

Table of Contents

HIPAA Privacy Policy pages 2 to 15

Exhibit A – HIPAA Privacy Regulations pages A-1 to A-137

Exhibit B – Notice of Privacy Practices pages B-1 to B-5

Exhibit C – Business Associate Agreement pages C-1 to C-5

Exhibit D – List of classes of employees with access to PHI pages D-1 to D-2

HIPAA Privacy Policy for Optical Labs

**A. Introduction**

This Privacy Policy of *(replace this with your company name)* (the “Lab”) is implemented by the Lab for the purpose of complying with the Standards for the Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, Subparts A and E ("Privacy Rule"). In particular, this policy documents how the Lab will treat Protected Health Information (as defined below) in compliance with HIPAA Privacy Rule, and will otherwise comply with the Privacy Rule. This policy applies to all business locations operated by the Lab. A copy of the HIPAA Privacy Rule is attached hereto at Exhibit A.

**B. Privacy Official**

The Privacy Official designated by the Lab as the person responsible for development and implementation of this Privacy Policy is (*replace this with the name or title of designated Privacy Official*).

**C. Contact Person OR OFFICE**

The Contact Person or Office designated by the Lab as the person responsible for receiving complaints concerning this policy and for providing further information about matters covered by this Privacy Policy is (*replace this with the name or title of designated Contact Person or Office*).

**D. NOTICE OF PRIVACY PRACTICES**

The Notice of Privacy Practices for the Lab is attached hereto at Exhibit B. The Notice of Privacy Practices shall be provided to any person upon request. In addition, the Notice of Privacy Practices shall be posted prominently on any Web site maintained by the Lab which Web site provides information about the Lab’s customer services or benefits.[[1]](#footnote-2)\*

**E. Protected Health Information (“PHI”)**

“Protected Health Information” ("PHI") includes any information that is created or received by the Lab in its role as a health care provider relating to past, present or future physical or mental health or condition of an individual, provision of health care, and/or future payment for the provision of health care and that identifies the individual or with respect to which there is a reasonable basis to believe that it could be used to identify the individual. PHI does not include employment records held by a Lab in its role as an employer.

PHI would include any information which relates to eyeglasses or the provision of eye care, from which one might reasonably identify the individual who is the subject of such eye care. While it is unlikely that an optical lab would receive any information other than an individual’s name, the range of possible PHI information includes the following:

* Medical information.
* Billing information.
* Financial information.
* Patient’s names.
* Patient addresses which include geographic subdivisions smaller than a state [including street address, city, county, precinct, certain zip codes . . . *See* 45 CFR § 164.514(b)(2) at Exhibit A hereto].
* All elements of dates (except for year) for dates related to the patient, including birth date, treatment date, and all elements of dates indicative of an age over 89.
* Telephone numbers.
* Fax numbers.
* E-mail addresses.
* Social security numbers.
* Medical record numbers.
* Health plan beneficiary numbers.
* Account numbers.
* Certificates/license numbers.
* Vehicle identifiers and serial numbers, including license plate numbers.
* Device identifiers and serial numbers.
* Web site URLs.
* Internet protocol (IP) address numbers.
* Biometric identifiers including finger and voice prints.
* Full face photographic images.
* Any other unique identifying number, characteristic or code.

If health information is stripped of all of the above-described individual identifiers in accordance with 45 CFR § 164.514(b), and the Lab has no actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual who is the subject of the information, then the information does not constitute PHI. For example, a listing of eyeglasses prescriptions, or lens or frame types, without any other information, may not constitute PHI.

**F. Allowed Use/Disclosure/Request of PHI by the Lab**

The Lab and its employees may only use, disclose or request PHI as expressly allowed in this policy.

1. Disclosure to the Patient – The Lab may disclose PHI about a patient to that patient upon request of the patient, without regard to the “Minimum Necessary” requirements described at Section G below.

2. Treatment Operations

a. Use within the Lab – The Lab may use among its personnel, as part of its treatment operations. Treatment operations include the provision, coordination and management of the eyeglass services provided by the Lab. Such use and disclosure is subject to the “Minimum Necessary” requirements described at Section G below. For example, it is permissible that employees identified by Lab as having a reasonable need to do so, use and see PHI as part of their processing of orders, since the Lab has under Section G below, identified those class(es) of employees using PHI who have a reasonable need to do so, and has limited the amount of PHI which they use to that which they have a reasonable need to use.

b. Disclosures made to Other Health Care Providers for their Treatment Activities – The Lab may disclose PHI to other health care providers (e.g., eye care professionals, or coating labs) for their treatment activities. Such a disclosure by the Lab to another health care provider for its treatment activities is not subject to the Minimum Necessary rules described at Section G below.

3. As Part of Payment Operations – The Lab may disclose PHI to another health care provider (e.g., eye care professionals) or vision plan in order to receive payment from such entity. Such use and disclosure of PHI as part of an invoice or other payment activity is subject to the “Minimum Necessary” rules described at Section G below.

4. Health Care Operations – The Lab may use or disclose PHI as part of its health care operations. Health care operations include conducting quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, and conducting or arranging for medical review, legal services, and auditing functions. The Lab may also disclose PHI to other health care providers for health care operations activities of the entity that receives the information if: (1) the entity either has or had a relationship with the individual who is the subject of the PHI being requested, (2) the PHI pertains to such relationship, and (3) the purpose of the disclosure is for (i), conducting quality assessment and improvement activities (ii) reviewing the competence or qualifications of health care professionals, or (iii) health care fraud and abuse detection or compliance (See 45 C.F.R. § 164.506 for additional explanation). Such uses and disclosures of PHI as part of an invoice or other payment activity are subject to the “Minimum Necessary” rules described at Section G below.

5. To Business Associates – A Business Associate is a person or organization that performs a function or activity involving the use or disclosure of PHI on behalf of the Lab, but is not a part of the Lab’s workforce. The Lab may disclose PHI to a Business Associate if the Lab obtains satisfactory assurances from the Business Associate that it will appropriately safeguard the information. The Business Associate will sign a Business Associate Agreement stating that the Business Associate will not use or disclose PHI in any manner that would not be permissible under the Privacy Rule or the Business Associate Agreement (*See* Exhibit C). The Business Associate functions which trigger this rule typically involve contractors who assist with claims processing or administration, data analysis, quality assurance, billing, legal, or accounting. **Importantly, Business Associates do not include the Lab’s employees, and even more importantly, the requirement to have Business Associates sign a Business Associate Agreement does not apply where a Lab discloses PHI to a health care provider for treatment of the patient, or where the Lab provides payment information to a vision plan**. For example, if the Lab provides PHI to an eye care professional in connection with fulfilling an order or to a coating lab to enable the coating lab to provide coating services, the Lab does not need to have the eye care professional or the coating lab sign a Business Associate Agreement. If the Lab makes payment claims to a vision plan by electronic direct data entry or standard transaction entry to a third party clearinghouse, the Lab does not need a Business Associate Agreement with the clearinghouse. If the Lab uses a third party clearinghouse to obtain PHI electronically from eye care professional customers, the Lab does not need a Business Associate Agreement with the clearinghouse. However, if the Lab uses a third party entity to provide software support, and that third party may access the Lab’s computer system and PHI contained therein, and may even receive and analyze backup tapes with PHI, that third party will be a Business Associate of the Lab, and the Lab will have to require that third party to sign a Business Associate Agreement. In such a case, or in another event that the Lab provides PHI to a Business Associate in a situation which triggers the requirement for a Business Associate Agreement (e.g., the Business Associate will be performing for the lab claims processing administration, data analysis, billing, legal or accounting services), the prior written approval of the Lab Privacy Official shall be obtained, and the Lab Privacy Official shall have the Business Associate sign the Business Associate Agreement at Exhibit C hereto as are deemed necessary and appropriate.

