and conspicuous disclosure to people who see the average star rating.

(7) Example 7. A woodworking influencer posts on-demand videos of various projects. A tool manufacturer sends the influencer an expensive full-size lathe in the hope that the influencer would post about it. The woodworker uses the lathe for several products and comments favorably about it in videos. If a significant minority of viewers are likely unaware that the influencer received the lathe free of charge, the woodworker should clearly and conspicuously disclose receiving it for free, a fact that could affect the credibility that viewers attach to the endorsements. The manufacturer should advise the woodworker at the time it provides the lathe that this connection should be disclosed, and it should have reasonable procedures in place to monitor the influencer's postings for compliance and follow those procedures. (See § 255.1(d).)

(8) Example 8. An online community has a section dedicated to discussions of robotic products. Community members ask and answer questions and otherwise exchange information and opinions about robotic products and developments. Unbeknownst to this community, an employee of a leading home robot manufacturer has been posting messages on the discussion board promoting the manufacturer's new product. Knowledge of this poster's employment likely would affect the weight or credibility of the endorsements. Therefore, the poster should clearly and conspicuously disclose their relationship to the manufacturer. To limit its own liability for such posts, the employer should engage in appropriate training of employees. To the extent that the employer has directed such endorsements or otherwise has reason to know about them, it should also be monitoring them and taking other steps to ensure compliance. (See § 255.1(d).) The disclosure requirements in this example would apply equally to employees posting their own reviews of the product on retail websites or review platforms.

(9) Example 9. A college student signs up to be part of a program in which points are awarded each time a participant posts on social media about a particular advertiser's products. Participants can then exchange their points for prizes, such as concert tickets or electronics. These incentives would materially affect the weight or credibility of the college student's endorsements. They should be clearly and conspicuously disclosed, and the advertiser should take steps to ensure that these disclosures are being provided.

(10) Example 10. Great Paper Company sells photocopy paper with packaging that has a seal of approval from the No Chlorine Products Association, a non-profit third-party association. Great Paper Company paid the No Chlorine Products Association a reasonable fee for the evaluation of its product and its manufacturing process. Consumers would reasonably expect that marketers have to pay for this kind of certification. Therefore, there is no unexpected material connection between the company and the association, and the use of the seal without disclosure of the fee paid to the association would not be deceptive.

(11) Example 11. A coffee lover creates a blog that reviews coffee makers. The blogger writes the content independently of the marketers of the coffee makers but includes affiliate links to websites on which consumers can buy these products from their marketers. Whenever a consumer clicks on such a link and buys the product, the blogger receives a portion of the sale. Because knowledge of this compensation could affect the weight or credibility site visitors give to the blogger's reviews, the reviews should clearly and conspicuously disclose the compensation.

(12) Example 12. (i) Near the beginning of a podcast, the host reads what is obviously a commercial for a product. Even without a statement identifying the advertiser as a sponsor, listeners would likely still expect that the podcaster was compensated, so there is no need for a disclosure of payment for the commercial. Depending upon the language of the commercial, however, the audience may believe that the host is expressing their own views in the commercial, in which case the host would need to hold the views expressed. (See § 255.0(b).)

(ii) Assume that the host also mentions the product in a social media post. The fact that the host did not have to make a disclosure in the podcast has no bearing on whether there has to be a disclosure in the social media post.

(13) Example 13. An app developer gives a consumer a game app to review. The consumer clearly and conspicuously discloses in the review that they were given the app, which normally costs 99 cents, for free. That disclosure suggests that the consumer did not receive anything else for the review. If the app developer also gave the consumer $50 for the review, the mere disclosure that the app was free would be inadequate.

(14) Example 14. Speed Ways, an internet Service Provider, advertises that it has the “Fastest ISP Service” as determined by the “Data Speed Testing Company.” If Speed Ways commissioned and paid for the analysis of its and competing services, it should clearly and conspicuously disclose its relationship to the testing company because the relationship would likely be material to consumers in evaluating the claim. If the “Data Speed Testing Company” is not a bona fide independent testing organization with expertise in judging ISP speeds or it did not conduct valid tests that supported the endorsement message, the endorsement would also be deceptive. (See § 255.3(c)(3)).

§ 255.6 Endorsements directed to children.

16 CFR 255.6 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-255.6

Endorsements in advertisements addressed to children may be of special concern because of the character of the audience. Practices that would not ordinarily be questioned in advertisements addressed to adults might be questioned in such cases.

§ 318.1 Purpose and scope.

16 CFR 318.1 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.1

(a) This part, which shall be called the “Health Breach Notification Rule,” implements section 13407 of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. 17937. This part applies to foreign and domestic vendors of personal health records, PHR related entities, and third party service providers, irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act, that maintain information of U.S. citizens or residents. This part does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

(b) This part preempts State law as set forth in section 13421 of the American Recovery and Reinvestment Act of 2009, 42 U.S.C 17951.

§ 318.2 Definitions.

16 CFR 318.2 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.2

Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information. A breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure.

Business associate means a business associate under the Health Insurance Portability and Accountability Act, Public Law 104-191, 110 Stat. 1936, as defined in 45 CFR 160.103.

Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(1) Reasonably understandable. You make your notice reasonably understandable if you:

(i) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(ii) Use short explanatory sentences or bullet lists whenever possible;

(iii) Use definite, concrete, everyday words and active voice whenever possible;

(iv) Avoid multiple negatives;

(v) Avoid legal and highly technical business terminology whenever possible; and

(vi) Avoid explanations that are imprecise and readily subject to different interpretations.

(2) Designed to call attention. You design your notice to call attention to the nature and significance of the information in it if you:

(i) Use a plain-language heading to call attention to the notice;

(ii) Use a typeface and type size that are easy to read;

(iii) Provide wide margins and ample line spacing;

(iv) Use boldface or italics for key words; and

(v) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information. The notice should stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

(3) Notices on websites or within-application messaging. If you provide a notice on a web page or using within-application messaging, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the website or software application (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(i) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

Covered health care provider means a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing health care services or supplies.

Electronic mail means email in combination with one or more of the following: text message, within-application messaging, or electronic banner.

Health care services or supplies means any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools.

HIPAA-covered entity means a covered entity under the Health Insurance Portability and Accountability Act (HIPAA), Public Law 104-191, 110 Stat. 1936, as defined in 45 CFR 160.103.

Personal health record (PHR) means an electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

PHR identifiable health information means information that:

(1) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

(i) Identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and

(2) Is created or received by a:

(i) Covered health care provider;

(ii) Health plan (as defined in 42 U.S.C. 1320d(5));

(iii) Employer; or

(iv) Health care clearinghouse (as defined in 42 U.S.C. 1320d(2)); and

(3) With respect to an individual, includes information that is provided by or on behalf of the individual.

PHR related entity means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that:

(1) Offers products or services through the website, including any online service, of a vendor of personal health records;

(2) Offers products or services through the websites, including any online service, of HIPAA-covered entities that offer individuals personal health records; or

(3) Accesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record.

State means any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

Third party service provider means an entity that:

(1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and

(2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.

Unsecured means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009, 42 U.S.C. 17932(h)(2).

Vendor of personal health records means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.

§ 318.3 Breach notification requirement.

16 CFR 318.3 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.3

(a) In general. In accordance with §§ 318.4 (regarding timeliness of notification), 318.5 (regarding methods of notice), and 318.6 (regarding content of notice), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR related entity, following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall:

(1) Notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such breach of security;

(2) Notify the Federal Trade Commission; and

(3) Notify prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(b) Third party service providers. A third party service provider shall, following the discovery of a breach of security, provide notice of the breach to an official designated in a written contract by the vendor of personal health records or the PHR related entity to receive such notices or, if such a designation is not made, to a senior official at the vendor of personal health records or PHR related entity to which it provides services, and obtain acknowledgment from such official that such notice was received. Such notification shall include the identification of each customer of the vendor of personal health records or PHR related entity whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, acquired during such breach. For purposes of ensuring implementation of this paragraph (b), vendors of personal health records and PHR related entities shall notify third party service providers of their status as vendors of personal health records or PHR related entities subject to this part. While some third party service providers may access unsecured PHR identifiable health information in the course of providing services, this does not render the third party service provider a PHR related entity.

(c) Breaches treated as discovered. A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service

provider, respectively. Such vendor, entity, or third party service provider shall be deemed to have knowledge of a breach if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

§ 318.4 Timeliness of notification.

16 CFR 318.4 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.4

(a) In general. Except as provided in paragraph (d) of this section (exception for law enforcement), all notifications required under § 318.3(a)(1) (required notice to individuals), (a)(3) (required notice to media), and (b) (required notice by third party service providers), shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

(b) Timing of notice to FTC. All notifications required under § 318.5(c) (regarding notice to FTC) involving the unsecured PHR identifiable health information of 500 or more individuals shall be provided contemporaneously with the notice required by paragraph (a) of this section. All logged notifications required under § 318.5(c) (regarding notice to FTC) involving the unsecured PHR identifiable health information of fewer than 500 individuals may be sent annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year.

(c) Burden of proof. The vendor of personal health records, PHR related entity, and third party service provider involved shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

(d) Law enforcement exception. If a law enforcement official determines that a notification, notice, or posting required under this part would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This paragraph (d) shall be implemented in the same manner as provided under 45 CFR 164.528(a)(2), in the case of a disclosure covered under § 164.528(a)(2).

§ 318.5 Methods of notice.

16 CFR 318.5 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.5

(a) Individual notice. A vendor of personal health records or PHR related entity that discovers a breach of security shall provide notice of such breach to an individual promptly, as described in § 318.4 (regarding timeliness of notification), and in the following form:

(1) Written notice at the last known address of the individual. Written notice may be sent by electronic mail if the individual has specified electronic mail as the primary method of communication. Any written notice sent by electronic mail must be Clear and Conspicuous. Where notice via electronic mail is not available or the individual has not specified electronic mail as the primary method of communication, a vendor of personal health records or PHR related entity may provide notice by first-class mail at the last known address of the individual. If the individual is deceased, the vendor of personal health records or PHR related entity that discovered the breach must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available.

(2) If, after making reasonable efforts to contact all individuals to whom notice is required under § 318.3(a), through the means provided in paragraph (a)(1) of this section, the vendor of personal health records or PHR related entity finds that contact information for ten or more individuals is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the breach, in the following form:

(i) Through a conspicuous posting for a period of 90 days on the home page of its website; or

(ii) In major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn if the individual's unsecured PHR identifiable health information may have been included in the breach.

(3) In any case deemed by the vendor of personal health records or PHR related entity to require urgency because of possible imminent misuse of unsecured PHR identifiable health information, that entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (a)(1) of this section.

(b) Notice to media. As described in § 318.3(a)(3), a vendor of personal health records or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(c) Notice to FTC. Vendors of personal health records and PHR related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security, as described in § 318.4(b) (regarding timing of notice to FTC). If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach and submit such a log annually to the Federal Trade Commission as described in § 318.4(b) (regarding timing of notice to FTC), documenting breaches from the preceding calendar year. All notices pursuant to this paragraph (c) shall be provided according to instructions at the Federal Trade Commission's website.

§ 318.6 Content of notice.

16 CFR 318.6 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.6

Regardless of the method by which notice is provided to individuals under § 318.5 (regarding methods of notice), notice of a breach of security shall be in plain language and include, to the extent possible, the following:

(a) A brief description of what happened, including: the date of the breach and the date of the discovery of the breach, if known; and the full name or identity (or, where providing the full name or identity would pose a risk to individuals or the entity providing notice, a description) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security, if this information is known to the vendor of personal health records or PHR related entity;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as but not limited to full name, Social Security number, date of birth, home address, account number, health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, or device identifier (in combination with another data element));

(c) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the entity that experienced the breach is doing to investigate the breach, to mitigate harm, to protect against any further breaches, and to protect affected individuals, such as offering credit monitoring or other services; and

(e) Contact procedures for individuals to ask questions or learn additional information, which must include two or more of the following: toll-free telephone number; email address; website; within-application; or postal address.

§ 318.7 Enforcement.

16 CFR 318.7 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.7

Any violation of this part shall be treated as a violation of a rule promulgated under section 18 of the Federal Trade Commission Act, 15 U.S.C. 57a, regarding unfair or deceptive acts or practices, and thus subject to civil penalties (as adjusted for inflation pursuant to § 1.98 of this chapter), and the Commission will enforce this part in the same manner, by the same means, and with the same jurisdiction, powers, and duties as are available to it pursuant to the Federal Trade Commission Act, 15 U.S.C. 41 et seq.

§ 318.8 Applicability date.

16 CFR 318.8 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.8

This part shall apply to breaches of security that are discovered on or after September 24, 2009.

§ 318.9 Sunset.

16 CFR 318.9 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-16/section-318.9

If new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered by this part, the provisions of this part shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

§45. Unfair methods of competition unlawful; prevention by Commission

15 U.S.C. 45 · GovInfo, United States Code · https://www.govinfo.gov/link/uscode/15/45?link-type=html

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C. 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C. 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless—

(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect—

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.

If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

(4)(A) For purposes of subsection (a), the term "unfair or deceptive acts or practices" includes such acts or practices involving foreign commerce that—

(i) cause or are likely to cause reasonably foreseeable injury within the United States; or

(ii) involve material conduct occurring within the United States.

(B) All remedies available to the Commission with respect to unfair and deceptive acts or practices shall be available for acts and practices described in this paragraph, including restitution to domestic or foreign victims.

(b) Proceeding by Commission; modifying and setting aside orders

Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership, or corporation to cease and desist from the violation of the law so charged in said complaint. Any person, partnership, or corporation may make application, and upon good cause shown may be allowed by the

Commission to intervene and appear in said proceeding by counsel or in person. The testimony in any such proceeding shall be reduced to writing and filed in the office of the Commission. If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited by this subchapter, it shall make a report in writing in which it shall state its findings as to the facts and shall issue and cause to be served on such person, partnership, or corporation an order requiring such person, partnership, or corporation to cease and desist from using such method of competition or such act or practice. Until the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, or, if a petition for review has been filed within such time then until the record in the proceeding has been filed in a court of appeals of the United States, as hereinafter provided, the Commission may at any time, upon such notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any report or any order made or issued by it under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, the Commission may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part any report or order made or issued by it under this section, whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require, except that (1) the said person, partnership, or corporation may, within sixty days after service upon him or it of said report or order entered after such a reopening, obtain a review thereof in the appropriate court of appeals of the United States, in the manner provided in subsection (c) of this section; and (2) in the case of an order, the Commission shall reopen any such order to consider whether such order (including any affirmative relief provision contained in such order) should be altered, modified, or set aside, in whole or in part, if the person, partnership, or corporation involved files a request with the Commission which makes a satisfactory showing that changed conditions of law or fact require such order to be altered, modified, or set aside, in whole or in part. The Commission shall determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph 1 (2) not later than 120 days after the date of the filing of such request.

(c) Review of order; rehearing

Any person, partnership, or corporation required by an order of the Commission to cease and desist from using any method of competition or act or practice may obtain a review of such order in the court of appeals of the United States, within any circuit where the method of competition or the act or practice in question was used or where such person, partnership, or corporation resides or carries on business, by filing in the court, within sixty days from the date of the service of such order, a written petition praying that the order of the Commission be set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Commission, and thereupon the Commission shall file in the court the record in the proceeding, as provided in section 2112 of title 28. Upon such filing of the petition the court shall have jurisdiction of the proceeding and of the question determined therein concurrently with the Commission until the filing of the record and shall have power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed and to issue such writs as are ancillary to its jurisdiction or are necessary in its judgement to prevent injury to the public or to competitors pendente lite. The findings of the Commission as to the facts, if supported by evidence, shall be conclusive. To the extent that the order of the Commission is affirmed, the court shall thereupon issue its own order commanding obedience to the terms of such order of the Commission. If either party shall apply to the court for leave to adduce additional evidence, and shall show to the satisfaction of the court that such additional evidence is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission, the court may order such additional evidence to be taken before the Commission and to be adduced upon the hearing in such manner and upon such terms and conditions as to the court may seem proper. The Commission may modify its findings as to the facts, or make new findings, by reason of the additional evidence so taken, and it shall file such modified or new findings, which, if supported by evidence, shall be conclusive, and its recommendation, if any, for the modification or setting aside of its original order, with the return of such additional evidence. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court upon certiorari, as provided in section 1254 of title 28.

(d) Jurisdiction of court

Upon the filing of the record with it the jurisdiction of the court of appeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive.

(e) Exemption from liability

No order of the Commission or judgement of court to enforce the same shall in anywise relieve or absolve any person, partnership, or corporation from any liability under the Antitrust Acts.

(f) Service of complaints, orders and other processes; return

Complaints, orders, and other processes of the Commission under this section may be served by anyone duly authorized by the Commission, either (a) by delivering a copy thereof to the person to be served, or to a member of the partnership to be served, or the president, secretary, or other executive officer or a director of the corporation to be served; or (b) by leaving a copy thereof at the residence or the principal office or place of business of such person, partnership, or corporation; or (c) by mailing a copy thereof by registered mail or by certified mail addressed to such person, partnership, or corporation at his or its residence or principal office or place of business. The verified return by the person so serving said complaint, order, or other process setting forth the manner of said service shall be proof of the same, and the return post office receipt for said complaint, order, or other process mailed by registered mail or by certified mail as aforesaid shall be proof of the service of the same.

(g) Finality of order

An order of the Commission to cease and desist shall become final—

(1) Upon the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time; but the Commission may thereafter modify or set aside its order to the extent provided in the last sentence of subsection (b).

(2) Except as to any order provision subject to paragraph (4), upon the sixtieth day after such order is served, if a petition for review has been duly filed; except that any such order may be stayed, in whole or in part and subject to such conditions as may be appropriate, by—

(A) the Commission;

(B) an appropriate court of appeals of the United States, if (i) a petition for review of such order is pending in such court, and (ii) an application for such a stay was previously submitted to the Commission and the Commission, within the 30-day period beginning on the date the application was received by the Commission, either denied the application or did not grant or deny the application; or

(C) the Supreme Court, if an applicable petition for certiorari is pending.

(3) For purposes of subsection (m)(1)(B) and of section 57b(a)(2) of this title, if a petition for review of the order of the Commission has been filed—

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(4) In the case of an order provision requiring a person, partnership, or corporation to divest itself of stock, other share capital, or assets, if a petition for review of such order of the Commission has been filed—

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(h) Modification or setting aside of order by Supreme Court

If the Supreme Court directs that the order of the Commission be modified or set aside, the order of the Commission rendered in accordance with the mandate of the Supreme Court shall become final upon the expiration of thirty days from the time it was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected to accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(i) Modification or setting aside of order by Court of Appeals

If the order of the Commission is modified or set aside by the court of appeals, and if (1) the time allowed for filing a petition for certiorari has expired and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered in accordance with the mandate of the court of appeals shall become final on the expiration of thirty days from the time such order of the Commission was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected so that it will accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(j) Rehearing upon order or remand

If the Supreme Court orders a rehearing; or if the case is remanded by the court of appeals to the Commission for a rehearing, and if (1) the time allowed for filing a petition for certiorari has expired, and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered upon such rehearing shall become final in the same manner as though no prior order of the Commission had been rendered.

(k) "Mandate" defined

As used in this section the term "mandate", in case a mandate has been recalled prior to the expiration of thirty days from the date of issuance thereof, means the final mandate.

(l) Penalty for violation of order; injunctions and other appropriate equitable relief

Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States. Each separate violation of such an order shall be a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense. In such actions, the United States district courts are empowered to grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission.

(m) Civil actions for recovery of penalties for knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices; jurisdiction; maximum amount of penalties; continuing violations; de novo determinations; compromise or settlement procedure

(1)(A) The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this subchapter respecting unfair or deceptive acts or practices (other than an interpretive rule or a rule violation of which the Commission has provided is not an unfair or deceptive act or practice in violation of subsection (a)(1)) with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule. In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(B) If the Commission determines in a proceeding under subsection (b) that any act or practice is unfair or deceptive, and issues a final cease and desist order, other than a consent order, with respect to such act or practice, then the Commission may commence a civil action to obtain a civil penalty in a district court of the United States against any person, partnership, or corporation which engages in such act or practice—

(1) after such cease and desist order becomes final (whether or not such person, partnership, or corporation was subject to such cease and desist order), and

(2) with actual knowledge that such act or practice is unfair or deceptive and is unlawful under subsection (a)(1) of this section.

In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(C) In the case of a violation through continuing failure to comply with a rule or with subsection (a)(1), each day of continuance of such failure shall be treated as a separate violation, for purposes of subparagraphs (A) and (B). In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(2) If the cease and desist order establishing that the act or practice is unfair or deceptive was not issued against the defendant in a civil penalty action under paragraph (1)(B) the issues of fact in such action against such defendant shall be tried de novo. Upon request of any party to such an action against such defendant, the court shall also review the determination of law made by the Commission in the proceeding under subsection (b) that the act or practice which was the subject of such proceeding constituted an unfair or deceptive act or practice in violation of subsection (a).

(3) The Commission may compromise or settle any action for a civil penalty if such compromise or settlement is accompanied by a public statement of its reasons and is approved by the court.

(n) Standard of proof; public policy considerations

The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

(Sept. 26, 1914, ch. 311, §5, 38 Stat. 719; Mar. 21, 1938, ch. 49, §3, 52 Stat. 111; June 23, 1938, ch. 601, title XI, §1107(f), 52 Stat. 1028; June 25, 1948, ch. 646, §32(a), 62 Stat. 991; May 24, 1949, ch. 139, §127, 63 Stat. 107; Mar. 16, 1950, ch. 61, §4(c), 64 Stat. 21; July 14, 1952, ch. 745, §2, 66 Stat. 632; Pub. L. 85–726, title XIV, §§1401(b), 1411, Aug. 23, 1958, 72 Stat. 806, 809; Pub. L. 85–791, §3, Aug. 28, 1958, 72 Stat. 942; Pub. L. 85–909, §3, Sept. 2, 1958, 72 Stat. 1750; Pub. L. 86–507, §1(13), June 11, 1960, 74 Stat. 200; Pub. L. 93–153, title IV, §408(c), (d), Nov. 16, 1973, 87 Stat. 591, 592; Pub. L. 93–637, title II, §§201(a), 204(b), 205(a), Jan. 4, 1975, 88 Stat. 2193, 2200; Pub. L. 94–145, §3, Dec. 12, 1975, 89 Stat. 801; Pub. L. 96–37, §1(a), July 23, 1979, 93 Stat. 95; Pub. L. 96–252, §2, May 28, 1980, 94 Stat. 374; Pub. L. 97–290, title IV, §403, Oct. 8, 1982, 96 Stat. 1246; Pub. L. 98–620, title IV, §402(12), Nov. 8, 1984, 98 Stat. 3358; Pub. L. 100–86, title VII, §715(a)(1), Aug. 10, 1987, 101 Stat. 655; Pub. L. 103–312, §§4, 6, 9, Aug. 26, 1994, 108 Stat. 1691, 1692, 1695; Pub. L. 109–455, §§3, 13, Dec. 22, 2006, 120 Stat. 3372, 3382; Pub. L. 112–203, §1, Dec. 4, 2012, 126 Stat. 1484.)

Amendment of Section

For repeal of amendment by section 13 of Pub. L. 109–455, see Termination Date of 2006 Amendment note below.

Part 2: EU General Data Protection Regulation (GDPR), official text

Article 1: Subject-matter and objectives

GDPR Art. 1 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2: Material scope

GDPR Art. 2 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
(a)
in the course of an activity which falls outside the scope of Union law;
(b)
by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
(c)
by a natural person in the course of a purely personal or household activity;
(d)
by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3: Territorial scope

GDPR Art. 3 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a)
the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b)
the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4: Definitions

GDPR Art. 4 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

For the purposes of this Regulation:
(1)
‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
(2)
‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
(3)
‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;
(4)
‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
(5)
‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
(6)
‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
(7)
‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
(8)
‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
(9)
‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
(10)
‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
(11)
‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
(12)
‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
(13)
‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
(14)
‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
(15)
‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16)
‘main establishment’ means:
(a)
as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
(b)
as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
(17)
‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
(18)
‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
(19)
‘group of undertakings’ means a controlling undertaking and its controlled undertakings;
(20)
‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
(21)
‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;
(22)
‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:
(a)
the controller or processor is established on the territory of the Member State of that supervisory authority;
(b)
data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c)
a complaint has been lodged with that supervisory authority;
(23)
‘cross-border processing’ means either:
(a)
processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b)
processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
(24)
‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
(25)
‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (19);
(26)
‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Article 5: Principles relating to processing of personal data

GDPR Art. 5 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Personal data shall be:
(a)
processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
(b)
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);
(c)
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
(d)
accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
(e)
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);
(f)
processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).
2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Article 6: Lawfulness of processing

GDPR Art. 6 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(a)
the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b)
processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c)
processing is necessary for compliance with a legal obligation to which the controller is subject;
(d)
processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e)
processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f)
processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
(a)
Union law; or

(b)
Member State law to which the controller is subject.
The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
(a)
any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b)
the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c)
the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d)
the possible consequences of the intended further processing for data subjects;
(e)
the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7: Conditions for consent

GDPR Art. 7 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8: Conditions applicable to child's consent in relation to information society services

GDPR Art. 8 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9: Processing of special categories of personal data

GDPR Art. 9 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
(a)
the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b)
processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c)
processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d)
processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e)
processing relates to personal data which are manifestly made public by the data subject;
(f)
processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g)
processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h)
processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i)
processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j)
processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10: Processing of personal data relating to criminal convictions and offences

GDPR Art. 10 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11: Processing which does not require identification

GDPR Art. 11 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

GDPR Art. 12 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.
3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
(a)
charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b)
refuse to act on the request.
The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the

information to be presented by the icons and the procedures for providing standardised icons.

Article 13: Information to be provided where personal data are collected from the data subject

GDPR Art. 13 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a)
the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b)
the contact details of the data protection officer, where applicable;
(c)
the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d)
where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e)
the recipients or categories of recipients of the personal data, if any;
(f)
where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a)
the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b)
the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c)
where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d)
the right to lodge a complaint with a supervisory authority;
(e)
whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f)
the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14: Information to be provided where personal data have not been obtained from the data subject

GDPR Art. 14 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
(a)
the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b)

the contact details of the data protection officer, where applicable;
(c)
the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d)
the categories of personal data concerned;
(e)
the recipients or categories of recipients of the personal data, if any;
(f)
where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
(a)
the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b)
where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(c)
the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d)
where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e)
the right to lodge a complaint with a supervisory authority;
(f)
from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g)
the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. The controller shall provide the information referred to in paragraphs 1 and 2:
(a)
within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b)
if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c)
if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.
4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
5. Paragraphs 1 to 4 shall not apply where and insofar as:
(a)
the data subject already has the information;
(b)
the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c)

obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d)
where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Article 15: Right of access by the data subject

GDPR Art. 15 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a)
the purposes of the processing;
(b)
the categories of personal data concerned;
(c)
the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d)
where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e)
the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f)
the right to lodge a complaint with a supervisory authority;
(g)
where the personal data are not collected from the data subject, any available information as to their source;
(h)
the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16: Right to rectification

GDPR Art. 16 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17: Right to erasure (‘right to be forgotten’)

GDPR Art. 17 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a)
the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b)

the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c)
the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d)
the personal data have been unlawfully processed;
(e)
the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f)
the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a)
for exercising the right of freedom of expression and information;
(b)
for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c)
for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d)
for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e)
for the establishment, exercise or defence of legal claims.

Article 18: Right to restriction of processing

GDPR Art. 18 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a)
the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b)
the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c)
the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d)
the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing

GDPR Art. 19 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20: Right to data portability

GDPR Art. 20 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
(a)
the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b)
the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 21: Right to object

GDPR Art. 21 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22: Automated individual decision-making, including profiling

GDPR Art. 22 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
(a)
is necessary for entering into, or performance of, a contract between the data subject and a data controller;
(b)

is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
(c)
is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Article 23: Restrictions

GDPR Art. 23 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
(a)
national security;
(b)
defence;
(c)
public security;
(d)
the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
(e)
other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
(f)
the protection of judicial independence and judicial proceedings;
(g)
the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
(h)
a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
(i)
the protection of the data subject or the rights and freedoms of others;
(j)
the enforcement of civil law claims.
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:
(a)
the purposes of the processing or categories of processing;
(b)
the categories of personal data;
(c)
the scope of the restrictions introduced;
(d)
the safeguards to prevent abuse or unlawful access or transfer;
(e)
the specification of the controller or categories of controllers;
(f)
the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories

of processing;
(g)
the risks to the rights and freedoms of data subjects; and
(h)
the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Article 24: Responsibility of the controller

GDPR Art. 24 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 25: Data protection by design and by default

GDPR Art. 25 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26: Joint controllers

GDPR Art. 26 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27: Representatives of controllers or processors not established in the Union

GDPR Art. 27 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
2. The obligation laid down in paragraph 1 of this Article shall not apply to:
(a)
processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in

a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b)

a public authority or body.

