Uses and Disclosures – General Rules

A. Standard. A covered entity or business associate may not use or disclose PHI, except as permitted or required.

1. Covered entities: Permitted uses and disclosures. A covered entity is permitted to use or disclose PHI as follows:

   a. To the individual;

   b. For treatment, payment, or health care operations;

   c. Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of Minimum Necessary and Safeguards with respect to such otherwise permitted or required use or disclosure;

   d. Except for uses and disclosures prohibited, pursuant to and in compliance with a valid authorization under Use and Disclosure – Authorization Required;

   e. Pursuant to an agreement under, or as otherwise permitted by, Use and Disclosure - Opportunity for Individual to Agree or Object Required; and

   f. As permitted by and in compliance:

      i. With this section,

      ii. Use and Disclosure – Authorization or Opportunity for Individual to Agree or Object Not Required,

      iii. Limited data set,

      iv. Fundraising, or

      v. Underwriting and related purposes.

2. Covered entities: Required disclosures. A covered entity is required to disclose PHI:

   a. To an individual, when requested under, and required by:

      i. Access of Individuals

      ii. Accounting of Disclosures

   b. When required by the Secretary to investigate or determine the covered entity's compliance with this subchapter.

2. Business associates: Permitted uses and disclosures. A business associate may use or disclose PHI only as permitted or required by its business associate contract or other arrangement. The business associate may not use or disclose PHI in a manner that would violate the requirements, if done by the covered entity, except if such uses or disclosures are permitted by its contract or other arrangement.

3. Business associates: Required uses and disclosures. A business associate is required to disclose PHI:

   a. When required by the Secretary to investigate or determine the business associate's compliance with this subchapter.

b. To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of PHI.

4. Prohibited uses and disclosures.

a. Sale of PHI:

i. Except pursuant to and in compliance with Use and Disclosure - Authorization Required a covered entity or business associate may not sell PHI.

ii. For purposes of this paragraph, sale of PHI means:

A. Except as provided in research purposes, a disclosure of PHI 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 PHI in exchange for the PHI.

B. Sale of PHI does not include a disclosure of PHI:

1. For public health purposes pursuant to Public Health Activities or Limited Data Set;

2. For research purposes or Limited Data Set 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 PHI for such purposes;

3. For treatment and payment purposes pursuant to Use and Disclosure - Treatment, Payment, Or Health Care Operations;

4. For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence of health care operations and pursuant to Use and Disclosure - Treatment, Payment, Or Health Care Operations

5. To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor 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;

6. To an individual, when requested under Access of Individuals and Accounting of Disclosures.

7. Required by law; and

8. 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 PHI for such purpose or a fee otherwise expressly permitted by other law.

B. Standard: Minimum necessary:

1. Minimum necessary applies. When using or disclosing PHI or when requesting PHI from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit PHI 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:

a. Disclosures to or requests by a health care provider for treatment;

b. Uses or disclosures made to the individual;

c. Uses or disclosures made pursuant to an authorization;

d. Disclosures made to the Secretary;

e. Uses or disclosures that are required by law, as described by Use and Disclosure – Authorization or Opportunity for Individual to Agree or Object Not Required; and

f. Uses or disclosures that is required for compliance with applicable requirements.

C. Standard: Uses and disclosures of PHI subject to an agreed upon restriction. A covered entity that has agreed to a restriction pursuant to Rights to Request Privacy Protection may not use or disclose the PHI covered by the restriction in violation of such restriction, except as otherwise provided.

D. Standard: Uses and disclosures of de-identified PHI.

1. Uses and disclosures to create de-identified information. A covered entity may use PHI to create information that is not individually identifiable health information or disclose PHI 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 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, provided that:

a. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of PHI; and

b. 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. Standard: Disclosures to business associates.

1. A covered entity may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI 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.

2. A business associate may disclose PHI to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, if the business associate obtains satisfactory assurances, in accordance with Business Associate Contracts that the subcontractor will appropriately safeguard the information.

3. Implementation specification: Documentation. The satisfactory assurances required by paragraph (E)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of Business Associate Contracts.

F. Standard: Deceased individuals. A covered entity must comply with the requirements of this subpart with respect to the PHI of a deceased individual for a period of 50 years following the death of the individual.

G. Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in (G)(2) and (G)(3)(e) of this section, treat a personal representative as the individual for purposes of this subchapter.

1. 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 PHI relevant to such personal representation.

2. 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 PHI 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 PHI 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.

3. Notwithstanding the provisions:

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 to Individuals, PHI 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 to Individuals, PHI 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 and where there is no applicable access provision under State or other law, including case law, a covered entity may provide or deny access 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.

d. Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to PHI relevant to such personal representation.

e. 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 Confidential Communications in communicating PHI.

I. Standard: Uses and disclosures consistent with notice. A covered entity is required to have a notice may not use or disclose PHI in a manner inconsistent with such notice. A covered entity that is required to include a specific statement in its notice if it intends to engage in fundraising, may not use or disclose PHI 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 PHI, provided that:

   a. The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and

   b. The disclosure is to:

      i. 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

      ii. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described.

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 PHI to a law enforcement official, provided that:

   a. The PHI disclosed is about the suspected perpetrator of the criminal act; and

   b. The PHI disclosed is limited to the information listed in Law Enforcement Purposes.