5. Other Uses – The HIPAA Privacy Rule allows uses and disclosures of PHI in specified situations other than those listed in Section F (1-5) above. For example, uses and disclosures of PHI are allowed in the following situations:

1. Uses and disclosures required by law
2. Uses and disclosures made pursuant to an individual authorization. An authorization is required for most uses and disclosures of PHI for marketing purposes, and when a use or disclosure of PHI constitutes a sale of PHI.
3. Disclosures to the Secretary of the Department of Health and Human Services for enforcement purposes

Before a Lab employee makes a use or disclosure PHI not listed in Section F (1-5) above, he/she must provide a written memo to the Lab Privacy Official explaining why it is necessary to use or disclose such PHI. Such uses and disclosures may only be made after receiving written approval from the Lab Privacy Official in response to such memo. If necessary, the memo must also explain why the proposed disclosure is disclosing the minimum amount of PHI necessary (*See* Section G). For uses and disclosure which require an authorization, the Privacy Official may only provide such approval after obtaining the authorization.

**G. Using/Disclosing or Requesting PHI – Assuring Minimum Disclosure Necessary**

1. Persons Accessing PHI – The Lab has identified at Exhibit D hereto those classes of lab employees who have a reasonable need to have access to PHI in order to carry out their duties, and for each such class of employees the types of PHI to which they need access. Those classes of employees listed in Exhibit D may use PHI within the Lab as is reasonably incident to the performance of their work. Disclosure by such employees of PHI to persons outside the Lab are governed by Section G (2) below.

2. Routine Disclosures of PHI – Set forth below are the disclosures of PHI which will be made on a routine and recurring basis by the Lab, and the procedures which will be followed to limit the PHI so disclosed to the minimum amount reasonably necessary to achieve the purpose of disclosure.

a. Disclosure of PHI to Health Care Providers (eye care professionals or coating labs) as part of their Treatment Operations – For example: (i) telephone inquiries concerning services requested, or the status or details of performance of such services; (ii) delivery of eyeglasses to eye care professionals, along with PHI - such disclosures, if part of a request for treatment, are not subject to the Minimum Necessary requirements;

b. PHI Disclosed as part of Payment Operations – Invoice to health care provider (eye care professionals) or vision plan – Provide no more PHI in invoice to health care provider or vision plan than is requested by health care provider or vision plan, or that the Lab can demonstrate is reasonably necessary. Payment claims submitted electronically to vision plans which are compliant with the HIPAA Electronic Transaction Standards are considered to disclose only the minimum PHI necessary.

c. Other Routine and Recurring Disclosures of PHI

(i) Warranty/Return Claims - disclosure of PHI to a lens manufacturer to support a request for refund or replacement lens due to customer rejection may require a patient authorization. To avoid having to obtain such a patient authorization, the Lab must de-identify the PHI provided to the lens manufacturer in accordance with 45 CFR § 164.514(b) (for example, provide only the manufacturer's invoice number or the Lab’s invoice number covering the rejected lens, provided that this information, alone or with the rejected lens, cannot be used to identify the individual).

3. Non-Routine Disclosures – Before a Lab employee makes any non-routine or non-recurring disclosure of PHI [i.e., a disclosure of PHI other than one described in Section G (2) above], he/she must provide a written memo to the Lab Privacy Official explaining why it is necessary to disclose such PHI, and why the proposed disclosure is disclosing the minimum amount of PHI necessary. Such non-routine disclosure may only be made after receiving written approval from the Lab Privacy Official in response to such memo.

4. Routine Requests - Any Routine Request by the Lab for PHI shall be limited to that PHI which is reasonably necessary to accomplish the purpose of the request. The Lab anticipates making the following typical requests for PHI on a routine and recurring basis, and in such situations the PHI requested should be limited to that noted below in order to limit the amount of PHI requested to that amount reasonably necessary to accomplish the purpose for which the request is made:

a. Request by the Lab of eye care professional for PHI in connection with processing and for fulfilling an order is a request in connection with treatment which may be made, and which is not subject to “Minimum Necessary” requirements of this Section G. The fact that the information may be obtained through a third party clearinghouse does not change this fact.

5. Non-Routine Requests - Any request made by the Lab for PHI other than a routine request listed under Section G (4) above, may only be made after providing to the Lab Privacy Official a written memo describing the need for the request, and why the request is limited to the minimum amount of PHI reasonably necessary to accomplish the purpose of the request, and after the Lab Privacy Official has, in response to such memo, approved in writing the making of such request.

**H. Safeguards**

The Lab has the following administrative, technical and physical safeguards to protect PHI in its possession:

1. Training of all Lab employees as described in Section I below governing this Privacy Policy and HIPAA Privacy Rule requirements.

2. Limitation of the number of employees as set forth in Exhibit D hereto having access to PHI, to the minimum number reasonably necessary.

3. It is Lab policy to prevent any unnecessary copying of PHI, and to limit those who may copy PHI to those individuals noted at Exhibit D hereto as having the need to copy PHI. All copies of PHI shall be safeguarded from any unintentional use or disclosure that is a violation of the Privacy Rule.

4. Storage, safekeeping, and disposal - when employees have completed use of PHI, including copies of PHI, it shall be placed and kept in an identified storage area to which only employees in classes listed in Exhibit D hereto have access. Where feasible, discarded information containing PHI shall be shredded or otherwise rendered unreadable.

**I.** **Training**

1. All employees of the Lab will be trained on HIPAA Privacy Policy Compliance within a reasonable period of time, not to exceed two weeks, after a person joins the workforce.

1. All employees shall be provided access to this Privacy Policy no later than three days before their training date*,* and shall participate in training with the Lab Privacy Official or an individual designated by the Lab Privacy Official, to gain an understanding of this Privacy Policy and to answer any questions which the employee may have concerning such policy.
2. All employees having gone through such training, will sign a simple document acknowledging that they have been so trained, and the Lab Privacy Official shall retain the original of all such signed acknowledgments of training.

4. All employees shall be provided copies within one week of any amendments to this Privacy Policy, and those employees' whose duties are materially affected by the amendments shall be trained in those amendments.