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28: Processor

GDPR Art. 28 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a)

processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b)

ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c)

takes all measures required pursuant to Article 32;

(d)

respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e)

taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f)

assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g)

at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h)

makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in

paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.
6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.
7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).
8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.
9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.
10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29: Processing under the authority of the controller or processor

GDPR Art. 29 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30: Records of processing activities

GDPR Art. 30 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
(a)
the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
(b)
the purposes of the processing;
(c)
a description of the categories of data subjects and of the categories of personal data;
(d)
the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e)
where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(f)
where possible, the envisaged time limits for erasure of the different categories of data;
(g)
where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
(a)
the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
(b)
the categories of processing carried out on behalf of each controller;
(c)

where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
(d)
where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31: Cooperation with the supervisory authority

GDPR Art. 31 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Article 32: Security of processing

GDPR Art. 32 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
(a)
the pseudonymisation and encryption of personal data;
(b)
the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c)
the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d)
a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33: Notification of a personal data breach to the supervisory authority

GDPR Art. 33 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
(a)
describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects

concerned and the categories and approximate number of personal data records concerned;
(b)
communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c)
describe the likely consequences of the personal data breach;
(d)
describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34: Communication of a personal data breach to the data subject

GDPR Art. 34 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(a)
the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b)
the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c)
it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Article 35: Data protection impact assessment

GDPR Art. 35 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
(a)
a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b)
processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c)
a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.
7. The assessment shall contain at least:
(a)
a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b)
an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c)
an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d)
the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Article 36: Prior consultation

GDPR Art. 36 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.
3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:
(a)
where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
(b)
the purposes and means of the intended processing;
(c)

the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
(d)
where applicable, the contact details of the data protection officer;
(e)
the data protection impact assessment provided for in Article 35; and
(f)
any other information requested by the supervisory authority.
4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.
5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Article 37: Designation of the data protection officer

GDPR Art. 37 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The controller and the processor shall designate a data protection officer in any case where:
(a)
the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
(b)
the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c)
the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38: Position of the data protection officer

GDPR Art. 38 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39: Tasks of the data protection officer

GDPR Art. 39 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data protection officer shall have at least the following tasks:
(a)
to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b)
to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c)
to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
(d)
to cooperate with the supervisory authority;
(e)
to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Article 40: Codes of conduct

GDPR Art. 40 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
(a)
fair and transparent processing;
(b)
the legitimate interests pursued by controllers in specific contexts;
(c)
the collection of personal data;
(d)
the pseudonymisation of personal data;
(e)
the information provided to the public and to data subjects;
(f)
the exercise of the rights of data subjects;
(g)
the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
(h)
the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;
(i)
the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;
(j)
the transfer of personal data to third countries or international organisations; or
(k)
out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.
4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.
5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.
6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.
7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.
8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.
9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).
10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.
11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41: Monitoring of approved codes of conduct

GDPR Art. 41 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.
2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:
(a)
demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
(b)
established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
(c)
established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
(d)
demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.
3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.
4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as

referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.
5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.
6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42: Certification

GDPR Art. 42 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.
2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.
3. The certification shall be voluntary and available via a process that is transparent.
4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.
5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.
6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.
7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.
8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43: Certification bodies

GDPR Art. 43 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:
(a)
the supervisory authority which is competent pursuant to Article 55 or 56;
(b)
the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (20) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.
2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:
(a)
demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;
(b)

undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;
(c)
established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
(d)
established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
(e)
demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.
3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.
4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.
5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.
6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.
7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).
9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 44: General principle for transfers

GDPR Art. 44 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Article 45: Transfers on the basis of an adequacy decision

GDPR Art. 45 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
(a)
the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well

as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
(b)
the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
(c)
the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.
3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).
4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.
5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).
On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).
6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.
7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.
8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.
9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46: Transfers subject to appropriate safeguards

GDPR Art. 46 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a)
a legally binding and enforceable instrument between public authorities or bodies;
(b)
binding corporate rules in accordance with Article 47;
(c)
standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d)
standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e)
an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f)
an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
(a)
contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
(b)
provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.
5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47: Binding corporate rules

GDPR Art. 47 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:
(a)
are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
(b)
expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
(c)
fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules referred to in paragraph 1 shall specify at least:
(a)
the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
(b)
the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
(c)
their legally binding nature, both internally and externally;
(d)
the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
(e)
the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f)
the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
(g)
how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;
(h)
the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
(i)
the complaint procedures;
(j)
the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
(k)
the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
(l)
the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
(m)
the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
(n)
the appropriate data protection training to personnel having permanent or regular access to personal data.
3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48: Transfers or disclosures not authorised by Union law

GDPR Art. 48 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49: Derogations for specific situations

GDPR Art. 49 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
(a)
the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b)
the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c)

the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d)
the transfer is necessary for important reasons of public interest;
(e)
the transfer is necessary for the establishment, exercise or defence of legal claims;
(f)
the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g)
the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.
Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.
2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.
4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50: International cooperation for the protection of personal data

GDPR Art. 50 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:
(a)
develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
(b)
provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
(c)
engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;
(d)
promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

Article 51: Supervisory authority

GDPR Art. 51 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.
4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 52: Independence

GDPR Art. 52 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53: General conditions for the members of the supervisory authority

GDPR Art. 53 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

—

their parliament;

—

their government;

—

their head of State; or

—

an independent body entrusted with the appointment under Member State law.
2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.
3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.
4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54: Rules on the establishment of the supervisory authority

GDPR Art. 54 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each Member State shall provide by law for all of the following:
(a)
the establishment of each supervisory authority;
(b)
the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;
(c)
the rules and procedures for the appointment of the member or members of each supervisory authority;
(d)
the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;
(e)
whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;
(f)
the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.
2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Article 55: Competence

GDPR Art. 55 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.
2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56: Competence of the lead supervisory authority

GDPR Art. 56 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.
4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).
5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.
6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57: Tasks

GDPR Art. 57 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a)
monitor and enforce the application of this Regulation;

(b)
promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c)
advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d)
promote the awareness of controllers and processors of their obligations under this Regulation;

(e)
upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f)
handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g)
cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h)
conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i)
monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j)
adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k)
establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l)
give advice on the processing operations referred to in Article 36(2);

(m)
encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n)
encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o)
where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

(p)
draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q)
conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r)
authorise contractual clauses and provisions referred to in Article 46(3);

(s)
approve binding corporate rules pursuant to Article 47;

(t)
contribute to the activities of the Board;
(u)
keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v)
fulfil any other tasks related to the protection of personal data.
2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.
3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.
4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58: Powers

GDPR Art. 58 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each supervisory authority shall have all of the following investigative powers:
(a)
to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;
(b)
to carry out investigations in the form of data protection audits;
(c)
to carry out a review on certifications issued pursuant to Article 42(7);
(d)
to notify the controller or the processor of an alleged infringement of this Regulation;
(e)
to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
(f)
to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.
2. Each supervisory authority shall have all of the following corrective powers:
(a)
to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
(b)
to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
(c)
to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
(d)
to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
(e)
to order the controller to communicate a personal data breach to the data subject;
(f)
to impose a temporary or definitive limitation including a ban on processing;
(g)
to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
(h)
to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i)
to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
(j)
to order the suspension of data flows to a recipient in a third country or to an international organisation.
3. Each supervisory authority shall have all of the following authorisation and advisory powers:
(a)
to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
(b)
to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c)
to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
(d)
to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
(e)
to accredit certification bodies pursuant to Article 43;
(f)
to issue certifications and approve criteria of certification in accordance with Article 42(5);
(g)
to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(h)
to authorise contractual clauses referred to in point (a) of Article 46(3);
(i)
to authorise administrative arrangements referred to in point (b) of Article 46(3);
(j)
to approve binding corporate rules pursuant to Article 47.
4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.
5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.
6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59: Activity reports

GDPR Art. 59 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Article 60: Cooperation between the lead supervisory authority and the other supervisory authorities concerned

GDPR Art. 60 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory

authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.
10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.
11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61: Mutual assistance

GDPR Art. 61 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.
2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.
4. The requested supervisory authority shall not refuse to comply with the request unless:
(a)
it is not competent for the subject-matter of the request or for the measures it is requested to execute; or
(b)
compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic

means, using a standardised format.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.
8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).
9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62: Joint operations of supervisory authorities

GDPR Art. 62 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.
2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.
3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.
4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.
5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.
6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.
7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Article 63: Consistency mechanism

GDPR Art. 63 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64: Opinion of the Board

GDPR Art. 64 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a)
aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);
(b)
concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;
(c)
aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);
(d)
aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);
(e)
aims to authorise contractual clauses referred to in point (a) of Article 46(3); or
(f)
aims to approve binding corporate rules within the meaning of Article 47.
2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.
3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.
4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.
5. The Chair of the Board shall, without undue, delay inform by electronic means:
(a)
the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and
(b)
the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.
6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.
7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.
8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65: Dispute resolution by the Board

GDPR Art. 65 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:
(a)
where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;
(b)
where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c)
where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.
2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.
3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.
4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.
5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.
6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66: Urgency procedure

GDPR Art. 66 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.
3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.
4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

Article 67: Exchange of information

GDPR Art. 67 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.
Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 68: European Data Protection Board

GDPR Art. 68 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality.
2. The Board shall be represented by its Chair.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.
6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69: Independence

GDPR Art. 69 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.
2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70: Tasks of the Board

GDPR Art. 70 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:
(a)
monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;
(b)
advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;
(c)
advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;
(d)
issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);
(e)
examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;
(f)
issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);
(g)
issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;
(h)
issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).
(i)

issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j)

issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k)

draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l)

review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m)

issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n)

encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o)

carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p)

specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q)

provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r)

provide the Commission with an opinion on the icons referred to in Article 12(7);

(s)

provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(t)

issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u)

promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v)

promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w)

promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x)

issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y)

maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee

referred to in Article 93 and make them public.
4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71: Reports

GDPR Art. 71 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.
2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72: Procedure

GDPR Art. 72 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.
2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73: Chair

GDPR Art. 73 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

Article 74: Tasks of the Chair

GDPR Art. 74 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Chair shall have the following tasks:
(a)
to convene the meetings of the Board and prepare its agenda;
(b)
to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;
(c)
to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75: Secretariat

GDPR Art. 75 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.
2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.
6. The secretariat shall be responsible in particular for:
(a)
the day-to-day business of the Board;
(b)
communication between the members of the Board, its Chair and the Commission;
(c)

communication with other institutions and the public;
(d)
the use of electronic means for the internal and external communication;
(e)
the translation of relevant information;
(f)
the preparation and follow-up of the meetings of the Board;
(g)
the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76: Confidentiality

GDPR Art. 76 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.
2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council (21).

Article 77: Right to lodge a complaint with a supervisory authority

GDPR Art. 77 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.
2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78: Right to an effective judicial remedy against a supervisory authority

GDPR Art. 78 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79: Right to an effective judicial remedy against a controller or processor

GDPR Art. 79 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 80: Representation of data subjects

GDPR Art. 80 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.
2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81: Suspension of proceedings

GDPR Art. 81 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.
2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.
3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82: Right to compensation and liability

GDPR Art. 82 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.
5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83: General conditions for imposing administrative fines

GDPR Art. 83 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
(a)
the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b)
the intentional or negligent character of the infringement;
(c)
any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d)
the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e)
any relevant previous infringements by the controller or processor;
(f)
the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g)
the categories of personal data affected by the infringement;
(h)
the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i)
where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j)
adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k)
any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a)
the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b)
the obligations of the certification body pursuant to Articles 42 and 43;
(c)
the obligations of the monitoring body pursuant to Article 41(4).
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a)
the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b)
the data subjects' rights pursuant to Articles 12 to 22;
(c)
the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d)
any obligations pursuant to Member State law adopted under Chapter IX;
(e)
non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in

that Member State.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84: Penalties

GDPR Art. 84 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.
2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 85: Processing and freedom of expression and information

GDPR Art. 85 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.
2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.
3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86: Processing and public access to official documents

GDPR Art. 86 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87: Processing of the national identification number

GDPR Art. 87 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88: Processing in the context of employment

GDPR Art. 88 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

GDPR Art. 89 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.
2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90: Obligations of secrecy

GDPR Art. 90 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91: Existing data protection rules of churches and religious associations

GDPR Art. 91 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

Article 92: Exercise of the delegation

GDPR Art. 92 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.
3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect

the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93: Committee procedure

GDPR Art. 93 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

Article 94: Repeal of Directive 95/46/EC

GDPR Art. 94 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. Directive 95/46/EC is repealed with effect from 25 May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95: Relationship with Directive 2002/58/EC

GDPR Art. 95 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

Article 96: Relationship with previously concluded Agreements

GDPR Art. 96 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97: Commission reports

GDPR Art. 97 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:
(a)
Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;
(b)
Chapter VII on cooperation and consistency.
3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.
5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98: Review of other Union legal acts on data protection

GDPR Art. 98 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99: Entry into force and application

GDPR Art. 99 · EUR-Lex, OJ L 119, 4.5.2016, p. 1 (as corrected) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from 25 May 2018.

Part 2: HIPAA Privacy, Security and Breach Notification Rules, official text

§ 160.101 Statutory basis and purpose.

45 CFR 160.101 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.101

The requirements of this subchapter implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

[78 FR 5687, Jan. 25, 2013]

§ 160.102 Applicability.

45 CFR 160.102 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.102

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

(c) To the extent required under the Social Security Act, 42 U.S.C. 1320a-7c(a)(5), nothing in this subchapter shall be construed to diminish the authority of any Inspector General, including such authority as provided in the Inspector General Act of 1978, as amended (5 U.S.C. App.).

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 78 FR 5687, Jan. 25, 2013]

§ 160.103 Definitions.

45 CFR 160.103 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.103

Except as otherwise provided, the following definitions apply to this subchapter:

Act means the Social Security Act.

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d-1320d-4, 1320d-7, 1320d-8, and 1320d-9;

(2) Section 264 of Pub. L. 104-191;

(3) Sections 13400-13424 of Public Law 111-5; or

(4) This subchapter.

ALJ means Administrative Law Judge.

ANSI stands for the American National Standards Institute.

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or penalty means the amount determined under § 160.404 of this part and includes the plural of these terms.

CMS stands for Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity means:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

EIN stands for the employer identification number assigned by the Internal Revenue Service, U.S. Department of the Treasury. The EIN is the taxpayer identifying number of an individual or other entity (whether or not an employer) assigned under one of the following:

(1) 26 U.S.C. 6011(b), which is the portion of the Internal Revenue Code dealing with identifying the taxpayer in tax returns and statements, or corresponding provisions of prior law.

(2) 26 U.S.C. 6109, which is the portion of the Internal Revenue Code dealing with identifying numbers in tax returns, statements, and other required documents.

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Employer is defined as it is in 26 U.S.C. 3401(d).

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

Group health plan (also see definition of health plan in this section) means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or

(2) Is administered by an entity other than the employer that established and maintains the plan.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does

either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer (as defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section) means an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO) (as defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section) means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(1) Health plan includes the following, singly or in combination:

(i) A group health plan, as defined in this section.

(ii) A health insurance issuer, as defined in this section.

(iii) An HMO, as defined in this section.

(iv) Part A or Part B of the Medicare program under title XVIII of the Act.

(v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w-101 through 1395w-152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

(xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.

(xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.

(xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.

(xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.

(xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

(2) Health plan excludes:

(i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

Implementation specification means specific requirements or instructions for implementing a standard.

Individual means the person who is the subject of protected health information.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Manifestation or manifested means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

Modify or modification refers to a change adopted by the Secretary, through regulation, to a standard or an implementation

specification.

Organized health care arrangement means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Person means a natural person (meaning a human being who is born alive), trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

Public health, as used in the terms “public health surveillance,” “public health investigation,” and “public health intervention,” means population-level activities to prevent disease in and promote the health of populations. Such activities include identifying, monitoring, preventing, or mitigating ongoing or prospective threats to the health or safety of a population, which may involve the collection of protected health information. But such activities do not include those with any of the following purposes:

(1) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating health care.

(2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating health care.

(3) To identify any person for any of the activities described at paragraphs (1) or (2) of this definition.

Reproductive health care means health care, as defined in this section, that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care.

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

Small health plan means a health plan with annual receipts of $5 million or less.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

Standard setting organization (SSO) means an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, State means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

Trading partner agreement means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

(1) Health care claims or equivalent encounter information.

(2) Health care payment and remittance advice.

(3) Coordination of benefits.

(4) Health care claim status.

(5) Enrollment and disenrollment in a health plan.

(6) Eligibility for a health plan.

(7) Health plan premium payments.

(8) Referral certification and authorization.

(9) First report of injury.

(10) Health care claims attachments.

(11) Health care electronic funds transfers (EFT) and remittance advice.

(12) Other transactions that the Secretary may prescribe by regulation.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Violation or violate means, as the context may require, failure to comply with an administrative simplification provision.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002; 67 FR 53266, Aug. 14, 2002; 68 FR 8374, Feb. 20, 2003; 71 FR 8424, Feb. 16, 2006; 76 FR 40495, July 8, 2011; 77 FR 1589, Jan. 10, 2012; 78 FR 5687, Jan. 25, 2013; 89 FR 33062, Apr. 26, 2024; 91 FR 14404, Mar. 24, 2026]

§ 160.104 Modifications.

45 CFR 160.104 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.104

(a) Except as provided in paragraph (b) of this section, the Secretary may adopt a modification to a standard or implementation specification adopted under this subchapter no more frequently than once every 12 months.

(b) The Secretary may adopt a modification at any time during the first year after the standard or implementation specification is initially adopted, if the Secretary determines that the modification is necessary to permit compliance with the standard or implementation specification.

(c) The Secretary will establish the compliance date for any standard or implementation specification modified under this section.

(1) The compliance date for a modification is no earlier than 180 days after the effective date of the final rule in which the Secretary adopts the modification.

(2) The Secretary may consider the extent of the modification and the time needed to comply with the modification in determining the compliance date for the modification.

(3) The Secretary may extend the compliance date for small health plans, as the Secretary determines is appropriate.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 38019, May 31, 2002]

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

45 CFR 160.105 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.105

Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.

[78 FR 5689, Jan. 25, 2013]

§ 160.201 Statutory basis.

45 CFR 160.201 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.201

The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104-191, section 264(c) of Public Law 104-191, and section 13421(a) of Public Law 111-5.

[78 FR 5689, Jan. 25, 2013]

§ 160.202 Definitions.

45 CFR 160.202 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.202

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act, section 264 of Public Law 104-191, or sections 13400-13424 of Public Law 111-5, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual, who is the subject of the individually identifiable health information, regarding access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information

about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 74 FR 42767, Aug. 24, 2009; 78 FR 5689, Jan. 25, 2013]

§ 160.203 General rule and exceptions.

45 CFR 160.203 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.203

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under § 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

[65 FR 82798, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002]

§ 160.204 Process for requesting exception determinations.

45 CFR 160.204 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.204

(a) A request to except a provision of State law from preemption under § 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or her designee. The request must be in writing and include the following information:

(1) The State law for which the exception is requested;

(2) The particular standard, requirement, or implementation specification for which the exception is requested;

(3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;

(4) How health care providers, health plans, and other entities would be affected by the exception;

(5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at § 160.203(a); and

(6) Any other information the Secretary may request in order to make the determination.

(b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.

(c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at § 160.203(a) has been met.

§ 160.205 Duration of effectiveness of exception determinations.

45 CFR 160.205 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.205

An exception granted under this subpart remains in effect until:

(a) Either the State law or the federal standard, requirement, or implementation specification that provided the basis for the exception is materially changed such that the ground for the exception no longer exists; or

(b) The Secretary revokes the exception, based on a determination that the ground supporting the need for the exception no longer exists.

§ 160.300 Applicability.

45 CFR 160.300 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.300

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

[78 FR 5690, Jan. 25, 2013]

§ 160.304 Principles for achieving compliance.

45 CFR 160.304 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.304

(a) Cooperation. The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) Assistance. The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

[78 FR 5690, Jan. 25, 2013]

§ 160.306 Complaints to the Secretary.

45 CFR 160.306 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.306

(a) Right to file a complaint. A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

(b) Requirements for filing complaints. Complaints under this section must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable administrative simplification provision(s).

(3) A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred, unless this time limit is waived by the Secretary for good cause shown.

(4) The Secretary may prescribe additional procedures for the filing of complaints, as well as the place and manner of filing, by notice in the Federal Register.

(c) Investigation. (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

[71 FR 8424, Feb. 16, 2006, as amended at 78 FR 5690, Jan. 25, 2013]

§ 160.308 Compliance reviews.

45 CFR 160.308 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.308

(a) The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

[78 FR 5690, Jan. 25, 2013]

§ 160.310 Responsibilities of covered entities and business associates.

45 CFR 160.310 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.310

(a) Provide records and compliance reports. A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) Cooperate with complaint investigations and compliance reviews. A covered entity or business associate must cooperate with

the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

(c) Permit access to information. (1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

[78 FR 5690, Jan. 25, 2013]

§ 160.312 Secretarial action regarding complaints and compliance reviews.

45 CFR 160.312 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.312

(a) Resolution when noncompliance is indicated. (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part.

(b) Resolution when no violation is found. If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

[78 FR 5690, Jan. 25, 2013]

§ 160.314 Investigational subpoenas and inquiries.

45 CFR 160.314 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.314

(a) The Secretary may issue subpoenas in accordance with 42 U.S.C. 405(d) and (e), 1320a-7a(j), and 1320d-5 to require the attendance and testimony of witnesses and the production of any other evidence during an investigation or compliance review pursuant to this part. For purposes of this paragraph, a person other than a natural person is termed an “entity.”

(1) A subpoena issued under this paragraph must—

(i) State the name of the person (including the entity, if applicable) to whom the subpoena is addressed;

(ii) State the statutory authority for the subpoena;

(iii) Indicate the date, time, and place that the testimony will take place;

(iv) Include a reasonably specific description of any documents or items required to be produced; and

(v) If the subpoena is addressed to an entity, describe with reasonable particularity the subject matter on which testimony is required. In that event, the entity must designate one or more natural persons who will testify on its behalf, and must state as to each such person that person's name and address and the matters on which he or she will testify. The designated person must testify as to matters known or reasonably available to the entity.

(2) A subpoena under this section must be served by—

(i) Delivering a copy to the natural person named in the subpoena or to the entity named in the subpoena at its last principal place of business; or

(ii) Registered or certified mail addressed to the natural person at his or her last known dwelling place or to the entity at its last known principal place of business.

(3) A verified return by the natural person serving the subpoena setting forth the manner of service or, in the case of service by registered or certified mail, the signed return post office receipt, constitutes proof of service.

(4) Witnesses are entitled to the same fees and mileage as witnesses in the district courts of the United States (28 U.S.C. 1821 and 1825). Fees need not be paid at the time the subpoena is served.

(5) A subpoena under this section is enforceable through the district court of the United States for the district where the subpoenaed natural person resides or is found or where the entity transacts business.

(b) Investigational inquiries are non-public investigational proceedings conducted by the Secretary.

(1) Testimony at investigational inquiries will be taken under oath or affirmation.

(2) Attendance of non-witnesses is discretionary with the Secretary, except that a witness is entitled to be accompanied, represented, and advised by an attorney.

(3) Representatives of the Secretary are entitled to attend and ask questions.

(4) A witness will have the opportunity to clarify his or her answers on the record following questioning by the Secretary.

(5) Any claim of privilege must be asserted by the witness on the record.

(6) Objections must be asserted on the record. Errors of any kind that might be corrected if promptly presented will be deemed to be waived unless reasonable objection is made at the investigational inquiry. Except where the objection is on the grounds of privilege, the question will be answered on the record, subject to objection.

(7) If a witness refuses to answer any question not privileged or to produce requested documents or items, or engages in conduct likely to delay or obstruct the investigational inquiry, the Secretary may seek enforcement of the subpoena under paragraph (a)(5) of this section.

(8) The proceedings will be recorded and transcribed. The witness is entitled to a copy of the transcript, upon payment of prescribed costs, except that, for good cause, the witness may be limited to inspection of the official transcript of his or her testimony.

(9)(i) The transcript will be submitted to the witness for signature.

(A) Where the witness will be provided a copy of the transcript, the transcript will be submitted to the witness for signature. The witness may submit to the Secretary written proposed corrections to the transcript, with such corrections attached to the transcript. If the witness does not return a signed copy of the transcript or proposed corrections within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of its being submitted to him or her for signature, the witness will be deemed to have agreed that the transcript is true and accurate.

(B) Where, as provided in paragraph (b)(8) of this section, the witness is limited to inspecting the transcript, the witness will have the opportunity at the time of inspection to propose corrections to the transcript, with corrections attached to the transcript. The witness will also have the opportunity to sign the transcript. If the witness does not sign the transcript or offer corrections within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of notice of the opportunity to inspect the transcript, the witness will be deemed to have agreed that the transcript is true and accurate.

(ii) The Secretary's proposed corrections to the record of transcript will be attached to the transcript.

(c) Consistent with § 160.310(c)(3), testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in any administrative or judicial proceeding.

§ 160.316 Refraining from intimidation or retaliation.

45 CFR 160.316 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.316

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

(a) Filing of a complaint under § 160.306;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under this part; or

(c) Opposing any act or practice made unlawful by this subchapter, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of protected health information in violation of subpart E of part 164 of this subchapter.

[71 FR 8424, Feb. 16, 2006, as amended at 78 FR 5691, Jan. 25, 2013]

§ 160.400 Applicability.

45 CFR 160.400 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.400

This subpart applies to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

§ 160.401 Definitions.

45 CFR 160.401 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.401

As used in this subpart, the following terms have the following meanings:

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

Reasonable diligence means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Willful neglect means conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.

[74 FR 56130, Oct. 30, 2009, as amended at 78 FR 5691, Jan. 25, 2013]

§ 160.402 Basis for a civil money penalty.

45 CFR 160.402 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.402

(a) General rule. Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) Violation by more than one covered entity or business associate. (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) Violation attributed to a covered entity or business associate. (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

[78 FR 5691, Jan. 25, 2013]

§ 160.404 Amount of a civil money penalty.

45 CFR 160.404 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.404

(a) The amount of a civil money penalty will be determined in accordance with paragraph (b) of this section, and §§ 160.406, 160.408, and 160.412. These amounts were adjusted in accordance with the Federal Civil Monetary Penalty Inflation Adjustment Act of 1990, (Pub. L. 101-140), as amended by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, (section 701 of Pub. L. 114-74), and appear at 45 CFR part 102. These amounts will be updated annually and published at 45 CFR part 102.

(b) The amount of a civil money penalty that may be imposed is subject to the following limitations:

(1) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty—

(i) In the amount of more than $100 for each violation; or

(ii) In excess of $25,000 for identical violations during a calendar year (January 1 through the following December 31);

(2) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty—

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

(A) In the amount of less than $100 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(ii) For a violation in which it is established that the violation was due to reasonable cause and not to willful neglect,

(A) In the amount of less than $1,000 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than $10,000 or more than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31);

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

(A) In the amount of less than $50,000 for each violation; or

(B) In excess of $1,500,000 for identical violations during a calendar year (January 1 through the following December 31).

(3) If a requirement or prohibition in one administrative simplification provision is repeated in a more general form in another administrative simplification provision in the same subpart, a civil money penalty may be imposed for a violation of only one of these administrative simplification provisions.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56130, Oct. 30, 2009; 78 FR 5691, Jan. 25, 2013; 81 FR 61581, Sept. 6, 2016]

§ 160.406 Violations of an identical requirement or prohibition.

45 CFR 160.406 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.406

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

[78 FR 5691, Jan. 25, 2013]

§ 160.408 Factors considered in determining the amount of a civil money penalty.

45 CFR 160.408 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.408

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

[78 FR 5691, Jan. 25, 2013]

§ 160.410 Affirmative defenses.

45 CFR 160.410 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.410

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d-6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d-6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:

(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable

diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

[78 FR 5692, Jan. 25, 2013]

§ 160.412 Waiver.

