This content is from the eCFR and is authoritative but unofficial.

Displaying title 45, up to date as of 9/26/2024. Title 45 was last amended 9/23/2024.

Title 45 —Public Welfare
Subtitle A —Department of Health and Human Services
Subchapter C —Administrative Data Standards and Related Requirements
Part 164 —Security and Privacy
Subpart E —Privacy of Individually Identifiable Health Information

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

(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;

Exhibit 2006
Datavant v. Vigilytics
IPR2024-00382

(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]