**J. Process for Handling Complaints**

1. Any person having a complaint concerning the Lab’s Privacy Policy and procedures or the Lab’s compliance with this policy or the Privacy Rule shall submit that complaint in writing to the Privacy Contact Person or Office designated pursuant to Section C above.

2. The Lab Privacy Contact Person or Office shall respond to such complaint in writing within two weeks if feasible, and in no event later than 30 days, setting forth any remedial action taken in response to such complaint, or explaining why no remedial action is justified. The Lab Privacy Official shall retain copies of all complaints so filed and all responses to such complaints.

**K. Sanctions**

1. Lab employees who fail to comply with this Privacy Policy shall be subject to sanctions, after an opportunity to meet with the Privacy Official and explain the reason for their failure to comply:

a. First Offense, Non-willful – Attend refresher training course within two months.

b. First Offense, Willful – Attend refresher training course within two months. Additional sanctions ranging from letter of reprimand in personnel file to termination, based upon severity of offense.

c. Subsequent Violations – Combination of required attendance at refresher training course and possible employee discipline ranging from letter of reprimand in file to termination of employment, based upon the number of previous violations, presence or lack of willfulness and other mitigating or aggravating circumstances.

d. Each instance of workforce disciplinary action regarding the privacy of PHI is to be documented in a written or electronic record by the Privacy Official. The Sanctions log will contain the following information:

i. Name of employee

ii. Description of the violation

iii. Level of breach or violation

iv. Location of breach of violation

v. Date and time of breach or violation

vi. Disciplinary action taken

This documentation must be retained for six years from the date of its creation or the date when it was last in effect, whichever is later.

**L. TERMINATION**

When an employee (or other member of the workforce) of the Lab leaves or is terminated, both physical and electronic access to PHI will be denied. The Lab will use appropriate safeguards to protect the privacy of PHI when an employee (or other member of the workforce) of the Lab leaves or is terminated.

**M. Mitigation**

In the event that any Lab employee becomes aware of a violation of this Privacy Policy or the Privacy Rule, the employee shall immediately notify the Lab Privacy Official in writing of the nature, cause and extent of the violation. The Lab Privacy Official shall take all reasonable measures to mitigate, to the extent practicable, any harmful effect that is known to the Lab of a use or disclosure of PHI in violation of this Privacy Policy or the Privacy Rule. The Lab Privacy Official shall take all reasonable measures to undo, or if not possible to undo, then to minimize, the future use or disclosure of the PHI involved, and to correct the Privacy Policy procedures to avoid repetition of such violations. Employees and others who are working on behalf of the Lab, who report, in good faith, violations of this Privacy Policy or the Privacy Rule shall not be retaliated against.

**n. No Retaliation**

It is the absolute policy of the Lab not to intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against any individual for the exercise by the individual of any rights under this Privacy Policy or under HIPAA or for filing any complaint with HHS, or testifying, assisting or participating in any HHS investigation, compliance review, proceeding or hearing concerning HIPAA, or opposing any action which violates HIPAA, provided that such opposition has been taken in good faith, and the manner of such opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

**o. No Waiver**

The Lab shall not require any individuals to waive their rights to file complaints to HHS alleging non-compliance of the Lab with HIPAA, as a condition of their receiving services from the Lab.

**p. Rights of Patients to Request Privacy Protection for PHI**

1. Although the Lab does not anticipate that it will receive requests from patients to restrict use or disclosure by the Lab of PHI concerning the patient, the Lab shall permit patients to make such requests. The Lab is not required to agree to restrict its use of PHI, except that the Lab must agree not to disclose a patient’s PHI to a health plan if (1) the disclosure is for payment or healthcare operations and is not otherwise required by law, and (2) relates to a health care item or service for which the patient, or another person on the patient’s behalf (other than a health plan) paid the Lab in full. It is the policy of the Lab to give consideration to all requests from patients to restrict the use or disclosure by the Lab of PHI, and to accommodate such requests where in the sole discretion of the Lab it is reasonably feasible and not unduly burdensome to do so.

**q. Right of Patients to Access PHI**

1. Although the Lab does not anticipate that patients will make requests to inspect and obtain copies of PHI concerning them, the Lab recognizes that a patient has the right to inspect and obtain a copy of any PHI which the Lab may possess concerning the patient. Patients also have a right to obtain an electronic copy of PHI that is maintained in any electronic system.

2. It is the policy of the Lab that any such request made by a patient must be made in writing and submitted to the Lab Privacy Official. If the request is for an electronic copy of PHI, the Lab must provide the individual with access to the PHI in the electronic form and format requested by the individual if it is readily producible in such a form and format, or, if not, in a readable electronic form as agreed to by the Lab and the patient . Requests shall be responded to within 30 days in accordance with the requirements of § 164.524(b) (copy attached at Exhibit A hereto).

**r. Amendment of PHI**

1. Although the Lab does not anticipate that patients will make such requests, the Lab recognizes that a patient has the right to have the Lab amend PHI for as long as it is maintained by the Lab. The Lab may deny such a request if: (i) the Lab determines that the PHI which is the subject of the request was not created by the Lab, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment, or (ii) that the PHI would not be available for inspection, (iii) or that the PHI is accurate and complete. The Lab shall respond to such request within 60 days in accordance with § 164.526(b) (copy attached at Exhibit A hereto).

**s. Right to an Accounting of Disclosures of PHI**

1. The patient has the right to receive an accounting of disclosures of PHI made by the Lab in the previous six years, except for disclosures to carry out treatment, payment or health care operations. Note that this excludes disclosures made to eye care professionals for their treatment activities, or to supporting entities such as coating labs for their treatment (i.e., coating) activities, and it excludes disclosures made to eye care professionals and vision plans for payment purposes. The Lab shall respond to a request for an accounting within 60 days and in accordance with § 164.528 (copy attached at Exhibit A hereto).

2. Disclosures and requests for accounting of disclosures will be tracked by the Lab in the Log of PHI Disclosures form that will be maintained in the individual’s file. The Lof will enable to the Lab to provide the individual with the following information regarding the disclosure:

a. Date of the disclosure;

b. The name of the recipient;

c. The address of the recipient, if known;

d. A brief description of the information that was disclosed; and

e. A brief statement of the purpose of the disclosure or a copy of the original request for information.

The Log must be retained for at least six years from the date of its creation or the date when it was last in effect, whichever is later. The Lab Privacy Official is responsible for receiving and processing requests for an accounting.

3. The first accounting requested by the patient within a 12-month period will be free. The Lab may charge the patient a reasonable cost-based fee for providing any additional accounting within a 12-month period. The fee schedule is based on the Lab’s costs for copy supplies and labor costs for preparation of the accounting. The estimated cost for the second accounting within a 12-month period will be calculated prior to preparing the accounting. The Lab will notify the patient of the cost involved prior to preparing the accounting and that they may choose to withdraw or modify their request at that time before any costs are incurred.