45 CFR 160.412 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.412

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

[8 FR 5692, Jan. 25, 2013]

§ 160.414 Limitations.

45 CFR 160.414 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.414

No action under this subpart may be entertained unless commenced by the Secretary, in accordance with § 160.420, within 6 years from the date of the occurrence of the violation.

§ 160.416 Authority to settle.

45 CFR 160.416 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.416

Nothing in this subpart limits the authority of the Secretary to settle any issue or case or to compromise any penalty.

§ 160.418 Penalty not exclusive.

45 CFR 160.418 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.418

Except as otherwise provided by 42 U.S.C. 1320d-5(b)(1) and 42 U.S.C. 299b-22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

[78 FR 5692, Jan. 25, 2013]

§ 160.420 Notice of proposed determination.

45 CFR 160.420 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.420

(a) If a penalty is proposed in accordance with this part, the Secretary must deliver, or send by certified mail with return receipt requested, to the respondent, written notice of the Secretary's intent to impose a penalty. This notice of proposed determination must include—

(1) Reference to the statutory basis for the penalty;

(2) A description of the findings of fact regarding the violations with respect to which the penalty is proposed (except that, in any case where the Secretary is relying upon a statistical sampling study in accordance with § 160.536 of this part, the notice must

provide a copy of the study relied upon by the Secretary);

(3) The reason(s) why the violation(s) subject(s) the respondent to a penalty;

(4) The amount of the proposed penalty and a reference to the subparagraph of § 160.404 upon which it is based.

(5) Any circumstances described in § 160.408 that were considered in determining the amount of the proposed penalty; and

(6) Instructions for responding to the notice, including a statement of the respondent's right to a hearing, a statement that failure to request a hearing within 90 days permits the imposition of the proposed penalty without the right to a hearing under § 160.504 or a right of appeal under § 160.548 of this part, and the address to which the hearing request must be sent.

(b) The respondent may request a hearing before an ALJ on the proposed penalty by filing a request in accordance with § 160.504 of this part.

[71 FR 8426, Feb. 16, 2006, as amended at 74 FR 56131, Oct. 30, 2009]

§ 160.422 Failure to request a hearing.

45 CFR 160.422 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.422

If the respondent does not request a hearing within the time prescribed by § 160.504 of this part and the matter is not settled pursuant to § 160.416, the Secretary will impose the proposed penalty or any lesser penalty permitted by 42 U.S.C. 1320d-5. The Secretary will notify the respondent by certified mail, return receipt requested, of any penalty that has been imposed and of the means by which the respondent may satisfy the penalty, and the penalty is final on receipt of the notice. The respondent has no right to appeal a penalty under § 160.548 of this part with respect to which the respondent has not timely requested a hearing.

§ 160.424 Collection of penalty.

45 CFR 160.424 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.424

(a) Once a determination of the Secretary to impose a penalty has become final, the penalty will be collected by the Secretary, subject to the first sentence of 42 U.S.C. 1320a-7a(f).

(b) The penalty may be recovered in a civil action brought in the United States district court for the district where the respondent resides, is found, or is located.

(c) The amount of a penalty, when finally determined, or the amount agreed upon in compromise, may be deducted from any sum then or later owing by the United States, or by a State agency, to the respondent.

(d) Matters that were raised or that could have been raised in a hearing before an ALJ, or in an appeal under 42 U.S.C. 1320a-7a(e), may not be raised as a defense in a civil action by the United States to collect a penalty under this part.

§ 160.426 Notification of the public and other agencies.

45 CFR 160.426 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.426

Whenever a proposed penalty becomes final, the Secretary will notify, in such manner as the Secretary deems appropriate, the public and the following organizations and entities thereof and the reason it was imposed: the appropriate State or local medical or professional organization, the appropriate State agency or agencies administering or supervising the administration of State health care programs (as defined in 42 U.S.C. 1320a-7(h)), the appropriate utilization and quality control peer review organization, and the appropriate State or local licensing agency or organization (including the agency specified in 42 U.S.C. 1395aa(a), 1396a(a)(33)).

§ 160.500 Applicability.

45 CFR 160.500 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.500

This subpart applies to hearings conducted relating to the imposition of a civil money penalty by the Secretary under 42 U.S.C. 1320d-5.

§ 160.502 Definitions.

45 CFR 160.502 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.502

As used in this subpart, the following term has the following meaning:

Board means the members of the HHS Departmental Appeals Board, in the Office of the Secretary, who issue decisions in panels of three.

§ 160.504 Hearing before an ALJ.

45 CFR 160.504 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.504

(a) A respondent may request a hearing before an ALJ. The parties to the hearing proceeding consist of—

(1) The respondent; and

(2) The officer(s) or employee(s) of HHS to whom the enforcement authority involved has been delegated.

(b) The request for a hearing must be made in writing signed by the respondent or by the respondent's attorney and sent by certified mail, return receipt requested, to the address specified in the notice of proposed determination. The request for a hearing must be mailed within 90 days after notice of the proposed determination is received by the respondent. For purposes of this section, the respondent's date of receipt of the notice of proposed determination is presumed to be 5 days after the date of the notice unless the respondent makes a reasonable showing to the contrary to the ALJ.

(c) The request for a hearing must clearly and directly admit, deny, or explain each of the findings of fact contained in the notice of proposed determination with regard to which the respondent has any knowledge. If the respondent has no knowledge of a particular finding of fact and so states, the finding shall be deemed denied. The request for a hearing must also state the circumstances or arguments that the respondent alleges constitute the grounds for any defense and the factual and legal basis for opposing the penalty, except that a respondent may raise an affirmative defense under § 160.410(b)(1) at any time.

(d) The ALJ must dismiss a hearing request where—

(1) On motion of the Secretary, the ALJ determines that the respondent's hearing request is not timely filed as required by paragraphs (b) or does not meet the requirements of paragraph (c) of this section;

(2) The respondent withdraws the request for a hearing;

(3) The respondent abandons the request for a hearing; or

(4) The respondent's hearing request fails to raise any issue that may properly be addressed in a hearing.

§ 160.506 Rights of the parties.

45 CFR 160.506 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.506

(a) Except as otherwise limited by this subpart, each party may—

(1) Be accompanied, represented, and advised by an attorney;

(2) Participate in any conference held by the ALJ;

(3) Conduct discovery of documents as permitted by this subpart;

(4) Agree to stipulations of fact or law that will be made part of the record;

(5) Present evidence relevant to the issues at the hearing;

(6) Present and cross-examine witnesses;

(7) Present oral arguments at the hearing as permitted by the ALJ; and

(8) Submit written briefs and proposed findings of fact and conclusions of law after the hearing.

(b) A party may appear in person or by a representative. Natural persons who appear as an attorney or other representative must conform to the standards of conduct and ethics required of practitioners before the courts of the United States.

(c) Fees for any services performed on behalf of a party by an attorney are not subject to the provisions of 42 U.S.C. 406, which authorizes the Secretary to specify or limit their fees.

§ 160.508 Authority of the ALJ.

45 CFR 160.508 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.508

(a) The ALJ must conduct a fair and impartial hearing, avoid delay, maintain order, and ensure that a record of the proceeding is made.

(b) The ALJ may—

(1) Set and change the date, time and place of the hearing upon reasonable notice to the parties;

(2) Continue or recess the hearing in whole or in part for a reasonable period of time;

(3) Hold conferences to identify or simplify the issues, or to consider other matters that may aid in the expeditious disposition of the proceeding;

(4) Administer oaths and affirmations;

(5) Issue subpoenas requiring the attendance of witnesses at hearings and the production of documents at or in relation to hearings;

(6) Rule on motions and other procedural matters;

(7) Regulate the scope and timing of documentary discovery as permitted by this subpart;

(8) Regulate the course of the hearing and the conduct of representatives, parties, and witnesses;

(9) Examine witnesses;

(10) Receive, rule on, exclude, or limit evidence;

(11) Upon motion of a party, take official notice of facts;

(12) Conduct any conference, argument or hearing in person or, upon agreement of the parties, by telephone; and

(13) Upon motion of a party, decide cases, in whole or in part, by summary judgment where there is no disputed issue of material fact. A summary judgment decision constitutes a hearing on the record for the purposes of this subpart.

(c) The ALJ—

(1) May not find invalid or refuse to follow Federal statutes, regulations, or Secretarial delegations of authority and must give deference to published guidance to the extent not inconsistent with statute or regulation;

(2) May not enter an order in the nature of a directed verdict;

(3) May not compel settlement negotiations;

(4) May not enjoin any act of the Secretary; or

(5) May not review the exercise of discretion by the Secretary with respect to whether to grant an extension under § 160.410(b)(2)(ii)(B) or (c)(2)(ii) of this part or to provide technical assistance under 42 U.S.C. 1320d-5(b)(2)(B).

[71 FR 8428, Feb. 16, 2006, as amended at 78 FR 34266, June 7, 2013]

§ 160.510 Ex parte contacts.

45 CFR 160.510 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.510

No party or person (except employees of the ALJ's office) may communicate in any way with the ALJ on any matter at issue in a case, unless on notice and opportunity for both parties to participate. This provision does not prohibit a party or person from inquiring about the status of a case or asking routine questions concerning administrative functions or procedures.

§ 160.512 Prehearing conferences.

45 CFR 160.512 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.512

(a) The ALJ must schedule at least one prehearing conference, and may schedule additional prehearing conferences as appropriate, upon reasonable notice, which may not be less than 14 business days, to the parties.

(b) The ALJ may use prehearing conferences to discuss the following—

(1) Simplification of the issues;

(2) The necessity or desirability of amendments to the pleadings, including the need for a more definite statement;

(3) Stipulations and admissions of fact or as to the contents and authenticity of documents;

(4) Whether the parties can agree to submission of the case on a stipulated record;

(5) Whether a party chooses to waive appearance at an oral hearing and to submit only documentary evidence (subject to the objection of the other party) and written argument;

(6) Limitation of the number of witnesses;

(7) Scheduling dates for the exchange of witness lists and of proposed exhibits;

(8) Discovery of documents as permitted by this subpart;

(9) The time and place for the hearing;

(10) The potential for the settlement of the case by the parties; and

(11) Other matters as may tend to encourage the fair, just and expeditious disposition of the proceedings, including the protection of privacy of individually identifiable health information that may be submitted into evidence or otherwise used in the proceeding, if appropriate.

(c) The ALJ must issue an order containing the matters agreed upon by the parties or ordered by the ALJ at a prehearing conference.

§ 160.514 Authority to settle.

45 CFR 160.514 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.514

The Secretary has exclusive authority to settle any issue or case without the consent of the ALJ.

§ 160.516 Discovery.

45 CFR 160.516 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.516

(a) A party may make a request to another party for production of documents for inspection and copying that are relevant and material to the issues before the ALJ.

(b) For the purpose of this section, the term “documents” includes information, reports, answers, records, accounts, papers and other data and documentary evidence. Nothing contained in this section may be interpreted to require the creation of a document, except that requested data stored in an electronic data storage system must be produced in a form accessible to the requesting party.

(c) Requests for documents, requests for admissions, written interrogatories, depositions and any forms of discovery, other than those permitted under paragraph (a) of this section, are not authorized.

(d) This section may not be construed to require the disclosure of interview reports or statements obtained by any party, or on behalf of any party, of persons who will not be called as witnesses by that party, or analyses and summaries prepared in conjunction with the investigation or litigation of the case, or any otherwise privileged documents.

(e)(1) When a request for production of documents has been received, within 30 days the party receiving that request must either fully respond to the request, or state that the request is being objected to and the reasons for that objection. If objection is made to part of an item or category, the part must be specified. Upon receiving any objections, the party seeking production may then, within 30 days or any other time frame set by the ALJ, file a motion for an order compelling discovery. The party receiving a request for production may also file a motion for protective order any time before the date the production is due.

(2) The ALJ may grant a motion for protective order or deny a motion for an order compelling discovery if the ALJ finds that the discovery sought—

(i) Is irrelevant;

(ii) Is unduly costly or burdensome;

(iii) Will unduly delay the proceeding; or

(iv) Seeks privileged information.

(3) The ALJ may extend any of the time frames set forth in paragraph (e)(1) of this section.

(4) The burden of showing that discovery should be allowed is on the party seeking discovery.

§ 160.518 Exchange of witness lists, witness statements, and exhibits.

45 CFR 160.518 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.518

(a) The parties must exchange witness lists, copies of prior written statements of proposed witnesses, and copies of proposed hearing exhibits, including copies of any written statements that the party intends to offer in lieu of live testimony in accordance with § 160.538, not more than 60, and not less than 15, days before the scheduled hearing, except that if a respondent intends to introduce the evidence of a statistical expert, the respondent must provide the Secretarial party with a copy of the statistical expert's report not less than 30 days before the scheduled hearing.

(b)(1) If, at any time, a party objects to the proposed admission of evidence not exchanged in accordance with paragraph (a) of this section, the ALJ must determine whether the failure to comply with paragraph (a) of this section should result in the exclusion of that evidence.

(2) Unless the ALJ finds that extraordinary circumstances justified the failure timely to exchange the information listed under paragraph (a) of this section, the ALJ must exclude from the party's case-in-chief—

(i) The testimony of any witness whose name does not appear on the witness list; and

(ii) Any exhibit not provided to the opposing party as specified in paragraph (a) of this section.

(3) If the ALJ finds that extraordinary circumstances existed, the ALJ must then determine whether the admission of that evidence would cause substantial prejudice to the objecting party.

(i) If the ALJ finds that there is no substantial prejudice, the evidence may be admitted.

(ii) If the ALJ finds that there is substantial prejudice, the ALJ may exclude the evidence, or, if he or she does not exclude the evidence, must postpone the hearing for such time as is necessary for the objecting party to prepare and respond to the evidence, unless the objecting party waives postponement.

(c) Unless the other party objects within a reasonable period of time before the hearing, documents exchanged in accordance with paragraph (a) of this section will be deemed to be authentic for the purpose of admissibility at the hearing.

§ 160.520 Subpoenas for attendance at hearing.

45 CFR 160.520 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.520

(a) A party wishing to procure the appearance and testimony of any person at the hearing may make a motion requesting the ALJ to issue a subpoena if the appearance and testimony are reasonably necessary for the presentation of a party's case.

(b) A subpoena requiring the attendance of a person in accordance with paragraph (a) of this section may also require the person (whether or not the person is a party) to produce relevant and material evidence at or before the hearing.

(c) When a subpoena is served by a respondent on a particular employee or official or particular office of HHS, the Secretary may comply by designating any knowledgeable HHS representative to appear and testify.

(d) A party seeking a subpoena must file a written motion not less than 30 days before the date fixed for the hearing, unless otherwise allowed by the ALJ for good cause shown. That motion must—

(1) Specify any evidence to be produced;

(2) Designate the witnesses; and

(3) Describe the address and location with sufficient particularity to permit those witnesses to be found.

(e) The subpoena must specify the time and place at which the witness is to appear and any evidence the witness is to produce.

(f) Within 15 days after the written motion requesting issuance of a subpoena is served, any party may file an opposition or other response.

(g) If the motion requesting issuance of a subpoena is granted, the party seeking the subpoena must serve it by delivery to the person named, or by certified mail addressed to that person at the person's last dwelling place or principal place of business.

(h) The person to whom the subpoena is directed may file with the ALJ a motion to quash the subpoena within 10 days after service.

(i) The exclusive remedy for contumacy by, or refusal to obey a subpoena duly served upon, any person is specified in 42 U.S.C. 405(e).

§ 160.522 Fees.

45 CFR 160.522 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.522

The party requesting a subpoena must pay the cost of the fees and mileage of any witness subpoenaed in the amounts that would be payable to a witness in a proceeding in United States District Court. A check for witness fees and mileage must accompany the subpoena when served, except that, when a subpoena is issued on behalf of the Secretary, a check for witness fees and mileage need not accompany the subpoena.

§ 160.524 Form, filing, and service of papers.

45 CFR 160.524 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.524

(a) Forms. (1) Unless the ALJ directs the parties to do otherwise, documents filed with the ALJ must include an original and two copies.

(2) Every pleading and paper filed in the proceeding must contain a caption setting forth the title of the action, the case number, and a designation of the paper, such as motion to quash subpoena.

(3) Every pleading and paper must be signed by and must contain the address and telephone number of the party or the person on whose behalf the paper was filed, or his or her representative.

(4) Papers are considered filed when they are mailed.

(b) Service. A party filing a document with the ALJ or the Board must, at the time of filing, serve a copy of the document on the other party. Service upon any party of any document must be made by delivering a copy, or placing a copy of the document in the United States mail, postage prepaid and addressed, or with a private delivery service, to the party's last known address. When a party is represented by an attorney, service must be made upon the attorney in lieu of the party.

(c) Proof of service. A certificate of the natural person serving the document by personal delivery or by mail, setting forth the manner of service, constitutes proof of service.

§ 160.526 Computation of time.

45 CFR 160.526 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.526

(a) In computing any period of time under this subpart or in an order issued thereunder, the time begins with the day following the act, event or default, and includes the last day of the period unless it is a Saturday, Sunday, or legal holiday observed by the Federal Government, in which event it includes the next business day.

(b) When the period of time allowed is less than 7 days, intermediate Saturdays, Sundays, and legal holidays observed by the Federal Government must be excluded from the computation.

(c) Where a document has been served or issued by placing it in the mail, an additional 5 days must be added to the time permitted for any response. This paragraph does not apply to requests for hearing under § 160.504.

§ 160.528 Motions.

45 CFR 160.528 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.528

(a) An application to the ALJ for an order or ruling must be by motion. Motions must state the relief sought, the authority relied upon and the facts alleged, and must be filed with the ALJ and served on all other parties.

(b) Except for motions made during a prehearing conference or at the hearing, all motions must be in writing. The ALJ may require that oral motions be reduced to writing.

(c) Within 10 days after a written motion is served, or such other time as may be fixed by the ALJ, any party may file a response to the motion.

(d) The ALJ may not grant a written motion before the time for filing responses has expired, except upon consent of the parties or following a hearing on the motion, but may overrule or deny the motion without awaiting a response.

(e) The ALJ must make a reasonable effort to dispose of all outstanding motions before the beginning of the hearing.

§ 160.530 Sanctions.

45 CFR 160.530 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.530

The ALJ may sanction a person, including any party or attorney, for failing to comply with an order or procedure, for failing to defend an action or for other misconduct that interferes with the speedy, orderly or fair conduct of the hearing. The sanctions must reasonably relate to the severity and nature of the failure or misconduct. The sanctions may include—

(a) In the case of refusal to provide or permit discovery under the terms of this part, drawing negative factual inferences or treating the refusal as an admission by deeming the matter, or certain facts, to be established;

(b) Prohibiting a party from introducing certain evidence or otherwise supporting a particular claim or defense;

(c) Striking pleadings, in whole or in part;

(d) Staying the proceedings;

(e) Dismissal of the action;

(f) Entering a decision by default;

(g) Ordering the party or attorney to pay the attorney's fees and other costs caused by the failure or misconduct; and

(h) Refusing to consider any motion or other action that is not filed in a timely manner.

§ 160.532 Collateral estoppel.

45 CFR 160.532 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.532

When a final determination that the respondent violated an administrative simplification provision has been rendered in any proceeding in which the respondent was a party and had an opportunity to be heard, the respondent is bound by that determination in any proceeding under this part.

§ 160.534 The hearing.

45 CFR 160.534 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.534

(a) The ALJ must conduct a hearing on the record in order to determine whether the respondent should be found liable under this part.

(b) (1) The respondent has the burden of going forward and the burden of persuasion with respect to any:

(i) Affirmative defense pursuant to § 160.410 of this part;

(ii) Challenge to the amount of a proposed penalty pursuant to §§ 160.404-160.408 of this part, including any factors raised as mitigating factors; or

(iii) Claim that a proposed penalty should be reduced or waived pursuant to § 160.412 of this part; and

(iv) Compliance with subpart D of part 164, as provided under § 164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

(3) The burden of persuasion will be judged by a preponderance of the evidence.

(c) The hearing must be open to the public unless otherwise ordered by the ALJ for good cause shown.

(d)(1) Subject to the 15-day rule under § 160.518(a) and the admissibility of evidence under § 160.540, either party may introduce, during its case in chief, items or information that arose or became known after the date of the issuance of the notice of proposed determination or the request for hearing, as applicable. Such items and information may not be admitted into evidence, if introduced—

(i) By the Secretary, unless they are material and relevant to the acts or omissions with respect to which the penalty is proposed in the notice of proposed determination pursuant to § 160.420 of this part, including circumstances that may increase penalties; or

(ii) By the respondent, unless they are material and relevant to an admission, denial or explanation of a finding of fact in the notice of proposed determination under § 160.420 of this part, or to a specific circumstance or argument expressly stated in the request for hearing under § 160.504, including circumstances that may reduce penalties.

(2) After both parties have presented their cases, evidence may be admitted in rebuttal even if not previously exchanged in accordance with § 160.518.

[71 FR 8428, Feb. 16, 2006, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5692, Jan. 25, 2013]

§ 160.536 Statistical sampling.

45 CFR 160.536 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.536

(a) In meeting the burden of proof set forth in § 160.534, the Secretary may introduce the results of a statistical sampling study as evidence of the number of violations under § 160.406 of this part, or the factors considered in determining the amount of the civil money penalty under § 160.408 of this part. Such statistical sampling study, if based upon an appropriate sampling and computed by valid statistical methods, constitutes prima facie evidence of the number of violations and the existence of factors material to the proposed civil money penalty as described in §§ 160.406 and 160.408.

(b) Once the Secretary has made a prima facie case, as described in paragraph (a) of this section, the burden of going forward shifts to the respondent to produce evidence reasonably calculated to rebut the findings of the statistical sampling study. The Secretary will then be given the opportunity to rebut this evidence.

§ 160.538 Witnesses.

45 CFR 160.538 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.538

(a) Except as provided in paragraph (b) of this section, testimony at the hearing must be given orally by witnesses under oath or affirmation.

(b) At the discretion of the ALJ, testimony of witnesses other than the testimony of expert witnesses may be admitted in the form of a written statement. The ALJ may, at his or her discretion, admit prior sworn testimony of experts that has been subject to adverse examination, such as a deposition or trial testimony. Any such written statement must be provided to the other party, along with the last known address of the witness, in a manner that allows sufficient time for the other party to subpoena the witness for cross-examination at the hearing. Prior written statements of witnesses proposed to testify at the hearing must be exchanged as provided in § 160.518.

(c) The ALJ must exercise reasonable control over the mode and order of interrogating witnesses and presenting evidence so as to:

(1) Make the interrogation and presentation effective for the ascertainment of the truth;

(2) Avoid repetition or needless consumption of time; and

(3) Protect witnesses from harassment or undue embarrassment.

(d) The ALJ must permit the parties to conduct cross-examination of witnesses as may be required for a full and true disclosure of the facts.

(e) The ALJ may order witnesses excluded so that they cannot hear the testimony of other witnesses, except that the ALJ may not order to be excluded—

(1) A party who is a natural person;

(2) In the case of a party that is not a natural person, the officer or employee of the party appearing for the entity pro se or designated as the party's representative; or

(3) A natural person whose presence is shown by a party to be essential to the presentation of its case, including a person engaged in assisting the attorney for the Secretary.

§ 160.540 Evidence.

45 CFR 160.540 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.540

(a) The ALJ must determine the admissibility of evidence.

(b) Except as provided in this subpart, the ALJ is not bound by the Federal Rules of Evidence. However, the ALJ may apply the Federal Rules of Evidence where appropriate, for example, to exclude unreliable evidence.

(c) The ALJ must exclude irrelevant or immaterial evidence.

(d) Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or by considerations of undue delay or needless presentation of cumulative evidence.

(e) Although relevant, evidence must be excluded if it is privileged under Federal law.

(f) Evidence concerning offers of compromise or settlement are inadmissible to the extent provided in Rule 408 of the Federal Rules of Evidence.

(g) Evidence of crimes, wrongs, or acts other than those at issue in the instant case is admissible in order to show motive, opportunity, intent, knowledge, preparation, identity, lack of mistake, or existence of a scheme. This evidence is admissible regardless of whether the crimes, wrongs, or acts occurred during the statute of limitations period applicable to the acts or omissions that constitute the basis for liability in the case and regardless of whether they were referenced in the Secretary's notice of proposed determination under § 160.420 of this part.

(h) The ALJ must permit the parties to introduce rebuttal witnesses and evidence.

(i) All documents and other evidence offered or taken for the record must be open to examination by both parties, unless otherwise ordered by the ALJ for good cause shown.

§ 160.542 The record.

45 CFR 160.542 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.542

(a) The hearing must be recorded and transcribed. Transcripts may be obtained following the hearing from the ALJ. A party that requests a transcript of hearing proceedings must pay the cost of preparing the transcript unless, for good cause shown by the party, the payment is waived by the ALJ or the Board, as appropriate.

(b) The transcript of the testimony, exhibits, and other evidence admitted at the hearing, and all papers and requests filed in the proceeding constitute the record for decision by the ALJ and the Secretary.

(c) The record may be inspected and copied (upon payment of a reasonable fee) by any person, unless otherwise ordered by the ALJ for good cause shown.

(d) For good cause, the ALJ may order appropriate redactions made to the record.

§ 160.544 Post hearing briefs.

45 CFR 160.544 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.544

The ALJ may require the parties to file post-hearing briefs. In any event, any party may file a post-hearing brief. The ALJ must fix the time for filing the briefs. The time for filing may not exceed 60 days from the date the parties receive the transcript of the hearing or, if applicable, the stipulated record. The briefs may be accompanied by proposed findings of fact and conclusions of law. The ALJ may permit the parties to file reply briefs.

§ 160.546 ALJ's decision.

45 CFR 160.546 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.546

(a) The ALJ must issue a decision, based only on the record, which must contain findings of fact and conclusions of law.

(b) The ALJ may affirm, increase, or reduce the penalties imposed by the Secretary.

(c) The ALJ must issue the decision to both parties within 60 days after the time for submission of post-hearing briefs and reply briefs, if permitted, has expired. If the ALJ fails to meet the deadline contained in this paragraph, he or she must notify the parties of the reason for the delay and set a new deadline.

(d) Unless the decision of the ALJ is timely appealed as provided for in § 160.548, the decision of the ALJ will be final and binding on the parties 60 days from the date of service of the ALJ's decision.

§ 160.548 Appeal of the ALJ's decision.

45 CFR 160.548 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.548

(a) Any party may appeal the decision of the ALJ to the Board by filing a notice of appeal with the Board within 30 days of the date of service of the ALJ decision. The Board may extend the initial 30 day period for a period of time not to exceed 30 days if a party files with the Board a request for an extension within the initial 30 day period and shows good cause.

(b) If a party files a timely notice of appeal with the Board, the ALJ must forward the record of the proceeding to the Board.

(c) A notice of appeal must be accompanied by a written brief specifying exceptions to the initial decision and reasons supporting the exceptions. Any party may file a brief in opposition to the exceptions, which may raise any relevant issue not addressed in the exceptions, within 30 days of receiving the notice of appeal and the accompanying brief. The Board may permit the parties to file reply briefs.

(d) There is no right to appear personally before the Board or to appeal to the Board any interlocutory ruling by the ALJ.

(e) Except for an affirmative defense under § 160.410(a)(1) or (2) of this part, the Board may not consider any issue not raised in the parties' briefs, nor any issue in the briefs that could have been raised before the ALJ but was not.

(f) If any party demonstrates to the satisfaction of the Board that additional evidence not presented at such hearing is relevant and material and that there were reasonable grounds for the failure to adduce such evidence at the hearing, the Board may remand the matter to the ALJ for consideration of such additional evidence.

(g) The Board may decline to review the case, or may affirm, increase, reduce, reverse or remand any penalty determined by the ALJ.

(h) The standard of review on a disputed issue of fact is whether the initial decision of the ALJ is supported by substantial evidence on the whole record. The standard of review on a disputed issue of law is whether the decision is erroneous.

(i) Within 60 days after the time for submission of briefs and reply briefs, if permitted, has expired, the Board must serve on each party to the appeal a copy of the Board's decision and a statement describing the right of any respondent who is penalized to seek judicial review.

(j)(1) The Board's decision under paragraph (i) of this section, including a decision to decline review of the initial decision,

becomes the final decision of the Secretary 60 days after the date of service of the Board's decision, except with respect to a decision to remand to the ALJ or if reconsideration is requested under this paragraph.

(2) The Board will reconsider its decision only if it determines that the decision contains a clear error of fact or error of law. New evidence will not be a basis for reconsideration unless the party demonstrates that the evidence is newly discovered and was not previously available.