**Central Table of Contents/Navigation Point**

**In order to more easily navigate this document, use the** [Go to Central ToC.](#ee)**,** [Go to Part 160 ToC.](#cc)**,** [Go to Part 164 ToC.](#First) **links that are placed after each section heading to return to this central navigation point, or to the tables of contents for Part 160 or Part 164, which are in turn hyperlinked to the text of each section.**

[PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS](#cc)

[PART 164 – SECURITY AND PRIVACY](#First)

**PART 160 – GENERAL ADMINISTRATIVE REQUIREMENTS**

**Subpart A – General Provisions**

[160.101 Statutory basis and purpose.](#Second)

[160.102 Applicability.](#Third)

[160.103 Definitions.](#Fourth)

[160.104 Modifications.](#Fifth)

[160.105 Compliance dates for implementation of new or modified standards and implementation specifications.](#s160105)

**Subpart B – Preemption of State Law**

[160.201 Statutory basis.](#Sixth)

[160.202 Definitions.](#Seventh)

[160.203 General rule and exceptions.](#Eighth)

[160.204 Process for requesting exception determinations.](#Ninth)

[160.205 Duration of effectiveness of exception determinations.](#Tenth)

**Subpart C – Compliance and Enforcement**

[160.300 Applicability.](#a)

[160.302 [Reserved].](#b)

[160.304 Principles for achieving compliance.](#c)

[160.306 Complaints to the Secretary.](#d)

[160.308 Compliance reviews.](#e)

[160.310 Responsibilities of covered entities and business associates](#f)

[160.312 Secretarial action regarding complaints and compliance reviews.](#g)

[160.314 Investigational subpoenas and inquiries.](#s160314)

[160.316 Refraining from intimidation or retaliation.](#s160316)

[PART 164 – SECURITY AND PRIVACY](#PART164)

[164.102 Statutory basis.](#s164102)

[164.103 Definitions](#s164103)

[164.104 Applicability](#S164104)

[164.105 Organizational requirements.](#S164105)

[164.106 Relationship to other parts.](#S164106)

[164.400 Applicability.](#s164400)

[164.402 Definitions.](#s164402)

[164.404 Notification to individuals.](#s164404)

[164.406 Notification to the media.](#S164406)

[164.408 Notification to the Secretary.](#S164408)

[164.410 Notification by a business associate.](#S164410)

[164.412 Law enforcement delay.](#S164412)

[164.414 Administrative requirements and burden of proof.](#S164414)

[164.500 Applicability.](#S164500)

[164.501 Definitions.](#S164501)

[164.502 Uses and disclosures of protected health information: general rules.](#S164502)

[164.504 Uses and disclosures: organizational requirements.](#S164504)

[164.506 Uses and disclosures to carry out treatment, payment, or health care operations.](#S164506)

[164.508 Uses and disclosures for which an authorization is required.](#S164508)

[164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.](#S164510)

[164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.](#S164512)

[164.514 Other requirements relating to uses and disclosures of protected health information.](#S164514)

[164.520 Notice of privacy practices for protected health information.](#S164520)

[164.522 Rights to request privacy protection for protected health information.](#S164522)

[164.524 Access of individuals to protected health information.](#S164524)

[164.526 Amendment of protected health information.](#S164526)

[164.528 Accounting of disclosures of protected health information.](#S164528)

[164.530 Administrative requirements.](#S164530)

[164.532 Transition provisions.](#S164532)

[164.534 Compliance dates for initial implementation of the privacy standards.](#S164534)

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d-1320d-9; sec. 264, Pub. L. 104-191, 110 Stat. 2033-

2034 (42 U.S.C. 1320d-2 (note)); 5 U.S.C. 552; secs. 13400-13424, Pub. L. 111-5, 123 Stat. 258-279;

and sec. 1104 of Pub. L. 111-148, 124 Stat. 146-154.

**Subpart A - General Provisions**

**§ 160.101 Statutory basis and purpose.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

The requirements of this subchapter implement sections 1171 through 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.

**§ 160.102 Applicability.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.).

**§ 160.103 Definitions.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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 (2) 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.

*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.

*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.

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

*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 XVII 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 Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).

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

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

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

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

(xix) 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.

*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, 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 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.

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

*Secretary* means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

*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 claims attachments.

(11) 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 entity or business associate, whether or not they are paid by the covered entity or business associate.

**§ 160.104 Modifications.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.

**§** **160.105 Compliance dates for implementation of new or modified standards and implementation specifications.**  [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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.

**Subpart B - Preemption of State Law**

**§160.201 Statutory Basis.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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.

**§ 160.202 Definitions.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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 Pub.L. 104-191, or sections 13400-13424 of Pub. L. 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.

**§ 160.203 General rule and exceptions.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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.

**§ 160.204 Process for requesting exception determinations.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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.

**Subpart C - Compliance and Enforcement**

**§ 160.300 Applicability.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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 requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

**§ 160.302 [Reserved].** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

**§ 160.304 Principles for achieving compliance.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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 requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(b) Assistance. The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

**§ 160.306 Complaints to the Secretary.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(a) Right to file a complaint. A person who believes a covered entity or business associate is not complying with the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter 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 entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable requirements of this part 160 or the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(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 act and/or omission that are the basis of the complaint.

**§ 160.308 Compliance reviews.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(a) The Secretary will conduct compliance reviews 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.

**§ 160.310 Responsibilities of covered entities and business associates.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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 requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(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 a covered entity or business associate to determine whether it is complying with the applicable requirements of this part 160 and the standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter.

(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 requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter. 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 requirements of this part 160 and the applicable standards, requirements, and implementation specifications of subpart E of part 164 of this subchapter, or if otherwise required by law, or if permitted under 5 U.S.C. 522a(b)(7).

**§ 160.312 Secretarial action regarding complaints and compliance reviews.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(a) Resolution where noncompliance is indicated.

(1) If an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates a failure to comply, the Secretary may so inform the covered entity and, if the matter arose from a complaint, the complainant, in writing and attempt to resolve the matter by informal means whenever possible.

(2) If the Secretary finds the covered entity is not in compliance and determines that the matter cannot be resolved by informal means, the Secretary may issue to the covered entity or business associate and, if the matter arose from a complaint, to the complainant written findings documenting the non-compliance.

(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 no-tice of proposed determination in accordance with § 160.420 of this part.

(b) Resolution when no violation is found. If, after an investigation or compliance review, 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. **§** **160.314 Investigational subpoenas and inquiries.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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 sub-chapter.

PART 164 – SECURITY AND PRIVACY [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

**Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d--1320d-9; sec. 264, Pub. L.104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400--13424, Pub. L. 111-5, 123 Stat. 258-279.**

**§** **164.102 Statutory basis.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

The provisions of this part are adopted pursu-ant 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.

**§** **164.103 Definitions.**  [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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 pro-gram providing public benefits.

**§** **164.104 Applicability.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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.

**§** **164.105 Organizational requirements.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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 clearing-house,” 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, re-ceived, 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 en-sure 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 le-gal 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 work-force 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 part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with subpart E of 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 para-graph (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 organization-al 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 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.

**§** **164.106 Relationship to other parts.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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.