(3) A party may file a motion for reconsideration with the Board before the date the decision becomes final under paragraph (j)(1) of this section. A motion for reconsideration must be accompanied by a written brief specifying any alleged error of fact or law and, if the party is relying on additional evidence, explaining why the evidence was not previously available. Any party may file a brief in opposition within 15 days of receiving the motion for reconsideration and the accompanying brief unless this time limit is extended by the Board for good cause shown. Reply briefs are not permitted.

(4) The Board must rule on the motion for reconsideration not later than 30 days from the date the opposition brief is due. If the Board denies the motion, the decision issued under paragraph (i) of this section becomes the final decision of the Secretary on the date of service of the ruling. If the Board grants the motion, the Board will issue a reconsidered decision, after such procedures as the Board determines necessary to address the effect of any error. The Board's decision on reconsideration becomes the final decision of the Secretary on the date of service of the decision, except with respect to a decision to remand to the ALJ.

(5) If service of a ruling or decision issued under this section is by mail, the date of service will be deemed to be 5 days from the date of mailing.

(k)(1) A respondent's petition for judicial review must be filed within 60 days of the date on which the decision of the Board becomes the final decision of the Secretary under paragraph (j) of this section.

(2) In compliance with 28 U.S.C. 2112(a), a copy of any petition for judicial review filed in any U.S. Court of Appeals challenging the final decision of the Secretary must be sent by certified mail, return receipt requested, to the General Counsel of HHS. The petition copy must be a copy showing that it has been time-stamped by the clerk of the court when the original was filed with the court.

(3) If the General Counsel of HHS received two or more petitions within 10 days after the final decision of the Secretary, the General Counsel will notify the U.S. Judicial Panel on Multidistrict Litigation of any petitions that were received within the 10 day period.

[71 FR 8428, Feb. 16, 2006, as amended at 78 FR 34266, June 7, 2013]

§ 160.550 Stay of the Secretary's decision.

45 CFR 160.550 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.550

(a) Pending judicial review, the respondent may file a request for stay of the effective date of any penalty with the ALJ. The request must be accompanied by a copy of the notice of appeal filed with the Federal court. The filing of the request automatically stays the effective date of the penalty until such time as the ALJ rules upon the request.

(b) The ALJ may not grant a respondent's request for stay of any penalty unless the respondent posts a bond or provides other adequate security.

(c) The ALJ must rule upon a respondent's request for stay within 10 days of receipt.

§ 160.552 Harmless error.

45 CFR 160.552 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-160.552

No error in either the admission or the exclusion of evidence, and no error or defect in any ruling or order or in any act done or omitted by the ALJ or by any of the parties is ground for vacating, modifying or otherwise disturbing an otherwise appropriate ruling or order or act, unless refusal to take such action appears to the ALJ or the Board inconsistent with substantial justice. The ALJ and the Board at every stage of the proceeding must disregard any error or defect in the proceeding that does not affect the substantial rights of the parties.

§ 164.102 Statutory basis.

45 CFR 164.102 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.102

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104-191, and sections 13400-13424 of Public Law 111-5.

[78 FR 5692, Jan. 25, 2013]

§ 164.103 Definitions.

45 CFR 164.103 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.103

As used in this part, the following terms have the following meanings:

Common control exists if an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.

Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in another entity.

Covered functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).

Hybrid entity means a single legal entity:

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with paragraph § 164.105(a)(2)(iii)(D).

Law enforcement official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Plan sponsor is defined as defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Required by law means a mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

[68 FR 8374, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 34266, June 7, 2013]

§ 164.104 Applicability.

45 CFR 164.104 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.104

(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this part apply to the following entities:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.105 Organizational requirements.

45 CFR 164.105 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.105

(a)(1) Standard: Health care component. If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, §§ 164.314, and 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) Implementation specifications:

(i) Application of other provisions. In applying a provision of this part, other than the requirements of this section, §§ 164.314, and 164.504, to a hybrid entity:

(A) A reference in such provision to a “covered entity” refers to a health care component of the covered entity;

(B) A reference in such provision to a “health plan,” “covered health care provider,” or “health care clearinghouse,” refers to a health care component of the covered entity if such health care component performs the functions of a health plan, health care provider, or health care clearinghouse, as applicable;

(C) A reference in such provision to “protected health information” refers to protected health information that is created or received by or on behalf of the health care component of the covered entity; and

(D) A reference in such provision to “electronic protected health information” refers to electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity.

(ii) Safeguard requirements. The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member

must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) Responsibilities of the covered entity. A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with §§ 164.316(a) and 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with §§ 164.314 and 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) Standard: Affiliated covered entities. Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) Implementation specifications—(i) Requirements for designation of an affiliated covered entity. (A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) Safeguard requirements. An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, §§ 164.308(a)(4)(ii)(A) and 164.504(g), as applicable.

(c)(1) Standard: Documentation. A covered entity must maintain a written or electronic record of a designation as required by paragraphs (a) or (b) of this section.

(2) Implementation specification: Retention period. A covered entity must retain the documentation as required by paragraph (c)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

[68 FR 8375, Feb. 20, 2003, as amended at 78 FR 5692, Jan. 25, 2013]

§ 164.106 Relationship to other parts.

45 CFR 164.106 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.106

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

[78 FR 5693, Jan. 25, 2013]

§ 164.302 Applicability.

45 CFR 164.302 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.302

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

[78 FR 5693, Jan. 25, 2013]

§ 164.304 Definitions.

45 CFR 164.304 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.304

As used in this subpart, the following terms have the following meanings:

Access means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to “access” as used in this subpart, not as used in subparts D or E of this part.)

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

Authentication means the corroboration that a person is the one claimed.

Availability means the property that data or information is accessible and useable upon demand by an authorized person.

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility means the physical premises and the interior and exterior of a building(s).

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software means software, for example, a virus, designed to damage or disrupt a system.

Password means confidential authentication information composed of a string of characters.

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Security or Security measures encompass all of the administrative, physical, and technical safeguards in an information system.

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

User means a person or entity with authorized access.

Workstation means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

[68 FR 8376, Feb. 20, 2003, as amended at 74 FR 42767, Aug. 24, 2009; 78 FR 5693, Jan. 25, 2013]

§ 164.306 Security standards: General rules.

45 CFR 164.306 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.306

(a) General requirements. Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach. (1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c) Standards. A covered entity or business associate must comply with the applicable standards as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information.

(d) Implementation specifications. In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

$(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

$(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

[68 FR 8376, Feb. 20, 2003; 68 FR 17153, Apr. 8, 2003; 78 FR 5693, Jan. 25, 2013]

§ 164.308 Administrative safeguards.

45 CFR 164.308 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.308

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3)(i) Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) Implementation specifications:

(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4)(i) Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

(ii) Implementation specifications:

(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement:

(A) Security reminders (Addressable). Periodic security updates.

(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.

(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.

(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

(6)(i) Standard: Security incident procedures. Implement policies and procedures to address security incidents.

(ii) Implementation specification: Response and reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

(7)(i) Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) Implementation specifications:

(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.

(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.

(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected

health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.310 Physical safeguards.

45 CFR 164.310 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.310

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) Implementation specifications:

(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d)(1) Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:

(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health

information, and/or the hardware or electronic media on which it is stored.

(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.312 Technical safeguards.

45 CFR 164.312 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.312

A covered entity or business associate must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) Implementation specifications:

(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013]

§ 164.314 Organizational requirements.

45 CFR 164.314 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.314

(a)(1) Standard: Business associate contracts or other arrangements. The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) Implementation specifications (Required)—(i) Business associate contracts. The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b)(1) Standard: Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

(2) Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—

(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

(ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

(iv) Report to the group health plan any security incident of which it becomes aware.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5694, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§ 164.316 Policies and procedures and documentation requirements.

45 CFR 164.316 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.316

A covered entity or business associate must, in accordance with § 164.306:

(a) Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b)(1) Standard: Documentation. (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) Implementation specifications:

(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

[68 FR 8376, Feb. 20, 2003, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.318 Compliance dates for the initial implementation of the security standards.

45 CFR 164.318 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.318

(a) Health plan. (1) A health plan that is not a small health plan must comply with the applicable requirements of this subpart no later than April 20, 2005.

(2) A small health plan must comply with the applicable requirements of this subpart no later than April 20, 2006.

(b) Health care clearinghouse. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 20, 2005.

(c) Health care provider. A covered health care provider must comply with the applicable requirements of this subpart no later than April 20, 2005.

§ 164.400 Applicability.

45 CFR 164.400 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.400

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

§ 164.402 Definitions.

45 CFR 164.402 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.402

As used in this subpart, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E

of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.

[78 FR 5695, Jan. 25, 2013]

§ 164.404 Notification to individuals.

45 CFR 164.404 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.404

(a) Standard—(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification—(1) Elements. The notification required by paragraph (a) of this section

shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) Plain language requirement. The notification required by paragraph (a) of this section shall be written in plain language.

(d) Implementation specifications: Methods of individual notification. The notification required by paragraph (a) of this section shall be provided in the following form:

(1) Written notice. (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E), written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

(2) Substitute notice. In the case in which there is insufficient or out-of-date contact information that precludes written notification to the individual under paragraph (d)(1)(i) of this section, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

(i) In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

(ii) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall:

(A) Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the covered entity involved, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

(B) Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.

(3) Additional notice in urgent situations. In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

§ 164.406 Notification to the media.

45 CFR 164.406 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.406

(a) Standard. For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification. The notification required by paragraph (a) of this section shall meet the requirements of § 164.404(c).

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.408 Notification to the Secretary.

45 CFR 164.408 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.408

(a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a)(2), notify the Secretary.

(b) Implementation specifications: Breaches involving 500 or more individuals. For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in § 164.412, provide the notification required by paragraph (a) of this section contemporaneously with the notice required by § 164.404(a) and in the manner specified on the HHS Web site.

(c) Implementation specifications: Breaches involving less than 500 individuals. For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.410 Notification by a business associate.

45 CFR 164.410 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.410

(a) Standard—(1) General rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

(b) Implementation specifications: Timeliness of notification. Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) Implementation specifications: Content of notification. (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to

include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

[74 FR 42767, Aug. 24, 2009, as amended at 78 FR 5695, Jan. 25, 2013]

§ 164.412 Law enforcement delay.

45 CFR 164.412 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.412

If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall:

(a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

(b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

§ 164.414 Administrative requirements and burden of proof.

45 CFR 164.414 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.414

(a) Administrative requirements. A covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.

(b) Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.

§ 164.500 Applicability.

45 CFR 164.500 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.500

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(b) Health care clearinghouses must comply with the standards, requirements, and implementation specifications as follows:

(1) When a health care clearinghouse creates or receives protected health information as a business associate of another covered entity, the clearinghouse must comply with:

(i) Section 164.500 relating to applicability;

(ii) Section 164.501 relating to definitions;

(iii) Section 164.502 relating to uses and disclosures of protected health information, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(iv) Section 164.504 relating to the organizational requirements for covered entities;

(v) Section 164.512 relating to uses and disclosures for which individual authorization or an opportunity to agree or object is not required, except that a clearinghouse is prohibited from using or disclosing protected health information other than as permitted in the business associate contract under which it created or received the protected health information;

(vi) Section 164.532 relating to transition requirements; and

(vii) Section 164.534 relating to compliance dates for initial implementation of the privacy standards.

(2) When a health care clearinghouse creates or receives protected health information other than as a business associate of a covered entity, the clearinghouse must comply with all of the standards, requirements, and implementation specifications of this subpart.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

(d) The standards, requirements, and implementation specifications of this subpart do not apply to the Department of Defense or to any other federal agency, or non-governmental organization acting on its behalf, when providing health care to overseas foreign national beneficiaries.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5695, Jan. 25, 2013]

§ 164.501 Definitions.

45 CFR 164.501 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.501

As used in this subpart, the following terms have the following meanings:

Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

Data aggregation means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set means:

(1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered health care provider;

(ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship means a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients

with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health oversight agency means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Indirect treatment relationship means a relationship between an individual and a health care provider in which:

(1) The health care provider delivers health care to the individual based on the orders of another health care provider; and

(2) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Inmate means a person incarcerated in or otherwise confined to a correctional institution.

Marketing:

(1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Payment means:

(1) The activities undertaken by:

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of the health care provider and/or health plan.

Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: Diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53266, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 74 FR 42769, Aug. 24, 2009; 78 FR 5695, Jan. 25, 2013]

§ 164.502 Uses and disclosures of protected health information: General rules.

45 CFR 164.502 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.502

(a) Standard. A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) Covered entities: Permitted uses and disclosures. A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with any of the following:

(A) This section.

(B) Section 164.512 and, where applicable, § 164.509.

(C) Section 164.514(e), (f), or (g).

(2) Covered entities: Required disclosures. A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) Business associates: Permitted uses and disclosures. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) Business associates: Required uses and disclosures. A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) Prohibited uses and disclosures—(i) Use and disclosure of genetic information for underwriting purposes: Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(1) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(2) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(3) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(4) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

(ii) Sale of protected health information:

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(2) Sale of protected health information does not include a disclosure of protected health information:

(i) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(ii) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(iii) For treatment and payment purposes pursuant to § 164.506(a);

(iv) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(vi) To an individual, when requested under § 164.524 or § 164.528;

(vii) Required by law as permitted under § 164.512(a); and

(viii) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(iii) Reproductive health care—(A) Prohibition. Subject to paragraphs (a)(5)(iii)(B) and (C) of this section, a covered entity or business associate may not use or disclose protected health information for any of the following activities:

(1) To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

(2) To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

(3) To identify any person for any purpose described in paragraphs (a)(5)(iii)(A)(1) or (2) of this section.

(B) Rule of applicability. The prohibition at paragraph (a)(5)(iii)(A) of this section applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and the covered entity or business associate that received the request for protected health information has reasonably determined that one or more of the following conditions exists:

(1) The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.

(2) The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.

(3) The presumption at paragraph (a)(5)(iii)(C) of this section applies.

(C) Presumption. The reproductive health care provided by another person is presumed lawful under paragraph (a)(5)(iii)(B)(1) or (2) of this section unless the covered entity or business associate has any of the following:

(1) Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.

(2) Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

(D) Scope. For the purposes of this subpart, seeking, obtaining, providing, or facilitating reproductive health care includes, but is not limited to, any of the following: expressing interest in, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, administering, authorizing, providing coverage for, approving, counseling about, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same.

(b) Standard: Minimum necessary— Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(2) Minimum necessary does not apply. This requirement does not apply to:

(i) Disclosures to or requests by a health care provider for treatment;

(ii) Uses or disclosures made to the individual, as permitted under paragraph (a)(1)(i) of this section or as required by paragraph (a)(2)(i) of this section;

(iii) Uses or disclosures made pursuant to an authorization under § 164.508;

(iv) Disclosures made to the Secretary in accordance with subpart C of part 160 of this subchapter;

(v) Uses or disclosures that are required by law, as described by § 164.512(a); and

(vi) Uses or disclosures that are required for compliance with applicable requirements of this subchapter.

(c) Standard: Uses and disclosures of protected health information subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to § 164.522(a)(1) may not use or disclose the protected health information covered by the restriction in violation of such restriction, except as otherwise provided in § 164.522(a).

(d) Standard: Uses and disclosures of de-identified protected health information—(1) Uses and disclosures to create de-identified information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

(2) Uses and disclosures of de-identified information. Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:

(i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

(ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart.

(e)(1) Standard: Disclosures to business associates. (i) A covered entity may disclose protected health information to a business

associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) Implementation specification: Documentation. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) Standard: Deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter.

(2) Implementation specification: Adults and emancipated minors. If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(3)(i) Implementation specification: Unemancipated minors. If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to a health care service, if:

(A) The minor consents to such health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(B) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care service; or

(C) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

(ii) Notwithstanding the provisions of paragraph (g)(3)(i) of this section:

(A) If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis;

(B) If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, a covered entity may not disclose, or provide access in accordance with § 164.524 to, protected health information about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and

(C) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative under paragraphs (g)(3)(i)(A), (B), or (C) of this section and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access under § 164.524 to a parent, guardian, or other person acting in loco parentis, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

(4) Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.

(5) Implementation specification: Abuse, neglect, endangerment situations. Notwithstanding a State law or any requirement of this paragraph to the contrary, a covered entity may elect not to treat a person as the personal representative, provided that the conditions at paragraphs (g)(5)(i) and (ii) of this section are met:

(i) Paragraphs (g)(5)(i)(A) and (B) of this section both apply.

(A) The covered entity has a reasonable belief that any of the following is true:

(1) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person.

(2) Treating such person as the personal representative could endanger the individual.

(B) The covered entity, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

(ii) The covered entity does not have a reasonable belief under paragraph (g)(5)(i)(A) of this section if the basis for their belief is the provision or facilitation of reproductive health care by such person for and at the request of the individual.

(h) Standard: Confidential communications. A covered health care provider or health plan must comply with the applicable requirements of § 164.522(b) in communicating protected health information.

(i) Standard: Uses and disclosures consistent with notice. A covered entity that is required by § 164.520 to have a notice may not use or disclose protected health information in a manner inconsistent with such notice. A covered entity that is required by § 164.520(b)(1)(iii) to include a specific statement in its notice if it intends to engage in an activity listed in § 164.520(b)(1)(iii)(A)-(C), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

(j) Standard: Disclosures by whistleblowers and workforce member crime victims—(1) Disclosures by whistleblowers. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate discloses protected health information, provided that:

(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

(ii) The disclosure is to:

(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or

(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

(2) Disclosures by workforce members who are victims of a crime. A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce who is the victim of a criminal act discloses protected health information to a law enforcement official, provided that:

(i) The protected health information disclosed is about the suspected perpetrator of the criminal act; and

(ii) The protected health information disclosed is limited to the information listed in § 164.512(f)(2)(i).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 78 FR 5696, Jan. 25, 2013; 89 FR 33063, Apr. 26, 2024]

§ 164.504 Uses and disclosures: Organizational requirements.

45 CFR 164.504 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.504

(a) Definitions. As used in this section:

Plan administration functions means administration functions performed by the plan sponsor of a group health plan on behalf of the group health plan and excludes functions performed by the plan sponsor in connection with any other benefit or benefit plan of the plan sponsor.

Summary health information means information, that may be individually identifiable health information, and:

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at § 164.514(b)(2)(i) has been deleted, except that the geographic information described in § 164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

(b)-(d) [Reserved]

(e)(1) Standard: Business associate contracts. (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) Implementation specifications: Business associate contracts. A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) Implementation specifications: Other arrangements. (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with §§ 164.514(e)(4) and 164.314(a)(1), if applicable.

(4) Implementation specifications: Other requirements for contracts and other arrangements. (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) Implementation specifications: Business associate contracts with subcontractors. The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f)(1) Standard: Requirements for group health plans. (i) Except as provided under paragraph (f)(1)(ii) or (iii) of this section or as otherwise authorized under § 164.508, a group health plan, in order to disclose protected health information to the plan sponsor or to provide for or permit the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO with respect to the group health plan, must ensure that the plan documents restrict uses and disclosures of such information by the plan sponsor consistent with the requirements of this subpart.

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

(A) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or

(B) Modifying, amending, or terminating the group health plan.

(iii) The group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose to the plan sponsor information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) Implementation specifications: Requirements for plan documents. The plan documents of the group health plan must be amended to incorporate provisions to:

(i) Establish the permitted and required uses and disclosures of such information by the plan sponsor, provided that such permitted and required uses and disclosures may not be inconsistent with this subpart.

(ii) Provide that the group health plan will disclose protected health information to the plan sponsor only upon receipt of a certification by the plan sponsor that the plan documents have been amended to incorporate the following provisions and that the plan sponsor agrees to:

(A) Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

(C) Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;

(D) Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary for purposes of determining compliance by the group health plan with this subpart;

(I) If feasible, return or destroy all protected health information received from the group health plan that the sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(J) Ensure that the adequate separation required in paragraph (f)(2)(iii) of this section is established.

(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;

(B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and

(C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph.

(3) Implementation specifications: Uses and disclosures. A group health plan may:

(i) Disclose protected health information to a plan sponsor to carry out plan administration functions that the plan sponsor performs only consistent with the provisions of paragraph (f)(2) of this section;

(ii) Not permit a health insurance issuer or HMO with respect to the group health plan to disclose protected health information to the plan sponsor except as permitted by this paragraph;

(iii) Not disclose and may not permit a health insurance issuer or HMO to disclose protected health information to a plan sponsor as otherwise permitted by this paragraph unless a statement required by § 164.520(b)(1)(iii)(C) is included in the appropriate notice; and (iv) Not disclose protected health information to the plan sponsor for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.

(g) Standard: Requirements for a covered entity with multiple covered functions. (1) A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care

clearinghouse, must comply with the standards, requirements, and implementation specifications of this subpart, as applicable to the health plan, health care provider, or health care clearinghouse covered functions performed.

(2) A covered entity that performs multiple covered functions may use or disclose the protected health information of individuals who receive the covered entity's health plan or health care provider services, but not both, only for purposes related to the appropriate function being performed.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53267, Aug. 14, 2002; 68 FR 8381, Feb. 20, 2003; 78 FR 5697, Jan. 25, 2013]

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

45 CFR 164.506 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.506

(a) Standard: Permitted uses and disclosures. Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

(b) Standard: Consent for uses and disclosures permitted. (1) A covered entity may obtain consent of the individual to use or disclose protected health information to carry out treatment, payment, or health care operations.

(2) Consent, under paragraph (b) of this section, shall not be effective to permit a use or disclosure of protected health information when an authorization, under § 164.508, is required or when another condition must be met for such use or disclosure to be permissible under this subpart.

(c) Implementation specifications: Treatment, payment, or health care operations. (1) A covered entity may use or disclose protected health information for its own treatment, payment, or health care operations.

(2) A covered entity may disclose protected health information for treatment activities of a health care provider.

(3) A covered entity may disclose protected health information to another covered entity or a health care provider for the payment activities of the entity that receives the information.

(4) A covered entity may disclose protected health information to another covered entity for health care operations activities of the entity that receives the information, if each entity either has or had a relationship with the individual who is the subject of the protected health information being requested, the protected health information pertains to such relationship, and the disclosure is:

(i) For a purpose listed in paragraph (1) or (2) of the definition of health care operations; or

(ii) For the purpose of health care fraud and abuse detection or compliance.

(5) A covered entity that participates in an organized health care arrangement may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5698, Jan. 25, 2013]

§ 164.508 Uses and disclosures for which an authorization is required.

45 CFR 164.508 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.508

(a) Standard: Authorizations for uses and disclosures—(1) Authorization required: General rule. Except as otherwise permitted or required by this subchapter, a covered entity may not use or disclose protected health information without an authorization that is valid under this section. When a covered entity obtains or receives a valid authorization for its use or disclosure of protected health information, such use or disclosure must be consistent with such authorization.

(2) Authorization required: Psychotherapy notes. Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

(i) To carry out the following treatment, payment, or health care operations:

(A) Use by the originator of the psychotherapy notes for treatment;

(B) Use or disclosure by the covered entity for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(C) Use or disclosure by the covered entity to defend itself in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is required by § 164.502(a)(2)(ii) or permitted by § 164.512(a); § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; § 164.512(g)(1); or § 164.512(j)(1)(i).

(3) Authorization required: Marketing. (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of:

(A) A face-to-face communication made by a covered entity to an individual; or

(B) A promotional gift of nominal value provided by the covered entity.

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) Authorization required: Sale of protected health information. (i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) Implementation specifications: General requirements—(1) Valid authorizations. (i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

(ii) A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section.

(2) Defective authorizations. An authorization is not valid, if the document submitted has any of the following defects:

(i) The expiration date has passed or the expiration event is known by the covered entity to have occurred;

(ii) The authorization has not been filled out completely, with respect to an element described by paragraph (c) of this section, if applicable;

(iii) The authorization is known by the covered entity to have been revoked;

(iv) The authorization violates paragraph (b)(3) or (4) of this section, if applicable;

(v) Any material information in the authorization is known by the covered entity to be false.

(3) Compound authorizations. An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research.

Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

(4) Prohibition on conditioning of authorizations. A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

(i) A covered health care provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research under this section;

(ii) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

(A) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

(B) The authorization is not for a use or disclosure of psychotherapy notes under paragraph (a)(2) of this section; and

(iii) A covered entity may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to such third party.

(5) Revocation of authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

(i) The covered entity has taken action in reliance thereon; or

(ii) If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

(6) Documentation. A covered entity must document and retain any signed authorization under this section as required by § 164.530(j).

(c) Implementation specifications: Core elements and requirements—(1) Core elements. A valid authorization under this section must contain at least the following elements:

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement “end of the research study,” “none,” or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

(2) Required statements. In addition to the core elements, the authorization must contain statements adequate to place the individual on notice of all of the following:

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

(3) Plain language requirement. The authorization must be written in plain language.

(4) Copy to the individual. If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

[67 FR 53268, Aug. 14, 2002, as amended at 78 FR 5699, Jan. 25, 2013]

§ 164.509 Uses and disclosures for which an attestation is required.

45 CFR 164.509 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.509

(a) Standard: Attestations for certain uses and disclosures of protected health information to persons other than covered entities or business associates. (1) A covered entity or business associate may not use or disclose protected health information potentially related to reproductive health care for purposes specified in § 164.512(d), (e), (f), or (g)(1), without obtaining an attestation that is valid under paragraph (b)(1) of this section from the person requesting the use or disclosure and complying with all applicable conditions of this part.

(2) A covered entity or business associate that uses or discloses protected health information potentially related to reproductive health care for purposes specified in § 164.512(d), (e), (f), or (g)(1), in reliance on an attestation that is defective under paragraph (b)(2) of this section, is not in compliance with this section.

(b) Implementation specifications: General requirements—(1) Valid attestations. (i) A valid attestation is a document that meets the

requirements of paragraph (c)(1) of this section.

(ii) A valid attestation verifies that the use or disclosure is not otherwise prohibited by § 164.502(a)(5)(iii).

(iii) A valid attestation may be electronic, provided that it meets the requirements in paragraph (c)(1) of this section, as applicable.

(2) Defective attestations. An attestation is not valid if the document submitted has any of the following defects:

(i) The attestation lacks an element or statement required by paragraph (c) of this section.

(ii) The attestation contains an element or statement not required by paragraph (c) of this section

(iii) The attestation violates paragraph (b)(3) of this section.

(iv) The covered entity or business associate has actual knowledge that material information in the attestation is false.

(v) A reasonable covered entity or business associate in the same position would not believe that the attestation is true with respect to the requirement at paragraph (c)(1)(iv) of this section.

(3) Compound attestation. An attestation may not be combined with any other document except where such other document is needed to satisfy the requirements at paragraph (c)(iv) of this section or at § 164.502(a)(5)(iii)(C), as applicable.

(c) Implementation specifications: Content requirements and other obligations—(1) Required elements. A valid attestation under this section must contain the following elements:

(i) A description of the information requested that identifies the information in a specific fashion, including one of the following:

(A) The name of any individual(s) whose protected health information is sought, if practicable.

(B) If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought.

(ii) The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure.

(iv) A clear statement that the use or disclosure is not for a purpose prohibited under § 164.502(a)(5)(iii).

(v) A statement that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.

(vi) Signature of the person requesting the protected health information, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.

(2) Plain language requirement. The attestation must be written in plain language.

(d) Material misrepresentations. If, during the course of using or disclosing protected health information in reasonable reliance on a facially valid attestation, a covered entity or business associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or disclosure for a purpose prohibited under § 164.502(a)(5)(iii), the covered entity or business associate must cease such use or disclosure.

[89 FR 33063, Apr. 26, 2024]

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

45 CFR 164.510 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.510

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

(a) Standard: Use and disclosure for facility directories—(1) Permitted uses and disclosure. Except when an objection is expressed in accordance with paragraphs (a)(2) or (3) of this section, a covered health care provider may:

(i) Use the following protected health information to maintain a directory of individuals in its facility:

(A) The individual's name;

(B) The individual's location in the covered health care provider's facility;

(C) The individual's condition described in general terms that does not communicate specific medical information about the individual; and

(D) The individual's religious affiliation; and

(ii) Use or disclose for directory purposes such information:

(A) To members of the clergy; or

(B) Except for religious affiliation, to other persons who ask for the individual by name.

(2) Opportunity to object. A covered health care provider must inform an individual of the protected health information that it may include in a directory and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section.

(3) Emergency circumstances. (i) If the opportunity to object to uses or disclosures required by paragraph (a)(2) of this section cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a covered health care provider may use or disclose some or all of the protected health information permitted by paragraph (a)(1) of this section for the facility's directory, if such disclosure is:

(A) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and

(B) In the individual's best interest as determined by the covered health care provider, in the exercise of professional judgment.

(ii) The covered health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as required by paragraph (a)(2) of this section when it becomes practicable to do so.

(b) Standard: Uses and disclosures for involvement in the individual's care and notification purposes—(1) Permitted uses and disclosures. (i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

(2) Uses and disclosures with the individual present. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (b)(1) of this section and has the capacity to make health care decisions, the covered entity may use or disclose the protected health information if it:

(i) Obtains the individual's agreement;

(ii) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) Limited uses and disclosures when the individual is not present. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of protected health information.

(4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) Uses and disclosures when the individual is deceased. If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013]

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

45 CFR 164.512 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.512

Except as provided by § 164.502(a)(5)(iii), a covered entity may use or disclose protected health information without the written authorization of the individual, as described in § 164.508, or the opportunity for the individual to agree or object as described in § 164.510, in the situations covered by this section, subject to the applicable requirements of this section and § 164.509. When the covered entity is required by this section to inform the individual of, or when the individual may agree to, a use or disclosure permitted by this section, the covered entity's information and the individual's agreement may be given verbally.

(a) Standard: Uses and disclosures required by law. (1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

(2) A covered entity must meet the requirements described in paragraph (c), (e), or (f) of this section for uses or disclosures required by law.

(b) Standard: Uses and disclosures for public health activities—(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

(i) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(ii) A public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(iii) A person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

(A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;

(B) To track FDA-regulated products;

(C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or

(D) To conduct post marketing surveillance;

(iv) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; or

(v) An employer, about an individual who is a member of the workforce of the employer, if:

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

(1) To conduct an evaluation relating to medical surveillance of the workplace; or

(2) To evaluate whether the individual has a work-related illness or injury;

(B) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

(C) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

(D) The covered health care provider provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:

(1) By giving a copy of the notice to the individual at the time the health care is provided; or

(2) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(1) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

(2) Permitted uses. If the covered entity also is a public health authority, the covered entity is permitted to use protected health information in all cases in which it is permitted to disclose such information for public health activities under paragraph (b)(1) of this section.

(c) Standard: Disclosures about victims of abuse, neglect, or domestic violence—(1) Permitted disclosures. Except for reports of child abuse or neglect permitted by paragraph (b)(1)(ii) of this section, a covered entity may disclose protected health information about an individual whom the covered entity reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

(i) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;

(ii) If the individual agrees to the disclosure; or

(iii) To the extent the disclosure is expressly authorized by statute or regulation and:

(A) The covered entity, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

(B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

(2) Informing the individual. A covered entity that makes a disclosure permitted by paragraph (c)(1) of this section must promptly inform the individual that such a report has been or will be made, except if:

(i) The covered entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(ii) The covered entity would be informing a personal representative, and the covered entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(3) Rule of construction. Nothing in this section shall be construed to permit disclosures prohibited by § 164.502(a)(5)(iii) when the sole basis of the report of abuse, neglect, or domestic violence is the provision or facilitation of reproductive health care.

(d) Standard: Uses and disclosures for health oversight activities—(1) Permitted disclosures. A covered entity may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:

(i) The health care system;

(ii) Government benefit programs for which health information is relevant to beneficiary eligibility;

(iii) Entities subject to government regulatory programs for which health information is necessary for determining compliance with

program standards; or

(iv) Entities subject to civil rights laws for which health information is necessary for determining compliance.

(2) Exception to health oversight activities. For the purpose of the disclosures permitted by paragraph (d)(1) of this section, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(i) The receipt of health care;

(ii) A claim for public benefits related to health; or

(iii) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

(3) Joint activities or investigations. Nothwithstanding paragraph (d)(2) of this section, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of paragraph (d) of this section.

(4) Permitted uses. If a covered entity also is a health oversight agency, the covered entity may use protected health information for health oversight activities as permitted by paragraph (d) of this section.

(e) Standard: Disclosures for judicial and administrative proceedings—(1) Permitted disclosures. A covered entity may disclose protected health information in the course of any judicial or administrative proceeding:

(i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

(ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

(B) The notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and

(C) The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:

(1) No objections were filed; or

(2) All objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(iv) For the purposes of paragraph (e)(1)(ii)(B) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information, if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

(A) The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

(B) The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

(v) For purposes of paragraph (e)(1) of this section, a qualified protective order means, with respect to protected health information requested under paragraph (e)(1)(ii) of this section, an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

(A) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and

(B) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

(2) Other uses and disclosures under this section. The provisions of this paragraph do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of protected health information.

(f) Standard: Disclosures for law enforcement purposes. A covered entity may disclose protected health information for a law enforcement purpose to a law enforcement official if the conditions in paragraphs (f)(1) through (f)(6) of this section are met, as applicable.

(1) Permitted disclosures: Pursuant to process and as otherwise required by law. A covered entity may disclose protected health information:

(i) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for laws subject to paragraph (b)(1)(ii) or (c)(1)(i) of this section; or

(ii) In compliance with and as limited by the relevant requirements of:

(A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(B) A grand jury subpoena; or

(C) An administrative request for which response is required by law, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

(1) The information sought is relevant and material to a legitimate law enforcement inquiry;

(2) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

(3) De-identified information could not reasonably be used.

(2) Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(i) The covered entity may disclose only the following information:

(A) Name and address;

(B) Date and place of birth;

(C) Social security number;

(D) ABO blood type and rh factor;

(E) Type of injury;

(F) Date and time of treatment;

(G) Date and time of death, if applicable; and

(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(3) Permitted disclosure: Victims of a crime. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to paragraph (b) or (c) of this section, if:

(i) The individual agrees to the disclosure; or

(ii) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

(A) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;

(B) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and

(C) The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

(4) Permitted disclosure: Decedents. A covered entity may disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the covered entity has a suspicion that such death may have resulted from criminal conduct.

(5) Permitted disclosure: Crime on premises. A covered entity may disclose to a law enforcement official protected health information that the covered entity believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the covered entity.

(6) Permitted disclosure: Reporting crime in emergencies. (i) A covered health care provider providing emergency health care in response to a medical emergency, other than such emergency on the premises of the covered health care provider, may disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(A) The commission and nature of a crime;

(B) The location of such crime or of the victim(s) of such crime; and

(C) The identity, description, and location of the perpetrator of such crime.

(ii) If a covered health care provider believes that the medical emergency described in paragraph (f)(6)(i) of this section is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, paragraph (f)(6)(i) of this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to paragraph (c) of this section.

(g) Standard: Uses and disclosures about decedents—(1) Coroners and medical examiners. A covered entity may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

(2) Funeral directors. A covered entity may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

(h) Standard: Uses and disclosures for cadaveric organ, eye or tissue donation purposes. A covered entity may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

(i) Standard: Uses and disclosures for research purposes—(1) Permitted uses and disclosures. A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either:

(A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or

(B) A privacy board that:

(1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;

(2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and

(3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that:

(A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;

(B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and

(C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher:

(A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;

(B) Documentation, at the request of the covered entity, of the death of such individuals; and

(C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

(2) Documentation of waiver approval. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

(i) Identification and date of action. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;

(ii) Waiver criteria. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:

(A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements;

(1) An adequate plan to protect the identifiers from improper use and disclosure;

(2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and

(3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

(B) The research could not practicably be conducted without the waiver or alteration; and

(C) The research could not practicably be conducted without access to and use of the protected health information.

(iii) Protected health information needed. A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

(iv) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:

(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;

(C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and

(v) Required signature. The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

(j) Standard: Uses and disclosures to avert a serious threat to health or safety—(1) Permitted disclosures. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure:

(i)(A) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

(B) Is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

(ii) Is necessary for law enforcement authorities to identify or apprehend an individual:

(A) Because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim; or

(B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody, as those terms are defined in § 164.501.

(2) Use or disclosure not permitted. A use or disclosure pursuant to paragraph (j)(1)(ii)(A) of this section may not be made if the information described in paragraph (j)(1)(ii)(A) of this section is learned by the covered entity:

(i) In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure under paragraph (j)(1)(ii)(A) of this section, or counseling or therapy; or

(ii) Through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy described in paragraph (j)(2)(i) of this section.

(3) Limit on information that may be disclosed. A disclosure made pursuant to paragraph (j)(1)(ii)(A) of this section shall contain only the statement described in paragraph (j)(1)(ii)(A) of this section and the protected health information described in paragraph (f)(2)(i) of this section.

(4) Presumption of good faith belief. A covered entity that uses or discloses protected health information pursuant to paragraph (j)(1) of this section is presumed to have acted in good faith with regard to a belief described in paragraph (j)(1)(i) or (ii) of this section, if the belief is based upon the covered entity's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

(k) Standard: Uses and disclosures for specialized government functions—(1) Military and veterans activities—(i) Armed Forces personnel. A covered entity may use and disclose the protected health information of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the Federal Register the following information:

(A) Appropriate military command authorities; and

(B) The purposes for which the protected health information may be used or disclosed.

(ii) Separation or discharge from military service. A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of

Veterans Affairs.

(iii) Veterans. A covered entity that is a component of the Department of Veterans Affairs may use and disclose protected health information to components of the Department that determine eligibility for or entitlement to, or that provide, benefits under the laws administered by the Secretary of Veterans Affairs.

(iv) Foreign military personnel. A covered entity may use and disclose the protected health information of individuals who are foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the Federal Register pursuant to paragraph (k)(1)(i) of this section.

(2) National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333).

(3) Protective services for the President and others. A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

(4) Medical suitability determinations. A covered entity that is a component of the Department of State may use protected health information to make medical suitability determinations and may disclose whether or not the individual was determined to be medically suitable to the officials in the Department of State who need access to such information for the following purposes:

(i) For the purpose of a required security clearance conducted pursuant to Executive Orders 10450 and 12968;

(ii) As necessary to determine worldwide availability or availability for mandatory service abroad under sections 101(a)(4) and 504 of the Foreign Service Act; or

(iii) For a family to accompany a Foreign Service member abroad, consistent with section 101(b)(5) and 904 of the Foreign Service Act.

(5) Correctional institutions and other law enforcement custodial situations—(i) Permitted disclosures. A covered entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

(A) The provision of health care to such individuals;

(B) The health and safety of such individual or other inmates;

(C) The health and safety of the officers or employees of or others at the correctional institution;

(D) The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

(E) Law enforcement on the premises of the correctional institution; or

(F) The administration and maintenance of the safety, security, and good order of the correctional institution.

(ii) Permitted uses. A covered entity that is a correctional institution may use protected health information of individuals who are inmates for any purpose for which such protected health information may be disclosed.

(iii) No application after release. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

(6) Covered entities that are government programs providing public benefits. (i) A health plan that is a government program providing public benefits may disclose protected health information relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing of eligibility or enrollment information among such government agencies or the maintenance of such information in a single or combined data system accessible to all such government agencies is required or expressly authorized by statute or regulation.

(ii) A covered entity that is a government agency administering a government program providing public benefits may disclose protected health information relating to the program to another covered entity that is a government agency administering a government program providing public benefits if the programs serve the same or similar populations and the disclosure of protected health information is necessary to coordinate the covered functions of such programs or to improve administration and management relating to the covered functions of such programs.

(7) National Instant Criminal Background Check System. A covered entity may use or disclose protected health information for purposes of reporting to the National Instant Criminal Background Check System the identity of an individual who is prohibited from possessing a firearm under 18 U.S.C. 922(g)(4), provided the covered entity:

(i) Is a State agency or other entity that is, or contains an entity that is:

(A) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; or

(B) A court, board, commission, or other lawful authority that makes the commitment or adjudication that causes an individual to become subject to 18 U.S.C. 922(g)(4); and

(ii) Discloses the information only to:

(A) The National Instant Criminal Background Check System; or

(B) An entity designated by the State to report, or which collects information for purposes of reporting, on behalf of the State, to the National Instant Criminal Background Check System; and

(iii)(A) Discloses only the limited demographic and certain other information needed for purposes of reporting to the National Instant Criminal Background Check System; and

(B) Does not disclose diagnostic or clinical information for such purposes.

(l) Standard: Disclosures for workers' compensation. A covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5699, Jan. 25, 2013; 78 FR 34266, June 7, 2013; 81 FR 395, Jan. 6, 2016; 89 FR 33064, Apr. 26, 2024]

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

45 CFR 164.514 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.514

(a) Standard: De-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

(b) Implementation specifications: Requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and

methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other

information to identify an individual who is a subject of the information.

(c) Implementation specifications: Re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

(d)(1) Standard: minimum necessary requirements. In order to comply with § 164.502(b) and this section, a covered entity must meet the requirements of paragraphs (d)(2) through (d)(5) of this section with respect to a request for, or the use and disclosure of, protected health information.

(2) Implementation specifications: Minimum necessary uses of protected health information. (i) A covered entity must identify:

(A) Those persons or classes of persons, as appropriate, in its workforce who need access to protected health information to carry out their duties; and

(B) For each such person or class of persons, the category or categories of protected health information to which access is needed and any conditions appropriate to such access.

(ii) A covered entity must make reasonable efforts to limit the access of such persons or classes identified in paragraph (d)(2)(i)(A) of this section to protected health information consistent with paragraph (d)(2)(i)(B) of this section.

(3) Implementation specification: Minimum necessary disclosures of protected health information. (i) For any type of disclosure that it makes on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

(ii) For all other disclosures, a covered entity must:

(A) Develop criteria designed to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(iii) A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(A) Making disclosures to public officials that are permitted under § 164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

(B) The information is requested by another covered entity;

(C) The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

(D) Documentation or representations that comply with the applicable requirements of § 164.512(i) have been provided by a person requesting the information for research purposes.

(4) Implementation specifications: Minimum necessary requests for protected health information. (i) A covered entity must limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request

is made, when requesting such information from other covered entities.

(ii) For a request that is made on a routine and recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that limit the protected health information requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

(iii) For all other requests, a covered entity must:

(A) Develop criteria designed to limit the request for protected health information to the information reasonably necessary to accomplish the purpose for which the request is made; and

(B) Review requests for disclosure on an individual basis in accordance with such criteria.

(5) Implementation specification: Other content requirement. For all uses, disclosures, or requests to which the requirements in paragraph (d) of this section apply, a covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

(e)(1) Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section.

(2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names;

(ii) Postal address information, other than town or city, State, and zip code;

(iii) Telephone numbers;

(iv) Fax numbers;

(v) Electronic mail addresses;

(vi) Social security numbers;

(vii) Medical record numbers;

(viii) Health plan beneficiary numbers;

(ix) Account numbers;

(x) Certificate/license numbers;

(xi) Vehicle identifiers and serial numbers, including license plate numbers;

(xii) Device identifiers and serial numbers;

(xiii) Web Universal Resource Locators (URLs);

(xiv) Internet Protocol (IP) address numbers;

(xv) Biometric identifiers, including finger and voice prints; and

(xvi) Full face photographic images and any comparable images.

(3) Implementation specification: Permitted purposes for uses and disclosures. (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations.

(ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity.

(4) Implementation specifications: Data use agreement—(i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes.

(ii) Contents. A data use agreement between the covered entity and the limited data set recipient must:

(A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity;

(B) Establish who is permitted to use or receive the limited data set; and

(C) Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

(iii) Compliance. (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

(1) Discontinued disclosure of protected health information to the recipient; and

(2) Reported the problem to the Secretary.

(B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.

(f) Fundraising communications—(1) Standard: Uses and disclosures for fundraising. Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) Implementation specifications: Fundraising requirements. (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(2)(ii) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) Standard: Uses and disclosures for underwriting and related purposes. If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

(h)(1) Standard: Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:

(i) Except with respect to disclosures under § 164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: Verification—(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in § 164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by § 164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with § 164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with § 164.510 or acts on a good faith belief in making a disclosure in accordance with § 164.512(j).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53270, Aug. 14, 2002; 78 FR 5700, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§ 164.520 Notice of privacy practices for protected health information.

45 CFR 164.520 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.520

(a) Standard: Notice of privacy practices—(1) Right to notice. Except as provided by paragraph (a)(3) or (4) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) Notice requirements for covered entities creating or maintaining records subject to 42 U.S.C. 290dd-2. As provided in 42 CFR 2.22, an individual who is the subject of records protected under 42 CFR part 2 has a right to adequate notice of the uses and disclosures of such records, and of the individual's rights and the covered entity's legal duties with respect to such records.

(3) Exception for group health plans. (i) An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

(ii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives protected health information in addition to summary health information as defined in § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of paragraph (c)(1) of this section do not apply to such group health plan.

(iii) A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive protected health information other than summary health information as defined in § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

(4) Exception for inmates. An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution that is a covered entity.

(b) Implementation specifications: Content of notice—(1) Required elements. The covered entity, including any covered entity receiving or maintaining records subject to 42 U.S.C. 290dd-2, must provide a notice that is written in plain language and that contains the elements required by this paragraph.

(i) Header. The notice must contain the following statement as a header or otherwise prominently displayed:

“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

(ii) Uses and disclosures. The notice must contain:

(A) A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by this subpart to make for each of the following purposes: treatment, payment, and health care operations.

(B) A description of each of the other purposes for which the covered entity is permitted or required by this subpart to use or disclose protected health information without the individual's written authorization.

(C) If a use or disclosure for any purpose described in paragraphs (b)(1)(ii)(A) or (B) of this section is prohibited or materially limited by other applicable law, such as 42 CFR part 2, the description of such use or disclosure must reflect the more stringent law as defined in § 160.202 of this subchapter.

(D) For each purpose described in paragraph (b)(1)(ii)(A) or (B) of this section, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by this subpart and other applicable law, such as 42 CFR part 2.

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)-(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(F) A description, including at least one example, of the types of uses and disclosures prohibited under § 164.502(a)(5)(iii) in sufficient detail for an individual to understand the prohibition.

(G) A description, including at least one example, of the types of uses and disclosures for which an attestation is required under § 164.509.

(H) A statement adequate to put the individual on notice of the potential for information disclosed pursuant to this subpart to be subject to redisclosure by the recipient and no longer protected by this subpart

(iii) Separate statements for certain uses or disclosures. If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) or (B) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the

individual has a right to opt out of receiving such communications;

(B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan;

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes;

(D) Substance use disorder treatment records received from programs subject to 42 CFR part 2, or testimony relaying the content of such records, shall not be used or disclosed in civil, criminal, administrative, or legislative proceedings against the individual unless based on written consent, or a court order after notice and an opportunity to be heard is provided to the individual or the holder of the record, as provided in 42 CFR part 2. A court order authorizing use or disclosure must be accompanied by a subpoena or other legal requirement compelling disclosure before the requested record is used or disclosed; or

(E) If a covered entity that creates or maintains records subject to 42 CFR part 2 intends to use or disclose such records for fundraising for the benefit of the covered entity, the individual must first be provided with a clear and conspicuous opportunity to elect not to receive any fundraising communications.

(iv) Individual rights. The notice must contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

(B) The right to receive confidential communications of protected health information as provided by § 164.522(b), as applicable;

(C) The right to inspect and copy protected health information as provided by § 164.524;

(D) The right to amend protected health information as provided by § 164.526;

(E) The right to receive an accounting of disclosures of protected health information as provided by § 164.528; and

(F) The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph (c)(3) of this section, to obtain a paper copy of the notice from the covered entity upon request.

(v) Covered entity's duties. The notice must contain:

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices, and to notify affected individuals following a breach of unsecured protected health information;

(B) A statement that the covered entity is required to abide by the terms of the notice currently in effect; and

(C) For the covered entity to apply a change in a privacy practice that is described in the notice to protected health information that the covered entity created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all protected health information that it maintains. The statement must also describe how it will provide individuals with a revised notice.

(vi) Complaints. The notice must contain a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

(vii) Contact. The notice must contain the name, or title, and telephone number of a person or office to contact for further information as required by § 164.530(a)(1)(ii).

(viii) Effective date. The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

(2) Optional elements. (i) In addition to the information required by paragraph (b)(1) of this section, if a covered entity elects to limit the uses or disclosures that it is permitted to make under this subpart, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by § 164.512(j)(1)(i).

(ii) For the covered entity to apply a change in its more limited uses and disclosures to protected health information created or received prior to issuing a revised notice, in accordance with § 164.530(i)(2)(ii), the notice must include the statements required by paragraph (b)(1)(v)(C) of this section.

(3) Revisions to the notice. The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

(c) Implementation specifications: Provision of notice. A covered entity must make the notice required by this section available on request to any person and to individuals as specified in paragraphs (c)(1) through (c)(3) of this section, as applicable.

(1) Specific requirements for health plans. (i) A health plan must provide the notice:

(A) No later than the compliance date for the health plan, to individuals then covered by the plan;

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

(ii) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

(iii) The health plan satisfies the requirements of paragraph (c)(1) of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

(iv) If a health plan has more than one notice, it satisfies the requirements of paragraph (c)(1) of this section by providing the notice that is relevant to the individual or other person requesting the notice.

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

(2) Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must:

(i) Provide the notice:

(A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the

compliance date for the covered health care provider; or

(B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation.

(ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained;

(iii) If the covered health care provider maintains a physical service delivery site:

(A) Have the notice available at the service delivery site for individuals to request to take with them; and

(B) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

(iv) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (c)(2)(iii) of this section, if applicable.

(3) Specific requirements for electronic notice. (i) A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

(ii) A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of paragraph (c) of this section when timely made in accordance with paragraph (c)(1) or (2) of this section.

(iii) For purposes of paragraph (c)(2)(i) of this section, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements in paragraph (c)(2)(ii) of this section apply to electronic notice.

(iv) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

(d) Implementation specifications: Joint notice by separate covered entities. Covered entities that participate in organized health care arrangements may comply with this section by a joint notice, provided that:

(1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement;

(2) The joint notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one covered entity; and

(i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

(ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

(iii) If applicable, states that the covered entities participating in the organized health care arrangement will share protected health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

(3) The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint notice to an individual by any one of the

covered entities included in the joint notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint notice.

(4) The permission in paragraph (d) of this section for covered entities that participate in an organized health care arrangement to issue a joint notice may not be construed to remove any obligations or duties of entities creating or maintaining records subject to 42 U.S.C. 290dd-2, or to remove any rights of patients who are the subjects of such records.

(e) Implementation specifications: Documentation. A covered entity must document compliance with the notice requirements, as required by § 164.530(j), by retaining copies of the notices issued by the covered entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment, in accordance with paragraph (c)(2)(ii) of this section.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013; 89 FR 33064, Apr. 26, 2024]

§ 164.522 Rights to request privacy protection for protected health information.

45 CFR 164.522 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.522

(a)(1) Standard: Right of an individual to request restriction of uses and disclosures. (i) A covered entity must permit an individual to request that the covered entity restrict:

(A) Uses or disclosures of protected health information about the individual to carry out treatment, payment, or health care operations; and

(B) Disclosures permitted under § 164.510(b).

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

(iii) A covered entity that agrees to a restriction under paragraph (a)(1)(i) of this section may not use or disclose protected health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the covered entity may use the restricted protected health information, or may disclose such information to a health care provider, to provide such treatment to the individual.

(iv) If restricted protected health information is disclosed to a health care provider for emergency treatment under paragraph (a)(1)(iii) of this section, the covered entity must request that such health care provider not further use or disclose the information.

(v) A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under § 164.502(a)(2)(ii), § 164.510(a) or § 164.512.

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) Implementation specifications: Terminating a restriction. A covered entity may terminate a restriction, if:

(i) The individual agrees to or requests the termination in writing;

(ii) The individual orally agrees to the termination and the oral agreement is documented; or

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) Implementation specification: Documentation. A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

(b)(1) Standard: Confidential communications requirements. (i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

(ii) A health plan must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual.

(2) Implementation specifications: Conditions on providing confidential communications. (i) A covered entity may require the individual to make a request for a confidential communication described in paragraph (b)(1) of this section in writing.

(ii) A covered entity may condition the provision of a reasonable accommodation on:

(A) When appropriate, information as to how payment, if any, will be handled; and

(B) Specification of an alternative address or other method of contact.

(iii) A covered health care provider may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

(iv) A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002; 78 FR 5701, Jan. 25, 2013]

§ 164.524 Access of individuals to protected health information.

45 CFR 164.524 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.524

(a) Standard: Access to protected health information—(1) Right of access. Except as otherwise provided in paragraph (a)(2) or (a)(3) of this section, an individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set, except for:

(i) Psychotherapy notes; and

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

(2) Unreviewable grounds for denial. A covered entity may deny an individual access without providing the individual an opportunity for review, in the following circumstances.

(i) The protected health information is excepted from the right of access by paragraph (a)(1) of this section.

(ii) A covered entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of protected health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.

(iii) An individual's access to protected health information created or obtained by a covered health care provider in the course of

research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the covered health care provider has informed the individual that the right of access will be reinstated upon completion of the research.

(iv) An individual's access to protected health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(v) An individual's access may be denied if the protected health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(3) Reviewable grounds for denial. A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed, as required by paragraph (a)(4) of this section, in the following circumstances:

(i) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(ii) The protected health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(iii) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

(4) Review of a denial of access. If access is denied on a ground permitted under paragraph (a)(3) of this section, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the covered entity to act as a reviewing official and who did not participate in the original decision to deny. The covered entity must provide or deny access in accordance with the determination of the reviewing official under paragraph (d)(4) of this section.

(b) Implementation specifications: Requests for access and timely action—(1) Individual's request for access. The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set. The covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement.

(2) Timely action by the covered entity. (i) Except as provided in paragraph (b)(2)(ii) of this section, the covered entity must act on a request for access no later than 30 days after receipt of the request as follows.

(A) If the covered entity grants the request, in whole or in part, it must inform the individual of the acceptance of the request and provide the access requested, in accordance with paragraph (c) of this section.

(B) If the covered entity denies the request, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d) of this section.

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) Implementation specifications: Provision of access. If the covered entity provides an individual with access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Providing the access requested. The covered entity must provide the access requested by individuals, including inspection or obtaining a copy, or both, of the protected health information about them in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the covered entity need only produce the protected health information once in response to a request for access.

(2) Form of access requested. (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

(iii) The covered entity may provide the individual with a summary of the protected health information requested, in lieu of providing access to the protected health information or may provide an explanation of the protected health information to which access has been provided, if:

(A) The individual agrees in advance to such a summary or explanation; and

(B) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation.

(3) Time and manner of access. (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) Fees. If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

(iii) Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and

(iv) Preparing an explanation or summary of the protected health information, if agreed to by the individual as required by paragraph (c)(2)(iii) of this section.

(d) Implementation specifications: Denial of access. If the covered entity denies access, in whole or in part, to protected health information, the covered entity must comply with the following requirements.

(1) Making other information accessible. The covered entity must, to the extent possible, give the individual access to any other protected health information requested, after excluding the protected health information as to which the covered entity has a ground to deny access.

(2) Denial. The covered entity must provide a timely, written denial to the individual, in accordance with paragraph (b)(2) of this section. The denial must be in plain language and contain:

(i) The basis for the denial;

(ii) If applicable, a statement of the individual's review rights under paragraph (a)(4) of this section, including a description of how the individual may exercise such review rights; and

(iii) A description of how the individual may complain to the covered entity pursuant to the complaint procedures in § 164.530(d) or to the Secretary pursuant to the procedures in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(3) Other responsibility. If the covered entity does not maintain the protected health information that is the subject of the individual's request for access, and the covered entity knows where the requested information is maintained, the covered entity must inform the individual where to direct the request for access.

(4) Review of denial requested. If the individual has requested a review of a denial under paragraph (a)(4) of this section, the covered entity must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The covered entity must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards in paragraph (a)(3) of this section. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

(e) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The designated record sets that are subject to access by individuals; and

(2) The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 78 FR 5701, Jan. 25, 2013; 78 FR 34266, June 7, 2013; 79 FR 7316, Feb. 6, 2014]

§ 164.526 Amendment of protected health information.

45 CFR 164.526 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.526

(a) Standard: Right to amend. (1) Right to amend. An individual has the right to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

(2) Denial of amendment. A covered entity may deny an individual's request for amendment, if it determines that the protected health information or record that is the subject of the request:

(i) Was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

(ii) Is not part of the designated record set;

(iii) Would not be available for inspection under § 164.524; or

(iv) Is accurate and complete.

(b) Implementation specifications: Requests for amendment and timely action—(1) Individual's request for amendment. The covered entity must permit an individual to request that the covered entity amend the protected health information maintained in the designated record set. The covered entity may require individuals to make requests for amendment in writing and to provide a

reason to support a requested amendment, provided that it informs individuals in advance of such requirements.

(2) Timely action by the covered entity. (i) The covered entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows.