The authority citation for subpart C of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d-2 and 1320d-4; sec. 13401, Pub. L. 111-5, 123 Stat. 260.

**§ 164.400 Applicability.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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.

**§ 164.404 Notification to individuals.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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).

**§ 164.408 Notification to the Secretary.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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.

**§ 164.410 Notification by a business associate.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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 ex-tent 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.

**§ 164.412 Law enforcement delay.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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.

The authority citation for subpart E of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d-2, 1320d-4, and 1320d-9; sec. 264 of Pub. L. 104-191, 110 Stat. 2033-2034 (42 U.S.C. 1320d-2 (note)); and secs. 13400-13424, Pub. L.111-5, 123 Stat. 258-279.

**§ 164.500 Applicability.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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.

**§ 164.501 Definitions.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

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 con-tract 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 pre-scribed 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 the 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 in-formation 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 con-tract 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.

**§ 164.502 Uses and disclosures of protected health information: general rules.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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 other-wise permitted or required by this subpart, provided that the covered entity has com-plied 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 this section, § 164.512, § 164.514(e), (f), or (g).

(2) 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 pro-gram);

(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 preexisting 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.

(A) 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 be-half 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.

(b) Standard: Minimum necessary.

(1) 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 dis-closure 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 in-formation on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safe-guard the information.

(2) Implementation specification: documentation. The satisfactory assurances required by paragraph (e)(1) of this section 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 in-formation 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 per son 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 of an individual if:

(i) The covered entity has a reasonable belief that:

(A) The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or

(B) Treating such person as the personal representative could endanger the individual; and

(ii) 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.

(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 in-formation 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 profession-al 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 be-half 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 de-scribed 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 in-formation 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).

**§ 164.504 Uses and disclosures: organizational requirements.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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) to (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 dis-close 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 sub-chapter to a covered entity, such covered entity may disclose protected health in-formation 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 be-tween 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 be-tween the covered entity and the business associate may permit the business associate to disclose the protected health in-formation 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 purpose 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 the purpose 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 in-formation 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 in-formation in accordance with § 164.524;

(F) Make available protected health in-formation 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 be-tween the group health plan and the plan sponsor. The plan documents must:

(A) Describe those employees or classes of employees or other persons un-der 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.

**§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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 in-formation 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.

**§ 164.508 Uses and disclosures for which an authorization is required.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

(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 dis-closure 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 com-pound 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 un-der 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 pro-vided under this section at any time, pro-vided 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 e-tity 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.

**§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.** [Go to Central ToC.](#ee) [Go to Part 160 ToC.](#cc) [Go to Part 164 ToC.](#First)

A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or dis-closure 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 be-comes 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) Use 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.

**§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

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. 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 orally.

(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.

(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. Notwithstanding 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)(iv) 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, 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 2000 Privacy Final Rule, § 164.512(k)(4)(i);

(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.

(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.

**§ 164.514 Other requirements relating to uses and disclosures of protected health information.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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, including a subcontractor, to whom it provides the limited data set agrees 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) .........

(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,

(ii) Department of service information;

(iii) Treating physician;

(iv) Outcome information; and

(v) 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 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).

**§ 164.520 Notice of privacy practices for protected health information.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(a) Standard: notice of privacy practices.

(1) Right to notice. Except as provided by paragraph (a)(2) or (3) 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) 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.

(3) 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 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, 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.

(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 such authorization as provided by § 164.508(b)(5).

(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) 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; or

(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; or

(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..

(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 with respect to protected health information, 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.

(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.

**§ 164.522 Rights to request privacy protection for protected health information.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.

**§ 164.524 Access of individuals to protected health information.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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;

(ii) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

(iii) Protected health information maintained by a covered entity that is:

(A) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law; or

(B) Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

(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.

1. 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 or 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.

**§ 164.526 Amendment of protected health information.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.

**§ 164.530 Administrative requirements.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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, as necessary and appropriate for the members of the workforce to carry out their function 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, 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 or its compliance with such policies and procedures or the requirements of this subpart.

(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. 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 may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

(1) Individuals. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) Individuals and others. Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(h) Standard: Waiver of rights. A covered entity may not require individuals to waive their rights under § 160.306 of this subchapter or this subpart 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. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the 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 or 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;

(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.

(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).

**§ 164.532 Transition provisions.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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; or

(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.

(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, 1013,, 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 24, 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.

**§ 164.534 Compliance dates for initial implementation of the privacy standards.** [Go to Central ToC.](#ee)[Go to Part 160 ToC.](#cc)[Go to Part 164 ToC.](#First)

(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.

EXHIBIT B

Notice of Privacy Practices

Effective date of notice: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NOTICE OF PRIVACY PRACTICES**

[*company name (replace this and the lines below with the appropriate information for your company)*], Lab

[*mailing address*]

[*phone number*]

[*fax number*]

[*E-Mail*]

[*Lab Privacy Contact Person*]

**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.**

The terms “you” and “your” as used herein refer to the individual consumer whose protected health information concerning their eye care may come into the possession of the optical lab. The term “we,” “our” and “us” as used herein refer to the Lab named above.

We are obligated by law to maintain the privacy of your health information and give you notice of our privacy practices. This Notice describes how we protect your health information and what rights you have regarding it.

**I. PERMITTED USES AND DISCLOSURES**

A. Treatment, Payment, and Health Care Operations

The most common reason why we use or disclose your health information is for treatment, payment or health care operations. We may use or disclose your health information for these purposes without your authorization.

1. Treatment - Examples of how we use or disclose information for treatment purposes are: taking information related to your vision correction needs, such as lens prescription, lens type, frame type, and your identity, which information we receive from orders of the eye care professional from whom you order eye care products, and using that information to prepare your vision correction products in accordance with such orders, or disclosing such information to other labs which assist us in fulfilling such orders.

2. Payment - Examples of how we use or disclose your health information for eye care professional or vision care plans, or other sources of payment are: preparing and sending bills or claims; and collecting unpaid amounts (either ourselves or through a collection agency or attorney).

3. Health Care Operations - “Health care operations” mean those administrative and managerial functions that we have to do in order to run our lab. Examples of how we use or disclose your health information for health care operations are: financial or billing audits; internal quality assurance; personnel decisions; participation in managed care plans; defense of legal matters; business planning; and outside storage of our records.

B. Uses and Disclosures for Other Reasons without Your Authorization

In some limited situations, the law allows or requires us to use or disclose your health information without your permission. Not all of these situations will apply to us; some may never come up at our lab at all. Such uses or disclosures are:

• when a state or federal law mandates that certain health information be reported for a specific purpose;

• for public health purposes, such as contagious disease reporting, investigation or surveillance; and notices to and from the federal Food and Drug Administration regarding drugs or medical devices;

• disclosures to governmental authorities about victims of suspected abuse, neglect or domestic violence;

• uses and disclosures for health oversight activities, such as for the licensing of doctors; for audits by Medicare or Medicaid; or for investigation of possible violations of health care laws;

• disclosures for judicial and administrative proceedings, such as in response to subpoenas or orders of courts or administrative agencies;

• disclosures for law enforcement purposes, such as to provide information about someone who is or is suspected to be a victim of a crime; to provide information about a crime at our office; or to report a crime that happened somewhere else;

• disclosure to a medical examiner to identify a dead person or to determine the cause of death; or to funeral directors to aid in burial; or to organizations that handle organ or tissue donations;

• uses or disclosures for health related research when the research has been approved by in institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your health information;

• uses and disclosures to prevent a serious threat to health or safety;

• uses or disclosures for specialized government functions, such as for the protection of the president or high ranking government officials; for lawful national intelligence activities; for military purposes; or for the evaluation and health of members of the foreign service;

• disclosures relating to worker’s compensation programs;

• disclosures to “business associates” who perform functions, activities or services on our behalf that require the use or disclosure of your health information. To protect your health information, we require the business associate to appropriately safeguard health information about you.

Unless you object, we will also share relevant information about your care with your family, friends, or other person who you identity who are helping you with your eye care. If you are unable to agree or object to such disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment.

C. Other Uses and Disclosures – Authorization Required

We must obtain your written authorization to use and disclose your health information for most marketing purposes.

We must obtain your written authorization for any disclosure of your health information which constitutes a sale of health information.

Other uses and disclosures of your health information, not described above, will be made only with your written authorization. The content of an authorization is determined by federal law.

If we initiate the process and ask you to sign an authorization form, you do not have to sign it. If you do not sign the authorization, we cannot make the use or disclosure. If you do sign one, you may revoke it at any time except to the extent we have already acted in reliance upon it. Revocations must be in writing. Send them to the office Contact Person named at the beginning of this Notice.

**II. YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION**

The law gives you many rights regarding your health information. You have the right to:

A. Ask to Restrict

• ask us to restrict our uses and disclosures for purposes of treatment, payment or health care operations. We do not have to agree to a restriction that you request, except we must agree not to disclose your health information to your health plan if the disclosure (1) is for payment or healthcare operations and is not otherwise required by law, and (2) relates to a health care item or service which you paid for in full out of pocket. If we agree to the requested restriction, we may not use or disclose your health information in violation of that restriction unless it is needed to provide emergency treatment. To ask for a restriction, send a written request to the office Contact Person at the address, fax or e-mail shown at the beginning of this Notice.

B. Request to Receive Confidential Communication from us by Alternative Means or at an Alternative Location

• ask us to communicate with you in a certain way or at a certain location, such as by phoning you at work rather than at home, by mailing health information to a different address, or by sending E-mail to your personal E-Mail address.

We will accommodate all reasonable requests. We may also condition this accommodation by asking your for information as to how payment will be handled or specification of an alternative address or other method of contact. If you want to ask for confidential communications, send a written request to the office Contact Person at the address, fax or E-mail shown at the beginning of this Notice.

C. Inspection or Copies

• ask to see or to get photocopies of your health information. You will be able to review or have a copy of your health information within 30 days of asking us. By law, we can have one 30-day extension of the time for us to give you access or copies if we send you a written notice of the extension. You may have to pay a cost-based fee for copies of your health information. By law, there are a few limited situations in which we can deny your request to access your health information. If we deny your request, we will send you a written explanation, and instructions about how to get an impartial review of our denial if one is legally available. If you want to review or get copies of your health information, send a written request to the office Contact Person at the address, fax or E-mail shown at the beginning of this Notice.

D. Request to Amend

• ask us to amend your health information if you think that it is incorrect or incomplete. We may deny this request if we did not create the PHI, unless you provide us a reasonable basis to believe that the originator of the PHI is no longer available to act on your request. If we agree to your request, we will amend the information within 60 days from when you ask us. By law, we can have one 30-day extension of time to consider a request for amendment if we notify you in writing of the extension. We will send the corrected information to persons who we know got the wrong information, and others that you specify. If we do not agree, you can write a statement of your position, and we will include it with your health information along with any rebuttal statement that we may write. Once your statement of position and/or our rebuttal is included in your health information, we will send it along whenever we make a permitted disclosure of your health information. If you want to ask us to amend your health information, send a written request, including your reasons for the amendment, to the office Contact Person at the address, fax or E-mail shown at the beginning of this Notice.

E. Accounting

• get an accounting of the disclosures that we have made of your health information within the past six years (or a shorter period if you want). By law, the list will not include: disclosures for purposes of treatment, payment or health care operations; disclosures with your authorization; disclosures incident to a use or disclosure otherwise permitted or required by law; disclosures required by law; and some other limited disclosures. You are entitled to one such list per year without charge. If you want more frequent lists, you will have to pay for them in advance. We will usually respond to your request within 60 days of receiving it, but by law we can have one 30-day extension of time if we notify you of the extension in writing. If you want a list, send a written request to the office Contact Person at the address, fax or E-mail shown at the beginning of this Notice.

F. Additional Copies of Privacy Notice

• get additional paper copies of this Notice of Privacy Practices upon request. It does not matter whether you got one electronically or in paper form already. If you want additional paper copies, send a written request to the office Contact Person at the address, fax or E-mail shown at the beginning of this Notice.

G. Breach Notification

• be notified by us if you are affected by a breach of unsecured protected health information.

H. Fundraising Communication Opt Out

• We may contact you for fundraising purposes. You may opt out of receiving fundraising communications from us.

**III. OUR NOTICE OF PRIVACY PRACTICES**

By law, we must abide by the terms of this Notice of Privacy Practices currently in effect. We reserve the right to change this notice at any time as allowed by law. If we change this Notice, the new privacy practices will apply to your health information that we already have as well as to such information that we may generate in the future. If we change our Notice of Privacy Practices, we will post the new notice on our Web site.

**IV. COMPLAINTS**

If you think that we have not properly respected the privacy of your health information, you are free to complain to us or the U.S. Department of Health and Human Services, Office for Civil Rights. We will not retaliate against you if you make a complaint. If you want to complain to us, send a written complaint to the office Contact Person at the address, telephone number, fax or E-mail shown at the beginning of this Notice. If you prefer, you can discuss your complaint in person or by phone.

**V. FOR MORE INFORMATION**

If you want more information about our privacy practices, call or visit the office Contact Person at the address or phone number shown at the beginning of this Notice.

**EXHIBIT C**

The Vision Council Optical Lab Division Legal Counsel has concluded that there are instances where an optical lab may need to have a Business Associate Agreement (BAA) with its vendors who provide services for and on behalf of the optical lab that involve the use and disclosure of PHI. For example, when the lab utilizes the services of a supplier of lab processing software, and that supplier accesses the lab’s PHI – either online or via backup tapes – for the purpose of software support and process control trouble shooting.

On the following pages is a model Business Associate Agreement that division members of The Vision Council may use in this situation. The model agreement – with modifications – would also be applicable to other situations in which a lab might require a BAA.

It is the lab’s responsibility as the “covered entity” under HIPAA to secure this BAA with a lab software supplier, or other similar business associate.