(A) If the covered entity grants the requested amendment, in whole or in part, it must take the actions required by paragraphs (c)(1) and (2) of this section.

(B) If the covered entity denies the requested amendment, in whole or in part, it must provide the individual with a written denial, in accordance with paragraph (d)(1) of this section.

(ii) If the covered entity is unable to act on the amendment within the time required by paragraph (b)(2)(i) of this section, the covered entity may extend the time for such action by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for an amendment.

(c) Implementation specifications: Accepting the amendment. If the covered entity accepts the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Making the amendment. The covered entity must make the appropriate amendment to the protected health information or record that is the subject of the request for amendment by, at a minimum, identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.

(2) Informing the individual. In accordance with paragraph (b) of this section, the covered entity must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared in accordance with paragraph (c)(3) of this section.

(3) Informing others. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to:

(i) Persons identified by the individual as having received protected health information about the individual and needing the amendment; and

(ii) Persons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

(d) Implementation specifications: Denying the amendment. If the covered entity denies the requested amendment, in whole or in part, the covered entity must comply with the following requirements.

(1) Denial. The covered entity must provide the individual with a timely, written denial, in accordance with paragraph (b)(2) of this section. The denial must use plain language and contain:

(i) The basis for the denial, in accordance with paragraph (a)(2) of this section;

(ii) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

(iii) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of the protected health information that is the subject of the amendment; and

(iv) A description of how the individual may complain to the covered entity pursuant to the complaint procedures established in §

164.530(d) or to the Secretary pursuant to the procedures established in § 160.306. The description must include the name, or title, and telephone number of the contact person or office designated in § 164.530(a)(1)(ii).

(2) Statement of disagreement. The covered entity must permit the individual to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The covered entity may reasonably limit the length of a statement of disagreement.

(3) Rebuttal statement. The covered entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the covered entity must provide a copy to the individual who submitted the statement of disagreement.

(4) Recordkeeping. The covered entity must, as appropriate, identify the record or protected health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the covered entity's denial of the request, the individual's statement of disagreement, if any, and the covered entity's rebuttal, if any, to the designated record set.

(5) Future disclosures. (i) If a statement of disagreement has been submitted by the individual, the covered entity must include the material appended in accordance with paragraph (d)(4) of this section, or, at the election of the covered entity, an accurate summary of any such information, with any subsequent disclosure of the protected health information to which the disagreement relates.

(ii) If the individual has not submitted a written statement of disagreement, the covered entity must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the protected health information only if the individual has requested such action in accordance with paragraph (d)(1)(iii) of this section.

(iii) When a subsequent disclosure described in paragraph (d)(5)(i) or (ii) of this section is made using a standard transaction under part 162 of this subchapter that does not permit the additional material to be included with the disclosure, the covered entity may separately transmit the material required by paragraph (d)(5)(i) or (ii) of this section, as applicable, to the recipient of the standard transaction.

(e) Implementation specification: Actions on notices of amendment. A covered entity that is informed by another covered entity of an amendment to an individual's protected health information, in accordance with paragraph (c)(3) of this section, must amend the protected health information in designated record sets as provided by paragraph (c)(1) of this section.

(f) Implementation specification: Documentation. A covered entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required by § 164.530(j).

§ 164.528 Accounting of disclosures of protected health information.

45 CFR 164.528 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.528

(a) Standard: Right to an accounting of disclosures of protected health information. (1) An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except for disclosures:

(i) To carry out treatment, payment and health care operations as provided in § 164.506;

(ii) To individuals of protected health information about them as provided in § 164.502;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, as provided in § 164.502;

(iv) Pursuant to an authorization as provided in § 164.508;

(v) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in § 164.510;

(vi) For national security or intelligence purposes as provided in § 164.512(k)(2);

(vii) To correctional institutions or law enforcement officials as provided in § 164.512(k)(5);

(viii) As part of a limited data set in accordance with § 164.514(e); or

(ix) That occurred prior to the compliance date for the covered entity.

(2)(i) The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official, as provided in § 164.512(d) or (f), respectively, for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

(ii) If the agency or official statement in paragraph (a)(2)(i) of this section is made orally, the covered entity must:

(A) Document the statement, including the identity of the agency or official making the statement;

(B) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

(C) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement pursuant to paragraph (a)(2)(i) of this section is submitted during that time.

(3) An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

(b) Implementation specifications: Content of the accounting. The covered entity must provide the individual with a written accounting that meets the following requirements.

(1) Except as otherwise provided by paragraph (a) of this section, the accounting must include disclosures of protected health information that occurred during the six years (or such shorter time period at the request of the individual as provided in paragraph (a)(3) of this section) prior to the date of the request for an accounting, including disclosures to or by business associates of the covered entity.

(2) Except as otherwise provided by paragraphs (b)(3) or (b)(4) of this section, the accounting must include for each disclosure:

(i) The date of the disclosure;

(ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(iii) A brief description of the protected health information disclosed; and

(iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under § 164.502(a)(2)(ii) or § 164.512, if any.

(3) If, during the period covered by the accounting, the covered entity has made multiple disclosures of protected health information to the same person or entity for a single purpose under § 164.502(a)(2)(ii) or § 164.512, the accounting may, with respect to such multiple disclosures, provide:

(i) The information required by paragraph (b)(2) of this section for the first disclosure during the accounting period;

(ii) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(iii) The date of the last such disclosure during the accounting period.

(4)(i) If, during the period covered by the accounting, the covered entity has made disclosures of protected health information for a particular research purpose in accordance with § 164.512(i) for 50 or more individuals, the accounting may, with respect to such disclosures for which the protected health information about the individual may have been included, provide:

(A) The name of the protocol or other research activity;

(B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(C) A brief description of the type of protected health information that was disclosed;

(D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

(F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

(ii) If the covered entity provides an accounting for research disclosures, in accordance with paragraph (b)(4) of this section, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

(c) Implementation specifications: Provision of the accounting. (1) The covered entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows.

(i) The covered entity must provide the individual with the accounting requested; or

(ii) If the covered entity is unable to provide the accounting within the time required by paragraph (c)(1) of this section, the covered entity may extend the time to provide the accounting by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (c)(1) of this section, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will provide the accounting; and

(B) The covered entity may have only one such extension of time for action on a request for an accounting.

(2) The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

(d) Implementation specification: Documentation. A covered entity must document the following and retain the documentation as required by § 164.530(j):

(1) The information required to be included in an accounting under paragraph (b) of this section for disclosures of protected health information that are subject to an accounting under paragraph (a) of this section;

(2) The written accounting that is provided to the individual under this section; and

(3) The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53271, Aug. 14, 2002]

§ 164.530 Administrative requirements.

45 CFR 164.530 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.530

(a)(1) Standard: Personnel designations. (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

(ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

(2) Implementation specification: Personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) Implementation specifications: Training. (i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

(c)(1) Standard: Safeguards. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2)(i) Implementation specification: Safeguards. A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

(d)(1) Standard: Complaints to the covered entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.

(2) Implementation specification: Documentation of complaints. As required by paragraph (j) of this section, a covered entity must document all complaints received, and their disposition, if any.

(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section.

(2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate.

(g) Standard: Refraining from intimidating or retaliatory acts. A covered entity—

(1) May not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this subpart or subpart D of this part, including the filing of a complaint under this section; and

(2) Must refrain from intimidation and retaliation as provided in § 160.316 of this subchapter.

(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter, this subpart, or subpart D of this part, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(i)(1) Standard: Policies and procedures. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart and subpart D of this part. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.

(2) Standard: Changes to policies and procedures. (i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart or subpart D of this part.

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.520, and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it created or received prior to the effective date of the notice revision, if the covered entity has, in accordance with § 164.520(b)(1)(v)(C), included in the notice a statement reserving its right to make such a change in its privacy practices; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (i)(5) of this section.

(3) Implementation specification: Changes in law. Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice required by § 164.520, the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.520(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(4) Implementation specifications: Changes to privacy practices stated in the notice. (i) To implement a change as provided by paragraph (i)(2)(ii) of this section, a covered entity must:

(A) Ensure that the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, complies with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (j) of this section; and

(C) Revise the notice as required by § 164.520(b)(3) to state the changed practice and make the revised notice available as required by § 164.520(c). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not reserved its right under § 164.520(b)(1)(v)(C) to change a privacy practice that is stated in the notice,

the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or received while such notice is in effect. A covered entity may change a privacy practice that is stated in the notice, and the related policies and procedures, without having reserved the right to do so, provided that:

(A) Such change meets the implementation specifications in paragraphs (i)(4)(i)(A)-(C) of this section; and

(B) Such change is effective only with respect to protected health information created or received after the effective date of the notice.

(5) Implementation specification: Changes to other policies or procedures. A covered entity may change, at any time, a policy or procedure that does not materially affect the content of the notice required by § 164.520, provided that:

(i) The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and

(ii) Prior to the effective date of the change, the policy or procedure, as revised, is documented as required by paragraph (j) of this section.

(j)(1) Standard: Documentation. A covered entity must:

(i) Maintain the policies and procedures provided for in paragraph (i) of this section in written or electronic form;

(ii) If a communication is required by this subpart to be in writing, maintain such writing, or an electronic copy, as documentation; and

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity, or designation.

(iv) Maintain documentation sufficient to meet its burden of proof under § 164.414(b).

(2) Implementation specification: Retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

(k) Standard: Group health plans. (1) A group health plan is not subject to the standards or implementation specifications in paragraphs (a) through (f) and (i) of this section, to the extent that:

(i) The group health plan provides health benefits solely through an insurance contract with a health insurance issuer or an HMO; and

(ii) The group health plan does not create or receive protected health information, except for:

(A) Summary health information as defined in § 164.504(a); or

(B) Information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan.

(2) A group health plan described in paragraph (k)(1) of this section is subject to the standard and implementation specification in paragraph (j) of this section only with respect to plan documents amended in accordance with § 164.504(f).

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 71 FR 8433, Feb. 16, 2006; 74 FR 42769, Aug. 24, 2009]

§ 164.532 Transition provisions.

45 CFR 164.532 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.532

(a) Standard: Effect of prior authorizations. Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).

(b) Implementation specification: Effect of prior authorization for purposes other than research. Notwithstanding any provisions in § 164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with § 164.522(a).

(c) Implementation specification: Effect of prior permission for research. Notwithstanding any provisions in §§ 164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions, use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with § 164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

(1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) Standard: Effect of prior contracts or other arrangements with business associates. Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) Implementation specification: Deemed compliance—(1) Qualification. Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of § 164.314(a) or § 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) Limited deemed compliance period. A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

(3) Covered entity responsibilities. Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§ 164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) Effect of prior data use agreements. If, prior to January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

[65 FR 82802, Dec. 28, 2000, as amended at 67 FR 53272, Aug. 14, 2002; 78 FR 5702, Jan. 25, 2013; 78 FR 34266, June 7, 2013]

§ 164.534 Compliance dates for initial implementation of the privacy standards.

45 CFR 164.534 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.534

(a) Health care providers. A covered health care provider must comply with the applicable requirements of this subpart no later than April 14, 2003.

(b) Health plans. A health plan must comply with the applicable requirements of this subpart no later than the following as applicable:

(1) Health plans other than small health plans. April 14, 2003.

(2) Small health plans. April 14, 2004.

(c) Health clearinghouses. A health care clearinghouse must comply with the applicable requirements of this subpart no later than April 14, 2003.

[66 FR 12434, Feb. 26, 2001]

§ 164.535 Severability.

45 CFR 164.535 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-45/section-164.535

If any provision of the HIPAA Privacy Rule to Support Reproductive Health Care Privacy is held to be invalid or unenforceable facially, or as applied to any person, plaintiff, or circumstance, it shall be construed to give maximum effect to the provision permitted by law, unless such holding shall be one of utter invalidity or unenforceability, in which case the provision shall be severable from this part and shall not affect the remainder thereof or the application of the provision to other persons not similarly situated or to other dissimilar circumstances.

[89 FR 33066, Apr. 26, 2024]

Part 2: Telephone Consumer Protection Act (TCPA), official text

§227. Restrictions on use of telephone equipment

47 U.S.C. 227 · GovInfo, United States Code · https://www.govinfo.gov/link/uscode/47/227?link-type=html

(a) Definitions

As used in this section—

(1) The term "automatic telephone dialing system" means equipment which has the capacity—

(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and

(B) to dial such numbers.

(2) The term "established business relationship", for purposes only of subsection (b)(1)(C)(i), shall have the meaning given the term in section 64.1200 of title 47, Code of Federal Regulations, as in effect on January 1, 2003, except that—

(A) such term shall include a relationship between a person or entity and a business subscriber subject to the same terms applicable under such section to a relationship between a person or entity and a residential subscriber; and

(B) an established business relationship shall be subject to any time limitation established pursuant to paragraph (2)(G)).1

(3) The term "telephone facsimile machine" means equipment which has the capacity (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

(4) The term "telephone solicitation" means the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person, but such term does not include a call or message (A) to any person with that person's prior express invitation or permission, (B) to any person with whom the caller has an established business relationship, or (C) by a tax exempt nonprofit organization.

(5) The term "unsolicited advertisement" means any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission, in writing or otherwise.

(b) Restrictions on use of automated telephone equipment

(1) Prohibitions

It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States—

(A) to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice—

(i) to any emergency telephone line (including any "911" line and any emergency line of a hospital, medical physician or service office, health care facility, poison control center, or fire protection or law enforcement agency);

(ii) to the telephone line of any guest room or patient room of a hospital, health care facility, elderly home, or similar establishment; or

(iii) to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call, unless such call is made solely to collect a debt owed to or guaranteed by the United States;

(B) to initiate any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party, unless the call is initiated for emergency purposes, is made solely pursuant to the collection of a debt owed to or guaranteed by the United States, or is exempted by rule or order by the Commission under paragraph (2)(B);

(C) to use any telephone facsimile machine, computer, or other device to send, to a telephone facsimile machine, an unsolicited advertisement, unless—

(i) the unsolicited advertisement is from a sender with an established business relationship with the recipient;

(ii) the sender obtained the number of the telephone facsimile machine through—

(I) the voluntary communication of such number, within the context of such established business relationship, from the recipient of the unsolicited advertisement, or

(II) a directory, advertisement, or site on the Internet to which the recipient voluntarily agreed to make available its facsimile number for public distribution,

except that this clause shall not apply in the case of an unsolicited advertisement that is sent based on an established business relationship with the recipient that was in existence before July 9, 2005, if the sender possessed the facsimile machine number of the recipient before July 9, 2005; and

(iii) the unsolicited advertisement contains a notice meeting the requirements under paragraph (2)(D),

except that the exception under clauses (i) and (ii) shall not apply with respect to an unsolicited advertisement sent to a telephone facsimile machine by a sender to whom a request has been made not to send future unsolicited advertisements to such telephone facsimile machine that complies with the requirements under paragraph (2)(E); or

(D) to use an automatic telephone dialing system in such a way that two or more telephone lines of a multi-line business are engaged simultaneously.

(2) Regulations; exemptions and other provisions

The Commission shall prescribe regulations to implement the requirements of this subsection. In implementing the requirements of this subsection, the Commission—

(A) shall consider prescribing regulations to allow businesses to avoid receiving calls made using an artificial or prerecorded voice to which they have not given their prior express consent;

(B) may, by rule or order, exempt from the requirements of paragraph (1)(B) of this subsection, subject to such conditions as the Commission may prescribe—

(i) calls that are not made for a commercial purpose; and

(ii) such classes or categories of calls made for commercial purposes as the Commission determines—

(I) will not adversely affect the privacy rights that this section is intended to protect; and

(II) do not include the transmission of any unsolicited advertisement;

(C) may, by rule or order, exempt from the requirements of paragraph (1)(A)(iii) of this subsection calls to a telephone number assigned to a cellular telephone service that are not charged to the called party, subject to such conditions as the Commission may prescribe as necessary in the interest of the privacy rights this section is intended to protect;

(D) shall provide that a notice contained in an unsolicited advertisement complies with the requirements under this subparagraph only if—

(i) the notice is clear and conspicuous and on the first page of the unsolicited advertisement;

(ii) the notice states that the recipient may make a request to the sender of the unsolicited advertisement not to send any future unsolicited advertisements to a telephone facsimile machine or machines and that failure to comply, within the shortest reasonable time, as determined by the Commission, with such a request meeting the requirements under subparagraph (E) is unlawful;

(iii) the notice sets forth the requirements for a request under subparagraph (E);

(iv) the notice includes—

(I) a domestic contact telephone and facsimile machine number for the recipient to transmit such a request to the sender; and

(II) a cost-free mechanism for a recipient to transmit a request pursuant to such notice to the sender of the unsolicited advertisement; the Commission shall by rule require the sender to provide such a mechanism and may, in the discretion of the Commission and subject to such conditions as the Commission may prescribe, exempt certain classes of small business senders, but only if the Commission determines that the costs to such class are unduly burdensome given the revenues generated by such small businesses;

(v) the telephone and facsimile machine numbers and the cost-free mechanism set forth pursuant to clause (iv) permit an individual or business to make such a request at any time on any day of the week; and

(vi) the notice complies with the requirements of subsection (d);

(E) shall provide, by rule, that a request not to send future unsolicited advertisements to a telephone facsimile machine complies with the requirements under this subparagraph only if—

(i) the request identifies the telephone number or numbers of the telephone facsimile machine or machines to which the request relates;

(ii) the request is made to the telephone or facsimile number of the sender of such an unsolicited advertisement provided pursuant to subparagraph (D)(iv) or by any other method of communication as determined by the Commission; and

(iii) the person making the request has not, subsequent to such request, provided express invitation or permission to the sender, in writing or otherwise, to send such advertisements to such person at such telephone facsimile machine;

(F) may, in the discretion of the Commission and subject to such conditions as the Commission may prescribe, allow professional or trade associations that are tax-exempt nonprofit organizations to send unsolicited advertisements to their members in furtherance of the association's tax-exempt purpose that do not contain the notice required by paragraph (1)(C)(iii), except that the Commission may take action under this subparagraph only—

(i) by regulation issued after public notice and opportunity for public comment; and

(ii) if the Commission determines that such notice required by paragraph (1)(C)(iii) is not necessary to protect the ability of the members of such associations to stop such associations from sending any future unsolicited advertisements;

(G)(i) may, consistent with clause (ii), limit the duration of the existence of an established business relationship, however, before establishing any such limits, the Commission shall—

(I) determine whether the existence of the exception under paragraph (1)(C) relating to an established business relationship has resulted in a significant number of complaints to the Commission regarding the sending of unsolicited advertisements to telephone facsimile machines;

(II) determine whether a significant number of any such complaints involve unsolicited advertisements that were sent on the basis of an established business relationship that was longer in duration than the Commission believes is consistent with the reasonable expectations of consumers;

(III) evaluate the costs to senders of demonstrating the existence of an established business relationship within a specified period of time and the benefits to recipients of establishing a limitation on such established business relationship; and

(IV) determine whether with respect to small businesses, the costs would not be unduly burdensome; and

(ii) may not commence a proceeding to determine whether to limit the duration of the existence of an established business relationship before the expiration of the 3-month period that begins on July 9, 2005;

(H) may restrict or limit the number and duration of calls made to a telephone number assigned to a cellular telephone service to collect a debt owed to or guaranteed by the United States; and

(I) shall ensure that any exemption under subparagraph (B) or (C) contains requirements for calls made in reliance on the exemption with respect to—

(i) the classes of parties that may make such calls;

(ii) the classes of parties that may be called; and

(iii) the number of such calls that a calling party may make to a particular called party.

(3) Private right of action

A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State—

(A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation,

(B) an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or

(C) both such actions.

If the court finds that the defendant willfully or knowingly violated this subsection or the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph.

(4) Civil forfeiture

(A) In general

Any person that is determined by the Commission, in accordance with paragraph (3) or (4) of section 503(b) of this title, to have violated this subsection shall be liable to the United States for a forfeiture penalty pursuant to section 503(b)(1) of this title. Paragraph (5) of section 503(b) of this title shall not apply in the case of a violation of this subsection. A forfeiture penalty under this subparagraph shall be in addition to any other penalty provided for by this chapter. The amount of the forfeiture penalty determined under this subparagraph shall be determined in accordance with subparagraphs (A) through (F) of section 503(b)(2) of this title.

(B) Violation with intent

Any person that is determined by the Commission, in accordance with paragraph (3) or (4) of section 503(b) of this title, to have violated this subsection with the intent to cause such violation shall be liable to the United States for a forfeiture penalty pursuant to section 503(b)(1) of this title. Paragraph (5) of section 503(b) of this title shall not apply in the case of a violation of this

subsection. A forfeiture penalty under this subparagraph shall be in addition to any other penalty provided for by this chapter. The amount of the forfeiture penalty determined under this subparagraph shall be equal to an amount determined in accordance with subparagraphs (A) through (F) of section 503(b)(2) of this title plus an additional penalty not to exceed $10,000.

(C) Recovery

Any forfeiture penalty determined under subparagraph (A) or (B) shall be recoverable under section 504(a) of this title.

(D) Procedure

No forfeiture liability shall be determined under subparagraph (A) or (B) against any person unless such person receives the notice required by section 503(b)(3) of this title or section 503(b)(4) of this title.

(E) Statute of limitations

Notwithstanding paragraph (6) of section 503(b) of this title, no forfeiture penalty shall be determined or imposed against any person—

(i) under subparagraph (A) if the violation charged occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability; or

(ii) under subparagraph (B) if the violation charged occurred more than 4 years prior to the date of issuance of the required notice or notice of apparent liability.

(F) Rule of construction

Notwithstanding any law to the contrary, the Commission may not determine or impose a forfeiture penalty on a person under both subparagraphs (A) and (B) based on the same conduct.

(c) Protection of subscriber privacy rights

(1) Rulemaking proceeding required

Within 120 days after December 20, 1991, the Commission shall initiate a rulemaking proceeding concerning the need to protect residential telephone subscribers' privacy rights to avoid receiving telephone solicitations to which they object. The proceeding shall—

(A) compare and evaluate alternative methods and procedures (including the use of electronic databases, telephone network technologies, special directory markings, industry-based or company-specific "do not call" systems, and any other alternatives, individually or in combination) for their effectiveness in protecting such privacy rights, and in terms of their cost and other advantages and disadvantages;

(B) evaluate the categories of public and private entities that would have the capacity to establish and administer such methods and procedures;

(C) consider whether different methods and procedures may apply for local telephone solicitations, such as local telephone solicitations of small businesses or holders of second class mail permits;

(D) consider whether there is a need for additional Commission authority to further restrict telephone solicitations, including those calls exempted under subsection (a)(3) of this section, and, if such a finding is made and supported by the record, propose specific restrictions to the Congress; and

(E) develop proposed regulations to implement the methods and procedures that the Commission determines are most effective and efficient to accomplish the purposes of this section.

(2) Regulations

Not later than 9 months after December 20, 1991, the Commission shall conclude the rulemaking proceeding initiated under paragraph (1) and shall prescribe regulations to implement methods and procedures for protecting the privacy rights described in such paragraph in an efficient, effective, and economic manner and without the imposition of any additional charge to telephone subscribers.

(3) Use of database permitted

The regulations required by paragraph (2) may require the establishment and operation of a single national database to compile a list of telephone numbers of residential subscribers who object to receiving telephone solicitations, and to make that compiled list and parts thereof available for purchase. If the Commission determines to require such a database, such regulations shall—

(A) specify a method by which the Commission will select an entity to administer such database;

(B) require each common carrier providing telephone exchange service, in accordance with regulations prescribed by the Commission, to inform subscribers for telephone exchange service of the opportunity to provide notification, in accordance with regulations established under this paragraph, that such subscriber objects to receiving telephone solicitations;

(C) specify the methods by which each telephone subscriber shall be informed, by the common carrier that provides local exchange service to that subscriber, of (i) the subscriber's right to give or revoke a notification of an objection under subparagraph (A), and (ii) the methods by which such right may be exercised by the subscriber;

(D) specify the methods by which such objections shall be collected and added to the database;

(E) prohibit any residential subscriber from being charged for giving or revoking such notification or for being included in a database compiled under this section;

(F) prohibit any person from making or transmitting a telephone solicitation to the telephone number of any subscriber included in such database;

(G) specify (i) the methods by which any person desiring to make or transmit telephone solicitations will obtain access to the database, by area code or local exchange prefix, as required to avoid calling the telephone numbers of subscribers included in such database; and (ii) the costs to be recovered from such persons;

(H) specify the methods for recovering, from persons accessing such database, the costs involved in identifying, collecting, updating, disseminating, and selling, and other activities relating to, the operations of the database that are incurred by the entities carrying out those activities;

(I) specify the frequency with which such database will be updated and specify the method by which such updating will take effect for purposes of compliance with the regulations prescribed under this subsection;

(J) be designed to enable States to use the database mechanism selected by the Commission for purposes of administering or enforcing State law;

(K) prohibit the use of such database for any purpose other than compliance with the requirements of this section and any such State law and specify methods for protection of the privacy rights of persons whose numbers are included in such database; and

(L) require each common carrier providing services to any person for the purpose of making telephone solicitations to notify such person of the requirements of this section and the regulations thereunder.

(4) Considerations required for use of database method

If the Commission determines to require the database mechanism described in paragraph (3), the Commission shall—

(A) in developing procedures for gaining access to the database, consider the different needs of telemarketers conducting business on a national, regional, State, or local level;

(B) develop a fee schedule or price structure for recouping the cost of such database that recognizes such differences and—

(i) reflect the relative costs of providing a national, regional, State, or local list of phone numbers of subscribers who object to receiving telephone solicitations;

(ii) reflect the relative costs of providing such lists on paper or electronic media; and

(iii) not place an unreasonable financial burden on small businesses; and

(C) consider (i) whether the needs of telemarketers operating on a local basis could be met through special markings of area white pages directories, and (ii) if such directories are needed as an adjunct to database lists prepared by area code and local exchange prefix.

(5) Private right of action

A person who has received more than one telephone call within any 12-month period by or on behalf of the same entity in violation of the regulations prescribed under this subsection may, if otherwise permitted by the laws or rules of court of a State bring in an appropriate court of that State—

(A) an action based on a violation of the regulations prescribed under this subsection to enjoin such violation,

(B) an action to recover for actual monetary loss from such a violation, or to receive up to $500 in damages for each such violation, whichever is greater, or

(C) both such actions.

It shall be an affirmative defense in any action brought under this paragraph that the defendant has established and implemented, with due care, reasonable practices and procedures to effectively prevent telephone solicitations in violation of the regulations prescribed under this subsection. If the court finds that the defendant willfully or knowingly violated the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph.

(6) Relation to subsection (b)

The provisions of this subsection shall not be construed to permit a communication prohibited by subsection (b).

(d) Technical and procedural standards

(1) Prohibition

It shall be unlawful for any person within the United States—

(A) to initiate any communication using a telephone facsimile machine, or to make any telephone call using any automatic telephone dialing system, that does not comply with the technical and procedural standards prescribed under this subsection, or to use any telephone facsimile machine or automatic telephone dialing system in a manner that does not comply with such standards; or

(B) to use a computer or other electronic device to send any message via a telephone facsimile machine unless such person clearly marks, in a margin at the top or bottom of each transmitted page of the message or on the first page of the transmission, the date and time it is sent and an identification of the business, other entity, or individual sending the message and the telephone number of the sending machine or of such business, other entity, or individual.

(2) Telephone facsimile machines

The Commission shall revise the regulations setting technical and procedural standards for telephone facsimile machines to require that any such machine which is manufactured after one year after December 20, 1991, clearly marks, in a margin at the top or bottom of each transmitted page or on the first page of each transmission, the date and time sent, an identification of the business, other entity, or individual sending the message, and the telephone number of the sending machine or of such business, other entity, or individual.

(3) Artificial or prerecorded voice systems

The Commission shall prescribe technical and procedural standards for systems that are used to transmit any artificial or prerecorded voice message via telephone. Such standards shall require that—

(A) all artificial or prerecorded telephone messages (i) shall, at the beginning of the message, state clearly the identity of the business, individual, or other entity initiating the call, and (ii) shall, during or after the message, state clearly the telephone number or address of such business, other entity, or individual; and

(B) any such system will automatically release the called party's line within 5 seconds of the time notification is transmitted to the system that the called party has hung up, to allow the called party's line to be used to make or receive other calls.

(e) Prohibition on provision of misleading or inaccurate caller identification information

(1) In general

It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States, in connection with any voice service or text messaging service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted pursuant to paragraph (3)(B).

(2) Protection for blocking caller identification information

Nothing in this subsection may be construed to prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information.

(3) Regulations

(A) In general

The Commission shall prescribe regulations to implement this subsection.

(B) Content of regulations

(i) In general

The regulations required under subparagraph (A) shall include such exemptions from the prohibition under paragraph (1) as the Commission determines is appropriate.

(ii) Specific exemption for law enforcement agencies or court orders

The regulations required under subparagraph (A) shall exempt from the prohibition under paragraph (1) transmissions in connection with—

(I) any authorized activity of a law enforcement agency; or

(II) a court order that specifically authorizes the use of caller identification manipulation.

(4) Repealed. Pub. L. 115–141, div. P, title IV, §402(i)(3), Mar. 23, 2018, 132 Stat. 1089

(5) Penalties

(A) Civil forfeiture

(i) In general

Any person that is determined by the Commission, in accordance with paragraphs (3) and (4) of section 503(b) of this title, to have violated this subsection shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this paragraph shall be in addition to any other penalty provided for by this chapter. The amount of the forfeiture penalty determined under this paragraph shall not exceed $10,000 for each violation, or 3 times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act.

(ii) Recovery

Any forfeiture penalty determined under clause (i) shall be recoverable pursuant to section 504(a) of this title. Paragraph (5) of section 503(b) of this title shall not apply in the case of a violation of this subsection.

(iii) Procedure

No forfeiture liability shall be determined under clause (i) against any person unless such person receives the notice required by section 503(b)(3) of this title or section 503(b)(4) of this title.

(iv) 4-year statute of limitations

No forfeiture penalty shall be determined or imposed against any person under clause (i) if the violation charged occurred more than 4 years prior to the date of issuance of the required notice or notice or apparent liability.

(B) Criminal fine

Any person who willfully and knowingly violates this subsection shall upon conviction thereof be fined not more than $10,000 for each violation, or 3 times that amount for each day of a continuing violation, in lieu of the fine provided by section 501 of this title for such a violation. This subparagraph does not supersede the provisions of section 501 of this title relating to imprisonment or the imposition of a penalty of both fine and imprisonment.

(6) Enforcement by States

(A) In general

The chief legal officer of a State, or any other State officer authorized by law to bring actions on behalf of the residents of a State, may bring a civil action, as parens patriae, on behalf of the residents of that State in an appropriate district court of the United States to enforce this subsection or to impose the civil penalties for violation of this subsection, whenever the chief legal officer or other State officer has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected by a violation of this subsection or a regulation under this subsection.

(B) Notice

The chief legal officer or other State officer shall serve written notice on the Commission of any civil action under subparagraph (A) prior to initiating such civil action. The notice shall include a copy of the complaint to be filed to initiate such civil action, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such civil action.

(C) Authority to intervene

Upon receiving the notice required by subparagraph (B), the Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(D) Construction

For purposes of bringing any civil action under subparagraph (A), nothing in this paragraph shall prevent the chief legal officer or other State officer from exercising the powers conferred on that officer by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(E) Venue; service or process

(i) Venue

An action brought under subparagraph (A) shall be brought in a district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28.

(ii) Service of process

In an action brought under subparagraph (A)—

(I) process may be served without regard to the territorial limits of the district or of the State in which the action is instituted; and

(II) a person who participated in an alleged violation that is being litigated in the civil action may be joined in the civil action without regard to the residence of the person.

(7) Effect on other laws

This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(8) Definitions

For purposes of this subsection:

(A) Caller identification information

The term "caller identification information" means information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a voice service or a text message sent using a text messaging service.

(B) Caller identification service

The term "caller identification service" means any service or device designed to provide the user of the service or device with the telephone number of, or other information regarding the origination of, a call made using a voice service or a text message sent using a text messaging service. Such term includes automatic number identification services.

(C) Text message

The term "text message"—

(i) means a message consisting of text, images, sounds, or other information that is transmitted to or from a device that is identified as the receiving or transmitting device by means of a 10-digit telephone number or N11 service code;

(ii) includes a short message service (commonly referred to as "SMS") message and a multimedia message service (commonly referred to as "MMS") message; and

(iii) does not include—

(I) a real-time, two-way voice or video communication; or

(II) a message sent over an IP-enabled messaging service to another user of the same messaging service, except a message described in clause (ii).

(D) Text messaging service

The term "text messaging service" means a service that enables the transmission or receipt of a text message, including a service provided as part of or in connection with a voice service.

(E) Voice service

The term "voice service"—

(i) means any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of this title; and

(ii) includes transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine.

(9) Limitation

Notwithstanding any other provision of this section, subsection (f) shall not apply to this subsection or to the regulations under this subsection.

(f) Effect on State law

(1) State law not preempted

Except for the standards prescribed under subsection (d) and subject to paragraph (2) of this subsection, nothing in this section or in the regulations prescribed under this section shall preempt any State law that imposes more restrictive intrastate requirements or regulations on, or which prohibits—

(A) the use of telephone facsimile machines or other electronic devices to send unsolicited advertisements;

(B) the use of automatic telephone dialing systems;

(C) the use of artificial or prerecorded voice messages; or

(D) the making of telephone solicitations.

(2) State use of databases

If, pursuant to subsection (c)(3), the Commission requires the establishment of a single national database of telephone numbers of subscribers who object to receiving telephone solicitations, a State or local authority may not, in its regulation of telephone solicitations, require the use of any database, list, or listing system that does not include the part of such single national database

that relates to such State.

(g) Actions by States

(1) Authority of States

Whenever the attorney general of a State, or an official or agency designated by a State, has reason to believe that any person has engaged or is engaging in a pattern or practice of telephone calls or other transmissions to residents of that State in violation of this section or the regulations prescribed under this section, the State may bring a civil action on behalf of its residents to enjoin such calls, an action to recover for actual monetary loss or receive $500 in damages for each violation, or both such actions. If the court finds the defendant willfully or knowingly violated such regulations, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under the preceding sentence.

(2) Exclusive jurisdiction of Federal courts

The district courts of the United States, the United States courts of any territory, and the District Court of the United States for the District of Columbia shall have exclusive jurisdiction over all civil actions brought under this subsection. Upon proper application, such courts shall also have jurisdiction to issue writs of mandamus, or orders affording like relief, commanding the defendant to comply with the provisions of this section or regulations prescribed under this section, including the requirement that the defendant take such action as is necessary to remove the danger of such violation. Upon a proper showing, a permanent or temporary injunction or restraining order shall be granted without bond.

(3) Rights of Commission

The State shall serve prior written notice of any such civil action upon the Commission and provide the Commission with a copy of its complaint, except in any case where such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Commission shall have the right (A) to intervene in the action, (B) upon so intervening, to be heard on all matters arising therein, and (C) to file petitions for appeal.

(4) Venue; service of process

Any civil action brought under this subsection in a district court of the United States may be brought in the district wherein the defendant is found or is an inhabitant or transacts business or wherein the violation occurred or is occurring, and process in such cases may be served in any district in which the defendant is an inhabitant or where the defendant may be found.

(5) Investigatory powers

For purposes of bringing any civil action under this subsection, nothing in this section shall prevent the attorney general of a State, or an official or agency designated by a State, from exercising the powers conferred on the attorney general or such official by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(6) Effect on State court proceedings

Nothing contained in this subsection shall be construed to prohibit an authorized State official from proceeding in State court on the basis of an alleged violation of any general civil or criminal statute of such State.

(7) Limitation

Whenever the Commission has instituted a civil action for violation of regulations prescribed under this section, no State may, during the pendency of such action instituted by the Commission, subsequently institute a civil action against any defendant named in the Commission's complaint for any violation as alleged in the Commission's complaint.

(8) "Attorney general" defined

As used in this subsection, the term "attorney general" means the chief legal officer of a State.

(h) Annual report to Congress on robocalls and transmission of misleading or inaccurate caller identification information

(1) Report required

Not later than 1 year after December 30, 2019, and annually thereafter, the Commission, after consultation with the Federal Trade Commission, shall submit to Congress a report regarding enforcement by the Commission of subsections (b), (c), (d), and (e) during the preceding calendar year.

(2) Matters for inclusion

Each report required by paragraph (1) shall include the following:

(A) The number of complaints received by the Commission during each of the preceding 5 calendar years, for each of the following categories:

(i) Complaints alleging that a consumer received a call in violation of subsection (b) or (c).

(ii) Complaints alleging that a consumer received a call in violation of the standards prescribed under subsection (d).

(iii) Complaints alleging that a consumer received a call in connection with which misleading or inaccurate caller identification information was transmitted in violation of subsection (e).

(B) The number of citations issued by the Commission pursuant to section 503(b) of this title during the preceding calendar year to enforce subsection (d), and details of each such citation.

(C) The number of notices of apparent liability issued by the Commission pursuant to section 503(b) of this title during the preceding calendar year to enforce subsections (b), (c), (d), and (e), and details of each such notice including any proposed forfeiture amount.

(D) The number of final orders imposing forfeiture penalties issued pursuant to section 503(b) of this title during the preceding calendar year to enforce such subsections, and details of each such order including the forfeiture imposed.

(E) The amount of forfeiture penalties or criminal fines collected, during the preceding calendar year, by the Commission or the Attorney General for violations of such subsections, and details of each case in which such a forfeiture penalty or criminal fine was collected.

(F) Proposals for reducing the number of calls made in violation of such subsections.

(G) An analysis of the contribution by providers of interconnected VoIP service and non-interconnected VoIP service that discount high-volume, unlawful, short-duration calls to the total number of calls made in violation of such subsections, and recommendations on how to address such contribution in order to decrease the total number of calls made in violation of such subsections.

(3) No additional reporting required

The Commission shall prepare the report required by paragraph (1) without requiring the provision of additional information from providers of telecommunications service or voice service (as defined in section 227b(a) of this title).

(i) Information sharing

(1) In general

Not later than 18 months after December 30, 2019, the Commission shall prescribe regulations to establish a process that

streamlines the ways in which a private entity may voluntarily share with the Commission information relating to—

(A) a call made or a text message sent in violation of subsection (b); or

(B) a call or text message for which misleading or inaccurate caller identification information was caused to be transmitted in violation of subsection (e).

(2) Text message defined

In this subsection, the term "text message" has the meaning given such term in subsection (e)(8).

(j) Robocall blocking service

(1) In general

Not later than 1 year after December 30, 2019, the Commission shall take a final agency action to ensure the robocall blocking services provided on an opt-out or opt-in basis pursuant to the Declaratory Ruling of the Commission in the matter of Advanced Methods to Target and Eliminate Unlawful Robocalls (CG Docket No. 17–59; FCC 19–51; adopted on June 6, 2019)—

(A) are provided with transparency and effective redress options for both—

(i) consumers; and

(ii) callers; and 2

(B) are provided with no additional line item charge to consumers and no additional charge to callers for resolving complaints related to erroneously blocked calls; and

(C) make all reasonable efforts to avoid blocking emergency public safety calls.

(2) Text message defined

In this subsection, the term "text message" has the meaning given such term in subsection (e)(8).

(June 19, 1934, ch. 652, title II, §227, as added Pub. L. 102–243, §3(a), Dec. 20, 1991, 105 Stat. 2395; amended Pub. L. 102–556, title IV, §402, Oct. 28, 1992, 106 Stat. 4194; Pub. L. 103–414, title III, §303(a)(11), (12), Oct. 25, 1994, 108 Stat. 4294; Pub. L. 108–187, §12, Dec. 16, 2003, 117 Stat. 2717; Pub. L. 109–21, §§2(a)–(g), 3, July 9, 2005, 119 Stat. 359–362; Pub. L. 111–331, §2, Dec. 22, 2010, 124 Stat. 3572; Pub. L. 114–74, title III, §301(a), Nov. 2, 2015, 129 Stat. 588; Pub. L. 115–141, div. P, title IV, §402(i)(3), title V, §503(a)(1)–(4)(A), Mar. 23, 2018, 132 Stat. 1089, 1091, 1092; Pub. L. 116–105, §§3(a), 8(a), 10(a), (b), Dec. 30, 2019, 133 Stat. 3274, 3283, 3284.)

§ 64.1200 Delivery restrictions.

47 CFR 64.1200 · eCFR, eCFR, up to date as of 2026-11-05 · https://www.ecfr.gov/current/title-47/section-64.1200

Link to an amendment published at 91 FR 67219, Oct. 26, 2026.
(a) No person or entity may:

(1) Except as provided in paragraph (a)(2) of this section, initiate any telephone call (other than a call made for emergency purposes or is made with the prior express consent of the called party) using an automatic telephone dialing system or an artificial or prerecorded voice;

(i) To any emergency telephone line, including any 911 line and any emergency line of a hospital, medical physician or service office, health care facility, poison control center, or fire protection or law enforcement agency;

(ii) To the telephone line of any guest room or patient room of a hospital, health care facility, elderly home, or similar

establishment; or

(iii) To any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call.

(iv) A person will not be liable for violating the prohibition in paragraph (a)(1)(iii) of this section when the call is placed to a wireless number that has been ported from wireline service and such call is a voice call; not knowingly made to a wireless number; and made within 15 days of the porting of the number from wireline to wireless service, provided the number is not already on the national do-not-call registry or caller's company-specific do-not-call list. A person will not be liable for violating the prohibition in paragraph (a)(1)(iii) of this section when making calls exempted by paragraph (a)(9) of this section.

(2) Initiate, or cause to be initiated, any telephone call that includes or introduces an advertisement or constitutes telemarketing, using an automatic telephone dialing system or an artificial or prerecorded voice, to any of the lines or telephone numbers described in paragraphs (a)(1)(i) through (iii) of this section, other than a call made with the prior express written consent of the called party or the prior express consent of the called party when the call is made by or on behalf of a tax-exempt nonprofit organization, or a call that delivers a “health care” message made by, or on behalf of, a “covered entity” or its “business associate,” as those terms are defined in the HIPAA Privacy Rule, 45 CFR 160.103.

(3) Initiate any telephone call to any residential line using an artificial or prerecorded voice to deliver a message that includes or introduces an advertisement or constitutes telemarketing without the prior express written consent of the called party, or that exceeds the applicable numerical limitation on calls identified in paragraphs (a)(3)(ii) through (v) of this section without the prior express consent of the called party. A telephone call to any residential line using an artificial or prerecorded voice to deliver a message requires no consent if the call:

(i) Is made for emergency purposes;

(ii) Is not made for a commercial purpose and the caller makes no more than three calls within any consecutive 30-day period to the residential line and honors the called party's request to opt out of future calls as required in paragraphs (b) and (d) of this section;

(iii) Is made for a commercial purpose but does not include or introduce an advertisement or constitute telemarketing and the caller makes no more than three calls within any consecutive 30-day period to the residential line and honors the called party's request to opt out of future calls as required in paragraphs (b) and (d) of this section;

(iv) Is made by or on behalf of a tax-exempt nonprofit organization and the caller makes no more than three calls within any consecutive 30-day period to the residential line and honors the called party's request to opt out of future calls as required in paragraphs (b) and (d) of this section; or

(v) Delivers a “health care” message made by, or on behalf of, a “covered entity” or its “business associate,” as those terms are defined in the HIPAA Privacy Rule, 45 CFR 160.103, and the caller makes no more than one call per day to each patient's residential line, up to a maximum of three calls combined per week to each patient's residential line and honors the called party's request to opt out of future calls as required in paragraphs (b) and (d) of this section.

(4) Use a telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine, unless—

(i) The unsolicited advertisement is from a sender with an established business relationship, as defined in paragraph (f)(6) of this section, with the recipient; and

(ii) The sender obtained the number of the telephone facsimile machine through—

(A) The voluntary communication of such number by the recipient directly to the sender, within the context of such established business relationship; or

(B) A directory, advertisement, or site on the Internet to which the recipient voluntarily agreed to make available its facsimile

number for public distribution. If a sender obtains the facsimile number from the recipient's own directory, advertisement, or Internet site, it will be presumed that the number was voluntarily made available for public distribution, unless such materials explicitly note that unsolicited advertisements are not accepted at the specified facsimile number. If a sender obtains the facsimile number from other sources, the sender must take reasonable steps to verify that the recipient agreed to make the number available for public distribution.

(C) This clause shall not apply in the case of an unsolicited advertisement that is sent based on an established business relationship with the recipient that was in existence before July 9, 2005 if the sender also possessed the facsimile machine number of the recipient before July 9, 2005. There shall be a rebuttable presumption that if a valid established business relationship was formed prior to July 9, 2005, the sender possessed the facsimile number prior to such date as well; and

(iii) The advertisement contains a notice that informs the recipient of the ability and means to avoid future unsolicited advertisements. A notice contained in an advertisement complies with the requirements under this paragraph only if—

(A) The notice is clear and conspicuous and on the first page of the advertisement;

(B) The notice states that the recipient may make a request to the sender of the advertisement not to send any future advertisements to a telephone facsimile machine or machines and that failure to comply, within 30 days, with such a request meeting the requirements under paragraph (a)(4)(v) of this section is unlawful;

(C) The notice sets forth the requirements for an opt-out request under paragraph (a)(4)(v) of this section;

(D) The notice includes—

(1) A domestic contact telephone number and facsimile machine number for the recipient to transmit such a request to the sender; and

(2) If neither the required telephone number nor facsimile machine number is a toll-free number, a separate cost-free mechanism including a Web site address or email address, for a recipient to transmit a request pursuant to such notice to the sender of the advertisement. A local telephone number also shall constitute a cost-free mechanism so long as recipients are local and will not incur any long distance or other separate charges for calls made to such number; and

(E) The telephone and facsimile numbers and cost-free mechanism identified in the notice must permit an individual or business to make an opt-out request 24 hours a day, 7 days a week.

(iv) A request not to send future unsolicited advertisements to a telephone facsimile machine complies with the requirements under this subparagraph only if—

(A) The request identifies the telephone number or numbers of the telephone facsimile machine or machines to which the request relates;

(B) The request is made to the telephone number, facsimile number, Web site address or email address identified in the sender's facsimile advertisement; and

(C) The person making the request has not, subsequent to such request, provided express invitation or permission to the sender, in writing or otherwise, to send such advertisements to such person at such telephone facsimile machine.

(v) A sender that receives a request not to send future unsolicited advertisements that complies with paragraph (a)(4)(v) of this section must honor that request within the shortest reasonable time from the date of such request, not to exceed 30 days, and is prohibited from sending unsolicited advertisements to the recipient unless the recipient subsequently provides prior express invitation or permission to the sender. The recipient's opt-out request terminates the established business relationship exemption for purposes of sending future unsolicited advertisements. If such requests are recorded or maintained by a party other than the sender on whose behalf the unsolicited advertisement is sent, the sender will be liable for any failures to honor the opt-out request.

(vi) A facsimile broadcaster will be liable for violations of paragraph (a)(4) of this section, including the inclusion of opt-out

notices on unsolicited advertisements, if it demonstrates a high degree of involvement in, or actual notice of, the unlawful activity and fails to take steps to prevent such facsimile transmissions.

(5) Use an automatic telephone dialing system in such a way that two or more telephone lines of a multi-line business are engaged simultaneously.

(6) Disconnect an unanswered telemarketing call prior to at least 15 seconds or four (4) rings.

(7) Abandon more than three percent of all telemarketing calls that are answered live by a person, as measured over a 30-day period for a single calling campaign. If a single calling campaign exceeds a 30-day period, the abandonment rate shall be calculated separately for each successive 30-day period or portion thereof that such calling campaign continues. A call is “abandoned” if it is not connected to a live sales representative within two (2) seconds of the called person's completed greeting.

(i) Whenever a live sales representative is not available to speak with the person answering the call, within two (2) seconds after the called person's completed greeting, the telemarketer or the seller must provide:

(A) A prerecorded identification and opt-out message that is limited to disclosing that the call was for “telemarketing purposes” and states the name of the business, entity, or individual on whose behalf the call was placed, and a telephone number for such business, entity, or individual that permits the called person to make a do-not-call request during regular business hours for the duration of the telemarketing campaign; provided, that, such telephone number may not be a 900 number or any other number for which charges exceed local or long distance transmission charges, and

(B) An automated, interactive voice- and/or key press-activated opt-out mechanism that enables the called person to make a do-not-call request prior to terminating the call, including brief explanatory instructions on how to use such mechanism. When the called person elects to opt-out using such mechanism, the mechanism must automatically record the called person's number to the seller's do-not-call list and immediately terminate the call.

(ii) A call for telemarketing purposes that delivers an artificial or prerecorded voice message to a residential telephone line or to any of the lines or telephone numbers described in paragraphs (a)(1)(i) through (iii) of this section after the subscriber to such line has granted prior express written consent for the call to be made shall not be considered an abandoned call if the message begins within two (2) seconds of the called person's completed greeting.

(iii) The seller or telemarketer must maintain records establishing compliance with paragraph (a)(7) of this section.

(iv) Calls made by or on behalf of tax-exempt nonprofit organizations are not covered by this paragraph (a)(7).

(8) Use any technology to dial any telephone number for the purpose of determining whether the line is a facsimile or voice line.

(9) A person will not be liable for violating the prohibition in paragraph (a)(1)(iii) of this section for making any call exempted in this paragraph (a)(9), provided that the call is not charged to the called person or counted against the called person's plan limits on minutes or texts. As used in this paragraph (a)(9), the term “call” includes a text message, including a short message service (SMS) call.

(i) Calls made by a package delivery company to notify a consumer about a package delivery, provided that all of the following conditions are met:

(A) The notification must be sent only to the telephone number for the package recipient;

(B) The notification must identify the name of the package delivery company and include contact information for the package delivery company;

(C) The notification must not include any telemarketing, solicitation, or advertising content;

(D) The voice call or text message notification must be concise, generally one minute or less in length for voice calls or 160 characters or less in length for text messages;

(E) The package delivery company shall send only one notification (whether by voice call or text message) per package, except that one additional notification may be sent for each attempt to deliver the package, up to two attempts, if the recipient's signature is required for the package and the recipient was not available to sign for the package on the previous delivery attempt;

(F) The package delivery company must offer package recipients the ability to opt out of receiving future delivery notification calls and messages and must honor an opt-out request within a reasonable time from the date such request is made, not to exceed six business days; and,

(G) Each notification must include information on how to opt out of future delivery notifications; voice call notifications that could be answered by a live person must include an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the called person to make an opt-out request prior to terminating the call; voice call notifications that could be answered by an answering machine or voice mail service must include a toll-free number that the consumer can call to opt out of future package delivery notifications; text notifications must include the ability for the recipient to opt out by replying “STOP.”

(ii) Calls made by an inmate collect call service provider following an unsuccessful collect call to establish a billing arrangement with the called party to enable future collect calls, provided that all of the following conditions are met:

(A) Notifications must identify the name of the inmate collect call service provider and include contact information;

(B) Notifications must not include any telemarketing, solicitation, debt collection, or advertising content;

(C) Notifications must be clear and concise, generally one minute or less;

(D) Inmate collect call service providers shall send no more than three notifications following each inmate collect call that is unsuccessful due to the lack of an established billing arrangement, and shall not retain the called party's number after call completion or, in the alternative, after the third notification attempt; and

(E) Each notification call must include information on how to opt out of future calls; voice calls that could be answered by a live person must include an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the called person to make an opt-out request prior to terminating the call; voice calls that could be answered by an answering machine or voice mail service must include a toll-free number that the consumer can call to opt out of future notification calls; and,

(F) The inmate collect call service provider must honor opt-out requests immediately.

(iii) Calls made by any financial institution as defined in section 4(k) of the Bank Holding Company Act of 1956, 15 U.S.C. 6809(3)(A), provided that all of the following conditions are met:

(A) Voice calls and text messages must be sent only to the wireless telephone number provided by the customer of the financial institution;

(B) Voice calls and text messages must state the name and contact information of the financial institution (for voice calls, these disclosures must be made at the beginning of the call);

(C) Voice calls and text messages are strictly limited to those for the following purposes: transactions and events that suggest a risk of fraud or identity theft; possible breaches of the security of customers' personal information; steps consumers can take to prevent or remedy harm caused by data security breaches; and actions needed to arrange for receipt of pending money transfers;

(D) Voice calls and text messages must not include any telemarketing, cross-marketing, solicitation, debt collection, or advertising content;

(E) Voice calls and text messages must be concise, generally one minute or less in length for voice calls (unless more time is needed to obtain customer responses or answer customer questions) or 160 characters or less in length for text messages;

(F) A financial institution may initiate no more than three messages (whether by voice call or text message) per event over a

three-day period for an affected account;

(G) A financial institution must offer recipients within each message an easy means to opt out of future such messages; voice calls that could be answered by a live person must include an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the call recipient to make an opt-out request prior to terminating the call; voice calls that could be answered by an answering machine or voice mail service must include a toll-free number that the consumer can call to opt out of future calls; text messages must inform recipients of the ability to opt out by replying “STOP,” which will be the exclusive means by which consumers may opt out of such messages; and,

(H) A financial institution must honor opt-out requests immediately.

(iv) Calls made by, or on behalf of, healthcare providers, which include hospitals, emergency care centers, medical physician or service offices, poison control centers, and other healthcare professionals, provided that all of the following conditions are met:

(A) Voice calls and text messages must be sent only to the wireless telephone number provided by the patient;

(B) Voice calls and text messages must state the name and contact information of the healthcare provider (for voice calls, these disclosures would need to be made at the beginning of the call);

(C) Voice calls and text messages are strictly limited to those for the following purposes: appointment and exam confirmations and reminders, wellness checkups, hospital pre-registration instructions, pre-operative instructions, lab results, post-discharge follow-up intended to prevent readmission, prescription notifications, and home healthcare instructions;

(D) Voice calls and text messages must not include any telemarketing, solicitation, or advertising; may not include accounting, billing, debt-collection, or other financial content; and must comply with HIPAA privacy rules, 45 CFR 160.103;

(E) Voice calls and text messages must be concise, generally one minute or less in length for voice calls or 160 characters or less in length for text messages;

(F) A healthcare provider may initiate only one message (whether by voice call or text message) per day to each patient, up to a maximum of three voice calls or text messages combined per week to each patient;

(G) A healthcare provider must offer recipients within each message an easy means to opt out of future such messages; voice calls that could be answered by a live person must include an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the call recipient to make an opt-out request prior to terminating the call; voice calls that could be answered by an answering machine or voice mail service must include a toll-free number that the consumer can call to opt out of future healthcare calls; text messages must inform recipients of the ability to opt out by replying “STOP,” which will be the exclusive means by which consumers may opt out of such messages; and,

(H) A healthcare provider must honor opt-out requests immediately.

(10) A called party may revoke prior express consent, including prior express written consent, to receive calls or text messages made pursuant to paragraphs (a)(1) through (3) and (c)(2) of this section by using any reasonable method to clearly express a desire not to receive further calls or text messages from the caller or sender. Any revocation request made using an automated, interactive voice or key press-activated opt-out mechanism on a call; using the words “stop,” “quit,” “end,” “revoke,” “opt out,” “cancel,” or “unsubscribe” sent in reply to an incoming text message; or pursuant to a website or telephone number designated by the caller to process opt-out requests constitutes a reasonable means per se to revoke consent. If a called party uses any such method to revoke consent, that consent is considered definitively revoked and the caller may not send additional robocalls and robotexts. If a reply to an incoming text message uses words other than “stop,” “quit,” “end,” “revoke,” “opt out,” “cancel,” or “unsubscribe,” the caller must treat that reply text as a valid revocation request if a reasonable person would understand those words to have conveyed a request to revoke consent. Should the text initiator choose to use a texting protocol that does not allow reply texts, it must provide a clear and conspicuous disclosure on each text to the consumer that two-way texting is not available due to technical limitations of the texting protocol, and clearly and conspicuously provide on each text reasonable alternative ways to revoke consent. All requests to revoke prior express consent or prior express written consent made in any reasonable manner must be honored within a reasonable time not to exceed ten business days from receipt of such request. Callers or senders of text messages covered by

paragraphs (a)(1) through (3) and (c)(2) of this section may not designate an exclusive means to request revocation of consent.

(11) The use of any other means to revoke consent not listed in paragraph (a)(10) of this section, such as a voicemail or email to any telephone number or email address intended to reach the caller, creates a rebuttable presumption that the consumer has revoked consent when the called party satisfies their obligation to produce evidence that such a request has been made, absent evidence to the contrary. In those circumstances, a totality of circumstances analysis will determine whether the caller can demonstrate that a request to revoke consent has not been conveyed in a reasonable manner.