**BUSINESS ASSOCIATE AGREEMENT**

This Business Associate Agreement (“B.A. Agreement”) is entered into by and between *[Optical Laboratory]* (“Covered Entity”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(“Business Associate”) as of this \_\_\_\_\_\_ day of \_\_\_\_\_\_\_, 20\_\_ (“Effective Date”) .

**RECITALS**

WHEREAS, *[Optical Laboratory]* is a “Covered Entity” as defined under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and its implementing regulations (collectively, “HIPAA”), as amended by the regulations promulgated pursuant to the Health Information Technology for Economic and Clinical Health (“HITECH”) Act (Division A, Title XIII and Division B, Title IV of Public L. 111–5) (which was part of the American Recovery and Reinvestment Act of 2009), and \_\_\_\_\_\_\_\_\_\_\_\_\_ is a “Business Associate” as defined under HIPAA; and

WHEREAS, in connection with the *[services]* agreement between Covered Entity and Business Associate for Business Associate to provide *[certain services]* for and on behalf of Covered Entity (the “Agreement”), Covered Entity may provide Business Associate with Protected Health Information (defined below); and

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this BAA, which is drafted to satisfy specific components of HIPAA and relevant implementing regulations, including the Privacy Rule (defined below), the Security Rule (defined below) and the Breach Notification Rule (defined below).

**I. DEFINITIONS**

(a) “Breach” shall have the meaning given to such term in 45 C.F.R. § 164.402 and applicable State data breach notification law.

(b) “Breach Notification Rule” shall mean the rule related to breach notification for Unsecured Protected Health Information at 45 C.F.R. Parts 160 and 164.

(c) “Designated Record Set” shall have the meaning given to such term under the Privacy Rule at 45 C.F.R. § 164.501.

(d) "Electronic Protected Health Information" or ("EPHI") shall have the same meaning given to such term under the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity..

(e) “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information, codified at 45 C.F.R. Parts 160 and Part 164, Subparts A and E.

(f) “Protected Health Information” or “PHI” shall have the meaning given to such term under the Privacy and Security Rules at 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(g) “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information, codified at 45 C.F.R. § 164 Subparts A and C.

(h) Other capitalized terms used, but not otherwise defined, in this B.A. Agreement shall have the same meaning as those terms in the Privacy, Security or Breach Notification Rules.

**II. PRIVACY RULE****OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE**

(a) Limitations of Disclosures. Business Associate agrees to not use or disclose PHI other than as permitted or required by this B.A. Agreement or, the Agreement, or as Required By Law. Business Associate shall not use or disclose PHI in a manner that would violate the Privacy Rule if done by Covered Entity, unless expressly permitted to do so pursuant to the Privacy Rule, the Agreement, and this B.A. Agreement.

(b) Appropriate Safeguards. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this B.A. Agreement, the Agreement, or as Required By Law.

(c) Obligations on Behalf of Covered Entity. To the extent Business Associate carries out an obligation for which Covered Entity is responsible under the Privacy Rule, Business Associate must comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligation.

(d) Mitigation. Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of HIPAA, the Agreement, or this B.A. Agreement.

(e) Reporting of Improper Use or Disclosure. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this B.A. Agreement within five (5) days of which it becomes aware.

(f) Business Associate’s Subcontractors. Business Associate agrees to ensure that any Subcontractor, consistent with 45 C.F.R. § 164.502(e)(1)(ii), that creates, receives, maintains, or transmits PHI on behalf of Business Associate agrees in writing to the same restrictions and conditions that apply through this B.A. Agreement to Business Associate with respect to such PHI.

(g) Access to PHI. Business Associate shall provide access, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual or a third party designated by the Individual, in order to meet the requirements under the Privacy Rule at 45 C.F.R. § 164.524.

(h) Amendment of PHI. Business Associate shall make any PHI contained in a Designated Record Set available to Covered Entity (or an Individual as directed by Covered Entity) for purposes of amendment per 45 C.F.R. § 164.526. Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to the Privacy Rule, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity. If an Individual requests an amendment of PHI directly from Business Associate or its Subcontractors, Business Associate shall notify Covered Entity in writing within five (5) days of receiving such request. Any denial of amendment of PHI maintained by Business Associate or its Subcontractors shall be the responsibility of Covered Entity.

(i) Government Access to Records. Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI, available to the Secretary, in a time and manner designated by the Secretary, for determining Covered Entity’s compliance with the Privacy Rule.

(j) Documentation and Accounting of Disclosures. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528. Business Associate agrees to provide to Covered Entity, in time and manner requested by Covered Entity, information collected in accordance with this paragraph, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528.

(k) Retention of PHI. Notwithstanding Section VI(c) below, Business Associate and its Subcontractors shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under Section II(j) for a period of six (6) years after termination of the Agreement.

(l) Minimum Necessary. Business Associate shall only request, use and disclose the Minimum Necessary amount of PHI necessary to accomplish the purpose of the request, use or disclosure.

**III. PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE**

(a) Permitted Uses and Disclosures of PHI. Except as provided in Paragraphs (b), (c), and (d) of Section III, Business Associate may only use or disclose PHI to perform functions, activities or services for, or on behalf of Covered Entity, as specified in the Agreement.

(b) Use for Management and Administration. Except as otherwise limited in this B.A. Agreement, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), use PHI if necessary (i) for the proper management and administration of Business Associate, or (ii) to carry out the legal responsibilities of Business Associate.

(c) Disclosure for Management and Administration. Except as otherwise limited in this B.A. Agreement, Business Associate may, consistent with 45 C.F.R. 164.504(e)(4), disclose PHI for the proper management and administration of Business Associate, provided (i) the disclosure is Required by Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed (“Person”) that it will be held confidentially and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the Person, and that the Person agrees to immediately notify Business Associate in writing of any instances of which it becomes aware in which the confidentiality of the information has been breached or is suspected to have been breached.

(d) Reporting Violations. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

**IV. SECURITY RULE OBLIGATIONS OF BUSINESS ASSOCIATE**

(a) Compliance with the Security Rule. Business Associate agrees to comply with the Security Rule with respect to Electronic Protected Health Information and have in place reasonable and appropriate Administrative, Physical, and Technical Safeguards to protect the Confidentiality, Integrity, and Availability of EPHI and to prevent the use or disclosure of EPHI other than as permitted by the Agreement, this B.A. Agreement, and as Required By Law.

(b) Subcontractors. Business Associate shall ensure that any Subcontractor that creates, receives, maintains, or transmits EPHI on behalf of Business Associate agrees in writing to comply with the Security Rule with respect to such EPHI.

(c) Security Incident/Breach Notification Reporting. Business Associate shall report any Security Incident promptly upon becoming aware of such incident. Separate from the requirements related to Security Incident reporting, Business Associate shall also make the reports set forth below in Section V, related to a Breach of Unsecured PHI.

**V. BREACH NOTIFICATION (FEDERAL AND STATE) RULE OBLIGATIONS OF BUSINESS ASSOCIATE**

(a) Notification Requirement. Immediately following Business Associate’s discovery of a Breach, or upon Business Associate’s reasonable belief that a Breach has occurred, Business Associate shall provide written notification of such Breach to Covered Entity.