(12) A one-time text message confirming a request to revoke consent from receiving any further calls or text messages does not violate paragraphs (a)(1) and (2) of this section as long as the confirmation text merely confirms the text recipient's revocation request and does not include any marketing or promotional information, and is the only additional message sent to the called party after receipt of the revocation request. If the confirmation text is sent within five minutes of receipt, it will be presumed to fall within the consumer's prior express consent. If it takes longer, however, the sender will have to make a showing that such delay was reasonable. To the extent that the text recipient has consented to several categories of text messages from the text sender, the confirmation message may request clarification as to whether the revocation request was meant to encompass all such messages; the sender must cease all further texts for which consent is required absent further clarification that the recipient wishes to continue to receive certain text messages.

(b) All artificial or prerecorded voice telephone messages shall:

(1) At the beginning of the message, state clearly the identity of the business, individual, or other entity that is responsible for initiating the call. If a business is responsible for initiating the call, the name under which the entity is registered to conduct business with the State Corporation Commission (or comparable regulatory authority) must be stated;

(2) During or after the message, state clearly the telephone number (other than that of the autodialer or prerecorded message player that placed the call) of such business, other entity, or individual. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges. For telemarketing messages and messages made pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section to residential telephone subscribers, such telephone number must permit any individual to make a do-not-call request during regular business hours; and

(3) In every case where the artificial or prerecorded-voice telephone message is made pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or includes or introduces an advertisement or constitutes telemarketing and is delivered to a residential telephone line or any of the lines or telephone numbers described in paragraphs (a)(1)(i) through (iii) of this section, provide an automated, interactive voice- and/or key press-activated opt-out mechanism for the called person to make a do-not-call request, including brief explanatory instructions on how to use such mechanism, within two (2) seconds of providing the identification information required in paragraph (b)(1) of this section. When the called person elects to opt out using such mechanism, the mechanism must automatically record the called person's number to the caller's do-not-call list and immediately terminate the call. When the artificial or prerecorded-voice telephone message is left on an answering machine or a voice mail service, such message must also provide a toll free number that enables the called person to call back at a later time and connect directly to the automated, interactive voice- and/or key press-activated opt-out mechanism and automatically record the called person's number to the caller's do-not-call list.

(c) No person or entity shall initiate any telephone solicitation to:

(1) Any residential telephone subscriber before the hour of 8 a.m. or after 9 p.m. (local time at the called party's location), or

(2) A residential telephone subscriber who has registered his or her telephone number on the national do-not-call registry of persons who do not wish to receive telephone solicitations that is maintained by the Federal Government. Such do-not-call registrations must be honored indefinitely, or until the registration is cancelled by the consumer or the telephone number is removed by the database administrator. Any person or entity making telephone solicitations (or on whose behalf telephone solicitations are made) will not be liable for violating this requirement if:

(i) It can demonstrate that the violation is the result of error and that as part of its routine business practice, it meets the following standards:

(A) Written procedures. It has established and implemented written procedures to comply with the national do-not-call rules;

(B) Training of personnel. It has trained its personnel, and any entity assisting in its compliance, in procedures established pursuant to the national do-not-call rules;

(C) Recording. It has maintained and recorded a list of telephone numbers that the seller may not contact;

(D) Accessing the national do-not-call database. It uses a process to prevent telephone solicitations to any telephone number on any list established pursuant to the do-not-call rules, employing a version of the national do-not-call registry obtained from the administrator of the registry no more than 31 days prior to the date any call is made, and maintains records documenting this process.

Note to paragraph (c)(2)(i)(D):
The requirement in paragraph 64.1200(c)(2)(i)(D) for persons or entities to employ a version of the national do-not-call registry obtained from the administrator no more than 31 days prior to the date any call is made is effective January 1, 2005. Until January 1, 2005, persons or entities must continue to employ a version of the registry obtained from the administrator of the registry no more than three months prior to the date any call is made.

(E) Purchasing the national do-not-call database. It uses a process to ensure that it does not sell, rent, lease, purchase or use the national do-not-call database, or any part thereof, for any purpose except compliance with this section and any such state or federal law to prevent telephone solicitations to telephone numbers registered on the national database. It purchases access to the relevant do-not-call data from the administrator of the national database and does not participate in any arrangement to share the cost of accessing the national database, including any arrangement with telemarketers who may not divide the costs to access the national database among various client sellers; or

(ii) It has obtained the subscriber's prior express invitation or permission. Such permission must be evidenced by a signed, written agreement between the consumer and seller which states that the consumer agrees to be contacted by this seller and includes the telephone number to which the calls may be placed; or

(iii) The telemarketer making the call has a personal relationship with the recipient of the call.

(d) No person or entity shall initiate any artificial or prerecorded-voice telephone call pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or any call for telemarketing purposes to a residential telephone subscriber unless such person or entity has instituted procedures for maintaining a list of persons who request not to receive such calls made by or on behalf of that person or entity. The procedures instituted must meet the following minimum standards:

(1) Written policy. Persons or entities making artificial or prerecorded-voice telephone calls pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or calls for telemarketing purposes must have a written policy, available upon demand, for maintaining a do-not-call list.

(2) Training of personnel. Personnel engaged in making artificial or prerecorded-voice telephone calls pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or who are engaged in any aspect of telemarketing must be informed and trained in the existence and use of the do-not-call list.

(3) Recording, disclosure of do-not-call requests. If a person or entity making an artificial or prerecorded-voice telephone call pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or any call for telemarketing purposes (or on whose behalf such a call is made) receives a request from a residential telephone subscriber not to receive calls from that person or entity, the person or entity must record the request and place the subscriber's name, if provided, and telephone number on the do-not-call list at the time the request is made. Persons or entities making such calls (or on whose behalf such calls are made) must honor a residential subscriber's do-not-call request within a reasonable time from the date such request is made. This period may not exceed ten (10) business days from the receipt of such request. If such requests are recorded or maintained by a party other than the person or entity on whose behalf the call is made, the person or entity on whose behalf the call is made will be liable for any failures to honor the do-not-call request. A person or entity making an artificial or prerecorded-voice telephone call pursuant to an exemption under paragraphs (a)(3)(ii) through (v) or any call for telemarketing purposes must obtain a consumer's prior express permission to share or forward the consumer's request not to be called to a party other than the person or entity on whose behalf a

call is made or an affiliated entity.

(4) Identification of callers and telemarketers. A person or entity making an artificial or prerecorded-voice telephone call pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or any call for telemarketing purposes must provide the called party with the name of the individual caller, the name of the person or entity on whose behalf the call is being made, and a telephone number or address at which the person or entity may be contacted. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges.

(5) Affiliated persons or entities. In the absence of a specific request by the subscriber to the contrary, a residential subscriber's do-not-call request shall apply to the particular entity making the call (or on whose behalf a call is made), and will not apply to affiliated entities unless the consumer reasonably would expect them to be included given the identification of the caller and (for telemarketing calls) the product being advertised.

(6) Maintenance of do-not-call lists. A person or entity making artificial or prerecorded-voice telephone calls pursuant to an exemption under paragraphs (a)(3)(ii) through (v) of this section or any call for telemarketing purposes must maintain a record of a consumer's request not to receive further calls. A do-not-call request must be honored for 5 years from the time the request is made.

(e) The rules set forth in paragraph (c) and (d) of this section are applicable to any person or entity making telephone solicitations or telemarketing calls or text messages to wireless telephone numbers to the extent described in the Commission's Report and Order, CG Docket No. 02-278, FCC 03-153, “Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991.”

(f) As used in this section:

(1) The term advertisement means any material advertising the commercial availability or quality of any property, goods, or services.

(2) The terms automatic telephone dialing system and autodialer mean equipment which has the capacity to store or produce telephone numbers to be called using a random or sequential number generator and to dial such numbers.

(3) The term clear and conspicuous means a notice that would be apparent to the reasonable consumer, separate and distinguishable from the advertising copy or other disclosures. With respect to facsimiles and for purposes of paragraph (a)(4)(iii)(A) of this section, the notice must be placed at either the top or bottom of the facsimile.

(4) The term emergency purposes means calls made necessary in any situation affecting the health and safety of consumers.

(5) The term established business relationship for purposes of telephone solicitations means a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a residential subscriber with or without an exchange of consideration, on the basis of the subscriber's purchase or transaction with the entity within the eighteen (18) months immediately preceding the date of the telephone call or on the basis of the subscriber's inquiry or application regarding products or services offered by the entity within the three months immediately preceding the date of the call, which relationship has not been previously terminated by either party.

(i) The subscriber's seller-specific do-not-call request, as set forth in paragraph (d)(3) of this section, terminates an established business relationship for purposes of telemarketing and telephone solicitation even if the subscriber continues to do business with the seller.

(ii) The subscriber's established business relationship with a particular business entity does not extend to affiliated entities unless the subscriber would reasonably expect them to be included given the nature and type of goods or services offered by the affiliate and the identity of the affiliate.

(6) The term established business relationship for purposes of paragraph (a)(4) of this section on the sending of facsimile advertisements means a prior or existing relationship formed by a voluntary two-way communication between a person or entity and a business or residential subscriber with or without an exchange of consideration, on the basis of an inquiry, application, purchase or transaction by the business or residential subscriber regarding products or services offered by such person or entity,

which relationship has not been previously terminated by either party.

(7) The term facsimile broadcaster means a person or entity that transmits messages to telephone facsimile machines on behalf of another person or entity for a fee.

(8) The term one-ring scam means a scam in which a caller makes a call and allows the call to ring the called party for a short duration, in order to prompt the called party to return the call, thereby subjecting the called party to charges.

(9) The term prior express written consent means an agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.

(i) The written agreement shall include a clear and conspicuous disclosure informing the person signing that:

(A) By executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice; and

(B) The person is not required to sign the agreement (directly or indirectly), or agree to enter into such an agreement as a condition of purchasing any property, goods, or services.

(ii) The term “signature” shall include an electronic or digital form of signature, to the extent that such form of signature is recognized as a valid signature under applicable federal law or state contract law.

(10) The term seller means the person or entity on whose behalf a telephone call or message is initiated for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person.

(11) The term sender for purposes of paragraph (a)(4) of this section means the person or entity on whose behalf a facsimile unsolicited advertisement is sent or whose goods or services are advertised or promoted in the unsolicited advertisement.

(12) The term telemarketer means the person or entity that initiates a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person.

(13) The term telemarketing means the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person.

(14) The term telephone facsimile machine means equipment which has the capacity to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

(15) The term telephone solicitation means the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person, but such term does not include a call or message:

(i) To any person with that person's prior express invitation or permission;

(ii) To any person with whom the caller has an established business relationship; or

(iii) By or on behalf of a tax-exempt nonprofit organization.

(16) The term unsolicited advertisement means any material advertising the commercial availability or quality of any property, goods, or services which is transmitted to any person without that person's prior express invitation or permission, in writing or otherwise.

(17) The term personal relationship means any family member, friend, or acquaintance of the telemarketer making the call.

(18) The term effectively mitigate means identifying the source of the traffic and preventing that source from continuing to originate traffic of the same or similar nature.

(19) The term gateway provider means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. For purposes of this paragraph (f)(19):

(i) U.S.-based means that the provider has facilities located in the United States, including a point of presence capable of processing the call; and

(ii) Receives a call directly from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

(g) Beginning January 1, 2004, common carriers shall:

(1) When providing local exchange service, provide an annual notice, via an insert in the subscriber's bill, of the right to give or revoke a notification of an objection to receiving telephone solicitations pursuant to the national do-not-call database maintained by the federal government and the methods by which such rights may be exercised by the subscriber. The notice must be clear and conspicuous and include, at a minimum, the Internet address and toll-free number that residential telephone subscribers may use to register on the national database.

(2) When providing service to any person or entity for the purpose of making telephone solicitations, make a one-time notification to such person or entity of the national do-not-call requirements, including, at a minimum, citation to 47 CFR 64.1200 and 16 CFR 310. Failure to receive such notification will not serve as a defense to any person or entity making telephone solicitations from violations of this section.

(h) The administrator of the national do-not-call registry that is maintained by the federal government shall make the telephone numbers in the database available to the States so that a State may use the telephone numbers that relate to such State as part of any database, list or listing system maintained by such State for the regulation of telephone solicitations.

(i)-(j) [Reserved]

(k) Voice service providers may block calls so that they do not reach a called party as follows:

(1) A provider may block a voice call when the subscriber to which the originating number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only.

(2) A provider may block a voice call purporting to originate from any of the following:

(i) A North American Numbering Plan number that is not valid;

(ii) A valid North American Numbering Plan number that is not allocated to a provider by the North American Numbering Plan Administrator or the Pooling Administrator; and

(iii) A valid North American Numbering Plan number that is allocated to a provider by the North American Numbering Plan Administrator or Pooling Administrator, but is unused, so long as the provider blocking the calls is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of the blocking.

(iv) A telephone number that the provider identifies, based on reasonable analytics, as highly likely to be associated with a one-ring scam.

(3) A terminating provider may block a voice call without liability under the Communications Act or the Commission's rules where:

(i) Calls are blocked based on the use of reasonable analytics designed to identify unwanted calls;

(ii) Those analytics include consideration of caller ID authentication information where available;

(iii) A consumer may opt out of blocking and is provided with sufficient information to make an informed decision;

(iv) All analytics are applied in a non-discriminatory, competitively neutral manner;

(v) Blocking services are provided with no additional line-item charge to consumers; and

(vi) The terminating provider provides, without charge to the caller, the redress requirements set forth in paragraph (k)(8) of this section.

(4) A provider may block voice calls or cease to accept traffic from an originating or intermediate provider without liability under the Communications Act or the Commission's rules where the originating or intermediate provider, when notified by the Commission, fails to effectively mitigate illegal traffic within 48 hours or fails to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls. Prior to initiating blocking, the provider shall provide the Commission with notice and a brief summary of the basis for its determination that the originating or intermediate provider meets one or more of these two conditions for blocking.

(5) A provider may not block a voice call under paragraphs (k)(1) through (4), paragraph (k)(11), paragraphs (n)(2) and (3), paragraph (n)(5), or paragraph (o) of this section if the call is an emergency call placed to 911.

(6) When blocking consistent with paragraphs (k)(1) through (4), paragraph (k)(11), paragraphs (n)(2) and (3), paragraph (n)(5), or paragraph (o) of this section, a provider must make all reasonable efforts to ensure that calls from public safety answering points and government emergency numbers are not blocked.

(7) For purposes of this section, a provider may rely on Caller ID information to determine the purported originating number without regard to whether the call, in fact originated from that number.

(8) Each terminating provider that blocks calls pursuant to this section or utilizes caller ID authentication information in determining how to deliver calls must provide a single point of contact, readily available on the terminating provider's public-facing website, for receiving call blocking error complaints and verifying the authenticity of the calls of a calling party that is adversely affected by information provided by caller ID authentication. The terminating provider must resolve disputes pertaining to caller ID authentication information within a reasonable time and, at a minimum, provide a status update within 24 hours. When a caller makes a credible claim of erroneous blocking and the terminating provider determines that the calls should not have been blocked, or the call delivery decision is not appropriate, the terminating provider must promptly cease the call treatment for that number unless circumstances change. The terminating provider may not impose any charge on callers for reporting, investigating, or resolving either category of complaints, so long as the complaint is made in good faith.

(9) Any terminating provider that blocks calls based on any analytics program, either itself or through a third-party blocking service, must immediately return, and all voice service providers in the call path must transmit, an appropriate response code to the origination point of the call. For purposes of this rule, an appropriate response code is:

(i) In the case of a call terminating on an IP network, the use of Session Initiation Protocol (SIP) code 603+, as defined in ATIS-1000099, adopted August 16, 2022;

(ii) In the case of a call terminating on a non-IP network, the use of ISDN User Part (ISUP) code 21 with the cause location “user”;

(iii) In the case of a code transmitting from an IP network to a non-IP network, SIP code 603+ must map to ISUP code 21; and

(iv) In the case of a code transmitting from a non-IP network to an IP network, ISUP code 21 must map to SIP code 603 or 603+ where the cause location is “user.”

(10) Any terminating provider that blocks calls pursuant to an opt-out or opt-in analytics program, either itself or through a third-party blocking service, must provide, at the request of the subscriber to a number, at no additional charge and within 3 business days of such a request, a list of calls to that number, including the date and time of the call and the calling number, that the terminating provider or its designee blocked pursuant to such analytics program within the 28 days prior to the request.

(11) A terminating provider may block calls without liability under the Communications Act and the Commission's rules, without giving consumers the opportunity to opt out of such blocking, so long as:

(i) The provider reasonably determines, based on reasonable analytics that include consideration of caller ID authentication information where available, that calls are part of a particular call pattern that is highly likely to be illegal;

(ii) The provider manages its network-based blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that the particular call pattern is highly likely to be illegal before initiating blocking of calls that are part of that pattern;

(iii) The provider ceases blocking calls that are part of the call pattern as soon as the provider has actual knowledge that the blocked calls are likely lawful;

(iv) The provider discloses to consumers that it is engaging in such blocking;

(v) All analytics are applied in a non-discriminatory, competitively neutral manner;

(vi) Blocking services are provided with no additional line-item charge to consumers; and

(vii) The terminating provider provides, without line item charge to the caller, the redress requirements set forth in subparagraphs 8 and 9.

(l) A reporting carrier subject to § 52.15(f) of this title shall:

(1) Maintain records of the most recent date each North American Numbering Plan (NANP) telephone number allocated or ported to the reporting carrier was permanently disconnected.

(2) Beginning on the 15th day of the month after the Consumer and Governmental Affairs Bureau announces that the Administrator is ready to begin accepting these reports and on the 15th day of each month thereafter, report to the Administrator the most recent date each NANP telephone number allocated to or ported to it was permanently disconnected.

(3) For purposes of this paragraph (l), a NANP telephone number has been permanently disconnected when a subscriber permanently has relinquished the number, or the provider permanently has reversed its assignment of the number to the subscriber such that the number has been disassociated with the subscriber. A NANP telephone number that is ported to another provider is not permanently disconnected.

(4) Reporting carriers serving 100,000 or fewer domestic retail subscriber lines as reported on their most recent Forms 477, aggregated over all the providers' affiliates, must begin keeping the records required by paragraph (l)(1) of this section six months after the effective date for large providers and must begin filing the reports required by paragraph (l)(2) of this section no later than the 15th day of the month that is six months after the date announced by the Consumer and Governmental Affairs Bureau pursuant to paragraph (l)(2).

(m) A person will not be liable for violating the prohibitions in paragraph (a)(1), (2), or (3) of this section by making a call to a number for which the person previously had obtained prior express consent of the called party as required in paragraph (a)(1), (2), or (3) but at the time of the call, the number is not assigned to the subscriber to whom it was assigned at the time such prior express consent was obtained if the person, bearing the burden of proof and persuasion, demonstrates that:

(1) The person, based upon the most recent numbering information reported to the Administrator pursuant to paragraph (l) of this section, by querying the database operated by the Administrator and receiving a response of “no”, has verified that the number has not been permanently disconnected since the date prior express consent was obtained as required in paragraph (a)(1), (2), or (3) of

this section; and

(2) The person's call to the number was the result of the database erroneously returning a response of “no” to the person's query consisting of the number for which prior express consent was obtained as required in paragraph (a)(1), (2), or (3) of this section and the date on which such prior express consent was obtained.

(n) A voice service provider must:

(1) Upon receipt of a traceback request from the Commission, civil law enforcement, criminal law enforcement, or the industry traceback consortium, the provider must fully respond to the traceback request within 24 hours of receipt of the request. The 24-hour clock does not start outside of business hours, and requests received during that time are deemed received at 8 a.m. on the next business day. If the 24-hour response period would end on a non-business day, either a weekend or a Federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. For example, a request received at 3 p.m. on a Friday will be due at 3 p.m. on the following Monday, assuming that Monday is not a Federal legal holiday. For purposes of this paragraph (n)(1), business day is defined as Monday through Friday, excluding Federal legal holidays, and business hours is defined as 8 a.m. to 5:30 p.m. on a business day. For purposes of this paragraph (n)(1), all times are local time for the office that is required to respond to the request.

(2) Upon receipt of a Notice of Suspected Illegal Traffic from the Commission through its Enforcement Bureau, take the applicable actions with respect to the identified traffic described in paragraphs (n)(2)(i) through (iii) of this section. The provider will not be held liable under the Communications Act or the Commission's rules in this chapter for providers that inadvertently block lawful traffic as part of the requirement to block substantially similar traffic so long as it is blocking consistent with the requirements of paragraphs (n)(2)(i) through (iii). For purposes of this paragraph (n)(2), identified traffic means the illegal traffic identified in the Notification of Suspected Illegal Traffic issued by the Enforcement Bureau. The following procedures shall apply:

(i)(A) The Enforcement Bureau will issue a Notification of Suspected Illegal Traffic that identifies with as much particularity as possible the suspected illegal traffic; provides the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful; cites the statutory or regulatory provisions the identified traffic appears to violate; and directs the provider receiving the notice that it must comply with this section. The Enforcement Bureau's Notification of Suspected Illegal Traffic shall give the identified provider a minimum of 14 days to comply with the notice. Each notified provider must promptly investigate the identified traffic and report the results of that investigation to the Enforcement Bureau within the timeframe specified in the Notification of Suspected Illegal Traffic. If the provider's investigation determines that it served as the gateway or originating provider for the identified traffic, it must block or cease accepting the identified traffic and substantially similar traffic on an ongoing basis within the timeframe specified in the Notification of Suspected Illegal Traffic. The provider must include in its report to the Enforcement Bureau:

(1) A certification that it is blocking the identified traffic and will continue to do so; and

(2) A description of its plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.

(B) If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or if the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal. If the notified provider determines during this investigation that it did not serve as the gateway provider or originating provider for any of the identified traffic, it shall provide an explanation as to how it reached that conclusion and, if it is a non-gateway intermediate or terminating provider for the identified traffic, it must identify the upstream provider(s) from which it received the identified traffic and, if possible, take lawful steps to mitigate this traffic. If the Enforcement Bureau finds that an approved plan is not blocking substantially similar traffic, the identified provider shall modify its plan to block such traffic. If the Enforcement Bureau finds that the identified provider continues to allow suspected illegal traffic onto the U.S. network, it may proceed under paragraph (n)(2)(ii) or (iii) of this section, as appropriate.

(ii) If the provider fails to respond to the Notification of Suspected Illegal Traffic, the Enforcement Bureau determines that the response is insufficient, the Enforcement Bureau determines that the provider is continuing to originate substantially similar traffic or allow substantially similar traffic onto the U.S. network after the timeframe specified in the Notification of Suspected Illegal Traffic, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the

Enforcement Bureau shall issue an Initial Determination Order to the provider stating the Bureau's initial determination that the provider is not in compliance with this section. The Initial Determination Order shall include the Enforcement Bureau's reasoning for its determination and give the provider a minimum of 14 days to provide a final response prior to the Enforcement Bureau making a final determination on whether the provider is in compliance with this section.

(iii) If the provider does not provide an adequate response to the Initial Determination Order within the timeframe permitted in that Order or continues to originate substantially similar traffic onto the U.S. network, the Enforcement Bureau shall issue a Final Determination Order finding that the provider is not in compliance with this section. The Final Determination Orders shall be published in EB Docket No. 22-174 at https://www.fcc.gov/ecfs/search/search-filings. A Final Determination Order may be issued up to one year after the release date of the Initial Determination Order, and may be based on either an immediate failure to comply with this section or a determination that the provider has failed to meet its ongoing obligation under this section to block substantially similar traffic.

(3) When notified by the Commission through its Enforcement Bureau that a Final Determination Order has been issued finding that an upstream provider has failed to comply with paragraph (n)(2) of this section, block and cease accepting all traffic received directly from the upstream provider beginning 30 days after the release date of the Final Determination Order. This paragraph (n)(3) applies to any provider immediately downstream from the upstream provider. The Enforcement Bureau shall provide notification by publishing the Final Determination Order in EB Docket No. 22-174 at https://www.fcc.gov/ecfs/search/search-filings. Providers must monitor EB Docket No. 22-174 and initiate blocking no later than 30 days from the release date of the Final Determination Order. A provider that chooses to initiate blocking sooner than 30 days from the release date may do so consistent with paragraph (k)(4) of this section.

(4) Take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.

(5) Take reasonable and effective steps to ensure that any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network.

(o) A voice service provider must block any calls purporting to originate from a number on a reasonable do-not-originate list. A list so limited in scope that it leaves out obvious numbers that could be included with little effort may be deemed unreasonable. The do-not-originate list may include only:

(1) Numbers for which the subscriber to the number has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only;

(2) North American Numbering Plan numbers that are not valid;

(3) Valid North American Numbering Plan Numbers that are not allocated to a provider by the North American Numbering Plan Administrator; and

(4) Valid North American Numbering Plan numbers that are allocated to a provider by the North American Numbering Plan Administrator, but are unused, so long as the provider blocking the calls is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of blocking.

(p) A mobile wireless provider must block a text message purporting to originate from a North American Numbering Plan number on a reasonable do-not-originate list. A list so limited in scope that it leaves out obvious North American Numbering Plan numbers that could be included with little effort may be deemed unreasonable. The do-not-originate list may include only:

(1) North American Numbering Plan Numbers for which the subscriber to the number has requested that texts purporting to originate from that number be blocked;

(2) North American Numbering Plan numbers that are not valid;

(3) Valid North American Numbering Plan numbers that are not allocated to a provider by the North American Numbering Plan Administrator; and

(4) Valid North American Numbering Plan numbers that are allocated to a provider by the North American Numbering Plan Administrator, but are unused, so long as the provider blocking the message is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of blocking.

(q) [Reserved]

(r) A mobile wireless provider must provide a point of contact or ensure its aggregator partners or blocking contractors that block text messages on its network provide a point of contact to resolve complaints about erroneous blocking from message senders that can document that their messages have been blocked. Such point of contact may be the same point of contact for voice call blocking error complaints.

(s) A terminating mobile wireless provider must, upon receipt of a Notification of Illegal Texts from the Commission through its Enforcement Bureau, take the actions described in this paragraph (s), including, when required, blocking all texts from the identified number or numbers. The Enforcement Bureau will issue a Notification of Illegal Texts that identifies the number(s) used and the date(s) the texts were sent or received; provides the basis for the Enforcement Bureau's determination that the identified texts are unlawful; cites the statutory or regulatory provisions the identified texts violate; directs the provider receiving the notice that it must comply with this section; and provide a point of contact to be used by a subscriber to a listed number to dispute blocking. The Enforcement Bureau's Notification of Illegal Texts shall give the identified provider a reasonable amount of time to comply with the notice. The Enforcement Bureau shall make the Notification of Illegal Texts available in EB Docket No. 23-418 at https://www.fcc.gov/ecfs/search/search-filings. The provider must include a certification that it is blocking all texts from the number or numbers and will continue to do so unless the provider learns that the number has been reassigned, in which case the provider shall promptly notify the Enforcement Bureau of this fact and include any information it has obtained that demonstrates that the number has been reassigned. If, at any time in the future, the provider determines that the number has been reassigned, it shall notify the Enforcement Bureau and cease blocking. The provider is not required to monitor for number reassignments.

[68 FR 44177, July 25, 2003, as amended at 68 FR 59131, Oct. 14, 2003; 69 FR 60316, Oct. 8, 2004; 70 FR 19337, Apr. 13, 2005; 71 FR 25977, May 3, 2006; 71 FR 56893, Sept. 28, 2006; 71 FR 75122, Dec. 14, 2006; 73 FR 40185, July 14, 2008; 77 FR 34246, June 11, 2012; 83 FR 1577, Jan. 12, 2018; 84 FR 10267, Mar. 20, 2019; 84 FR 11232, Mar. 26, 2019; 85 FR 56534, Sept. 14, 2020; 86 FR 2563, Jan. 13, 2021; 86 FR 11447, 11448, Feb. 25, 2021; 86 FR 17734,17735, Apr. 6, 2021; 86 FR 74375, Dec. 30, 2021; 87 FR 7044, Feb. 8, 2022; 87 FR 42944, July 18, 2022; 87 FR 51921, Aug. 24, 2022; 87 FR 69207, Nov. 18, 2022; 88 FR 3677, Jan. 20, 2023; 88 FR 21500, Apr. 11, 2023; 88 FR 43458, July 10, 2023; 89 FR 5104, Jan. 26, 2024; 89 FR 15062, Mar. 1, 2024; 89 FR 15762, Mar. 5, 2024; 89 FR 5104, Jan. 26, 2024; 89 FR 87983, Nov. 6, 2024; 89 FR 5105, Jan. 26, 2024; 89 FR 15762, Mar. 5, 2024; 89 FR 17762, Mar. 12, 2024; 90 FR 13425, Mar. 24, 2025; 90 FR 42138, Aug. 29, 2025]