(b) Discovery of Breach. For purposes of reporting a Breach to Covered Entity, the discovery of a Breach shall occur on the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to or suspected by the Business Associate. Business Associate will be considered to have had 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 agent of the Business Associate.

(c)Content of Notification. Any notice referenced above in Section V(a) of this B.A. Agreement will include, to the extent known to the Business Associate, the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been accessed, acquired, or disclosed during such Breach, as well as the information, to the extent known by Business Associate, that Covered Entity is required to include in its notification to the individual pursuant to the Breach Notification Rule or applicable State data breach notification laws. Business Associate will also provide (on a continuing basis as information is discovered) to Covered Entity other available information that Covered Entity is required to include in its notification to the individual pursuant to the Breach Notification Rule or applicable State data breach notification laws.

(d) Cooperation with Covered Entity. Business Associate shall:

(i) Cooperate and assist Covered Entity with any investigation into any Breach or alleged Breach, including those conducted by any Federal agency, State Attorney General, State agency (or their respective agents);

(ii) Comply with Covered Entity’s determinations regarding Covered Entity’s and Business Associate’s obligations to mitigate to the extent practicable any potential harm to the individuals impacted by the Breach; and

(iii)As directed by the Covered Entity, assist with the implementation of any decision by Covered Entity or any Federal agency, State agency, including any State Attorney General, or their respective agents, to notify and provide mitigation to individuals impacted or potentially impacted by a Breach.

**VI. TERM AND TERMINATION**

(a) Term. The term of this B.A. Agreement shall commence as of the Effective Date, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the provisions of this Section VI.

(b) Termination for Cause. Upon Covered Entity’s knowledge of a material breach of the terms of this B.A. Agreement, Covered Entity shall:

(i) Provide an opportunity for Business Associate to cure, and, if Business Associate does not cure the breach within thirty (30) days, Covered Entity may immediately terminate this BAA and the Agreement;

(ii) Immediately terminate this BAA and the Agreementif Covered Entity has determined that (a) Business Associate has breached a material term of this BAA, and (b) cure is not possible; or

(iii) Immediately terminate this BAA if the Agreement has been terminated.

(c) Effect of Termination.

(i) Except as provided for in paragraph (ii) of this Section VI(c), upon termination of this B.A. Agreement for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, and shall not retain copies thereof. This provision shall apply to PHI that is in the possession of Subcontractors of Business Associate.

(ii) In the event that Business Associate and Covered Entity determine, by mutual agreement, that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this B.A. Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

**VII. MISCELLANEOUS**

(a)Regulatory References. A reference in this B.A. Agreement to a section in the Privacy, Security, or Breach Notification Rule means the section as in effect or as amended, and for which compliance is required.

(b) Survival. The respective rights and obligations of Business Associate under Section 6(c) of this BAA shall survive the termination of the BAA.

(c) No Third Party Beneficiaries. Nothing express or implied in this B.A. Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

(d) Amendment. The parties agree to take such action as is necessary to amend this B.A. Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy, Security or Breach Notification Rules, as well as HIPAA and HITECH.

(e) Effect on Agreement. Except as specifically required to implement the purposes of this B.A. Agreement, or to the extent inconsistent with this B.A. Agreement, all other terms of the Agreement shall remain in force and effect.

(f) Interpretation. The provisions of this B.A. Agreement shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provision in this B.A. Agreement. Any ambiguity in this B.A. Agreement shall be resolved to permit Covered Entity to comply with the Privacy, Security, and Breach Notification Rules, as well as HIPAA and HITECH.

(g) Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this B.A. Agreement is satisfactory for Business Associate to comply with any obligations it may have under HIPAA, the Privacy Rule, or any other applicable law or regulation pertaining to the confidentiality, use or safeguarding of health information. Business Associate is solely responsible for all decisions it makes regarding the use, disclosure or safeguarding of PHI.

(h) Indemnification.

(i) Business Associate shall indemnify, defend and hold Covered Entity and its officers, directors, employees, agents, successors and assigns (“Covered Entity Indemnities”) harmless, from and against any and all losses, claims, actions, demands, liabilities, damages, costs and expenses (including, but not limited to, costs of providing notifications and credit monitoring services to individuals pursuant to the Breach Notification Rule and State data breach notification laws, administrative costs associated with Covered Entity’s and Business Associate’s compliance with Breach Notification Rule and State data breach notification laws, judgments, settlements, court costs and reasonable attorneys’ fees actually incurred) (collectively, “Information Disclosure Costs”) arising from or related to: (1) any breach of this BAA by Business Associate, including but not limited to the use or disclosure by Business Associate of Individually Identifiable Information (including PHI) in violation of the terms of this B.A. Agreement or applicable law; and (2) whether in oral, paper or electronic media, any Breach caused, directly or indirectly, by Business Associate.

(i) Counterparts. This B.A. Agreement may be executed in multiple counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument. Facsimile or electronic (PDF) signatures shall be treated as original signatures. This B.A. Agreement shall be binding when one or more counterparts hereof, individually or taken together, shall bear the signatures of all of the parties reflected on this B.A. Agreement as the signatories thereto.

***[Optical Laboratory]*: *[Business Associate]*:**

By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Title:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

EXHIBIT D

A. The following classes of employees at the Lab need to have access to PHI for performance of their work:

(Insert here the employees or groups of employees who need to have access to PHI. In many labs, this could include all company employees.)

B. The following information represents the PHI to which the classes of employees in item A above may have access to, as is reasonably incident to the performance of their work:

Information that is created or received by the Lab and relates to the past, present, or future physical or mental health or condition of an individual, including:

* Medical Information.
* Billing information.
* Financial information.
* Patient’s names.
* Patient addresses which include geographic subdivisions smaller than a state [including street address, city, county, precinct, certain zip codes . . . *See* § 164.514(b)(2) at Exhibit A hereto].
* All elements of dates (except for year) for dates related to the patient, including birth date, treatment date, and all elements of dates indicative of an age over 89.
* Telephone numbers.
* Fax numbers.
* E-mail addresses.
* Social security numbers.
* Medical record numbers.
* Health plan beneficiary numbers.
* Account numbers.
* Certificates/license numbers.
* Vehicle identifiers and serial numbers, including license plate numbers.
* Device identifiers and serial numbers.
* Web site URLs.
* Internet protocol (IP) address numbers.
* Biometric identifiers including finger and voice prints.
* Full face photographic images.
* Any other unique identifying number, characteristic or code.

C. The classes of employees in item A above may copy any portions of the PHI to which they have access that are necessary to complete the order specifications of the eyewear to be produced.

1. \* In the unlikely event that a patient deals directly with the Lab, the Lab shall provide the patient with a copy of the Notice of Privacy Practices, make a good faith effort to obtain a written acknowledgement of receipt, and document the acknowledgment or the good faith effort to secure the acknowledgment. [↑](#footnote-ref-2)