



## Managing Information Privacy & Security in Healthcare

### Protected Health Information: General Rules on Use and Disclosure

By Sandra J. Sinay, JD, LLM and Barbara Demster, MS, RHIA, CHCQM

The HIPAA Privacy Rule, [§164.502](#), provides general rules concerning the use and disclosure of protected health information. A covered entity may not use or disclose protected health information, except as permitted or required by [§164.502](#) or by the Compliance and Enforcement provisions (subpart C of part 160 of the HIPAA Privacy Rule).

**Permitted Uses and Disclosures:** [§164.502](#). A covered entity is permitted to use or disclose protected health information as follows:

- To the individual who is the subject of the information;
- For treatment, payment, or health care operations, as permitted by and in compliance with [§164.506](#);
- Incident to a use or disclosure otherwise permitted or required by subsection (a)(1) of [§164.502](#) provided that the covered entity has complied with the applicable requirements of subsection (b) of [§164.502](#), subsection (d) of [§164.514](#), and subsection (c) of [§164.530](#);
- Pursuant to and in compliance with an authorization that complies with [§164.508](#);
- Pursuant to an agreement under, or as otherwise permitted by, [§164.510](#); and
- As permitted by and in compliance with subsection (a)(1) of [§164.502](#), [§164.512](#), or subsections (e),(f), or (g) of [§164.514](#).

**Required Disclosures:** Subsection (a)(2) of [§164.502](#). A covered entity is required to disclose protected health information:

- To an individual, when requested under, and as required by [§164.524](#) or [§164.528](#); and
- When required by the Secretary under the Compliance and Enforcement provisions (subpart C of part 160) to investigate or determine the covered entity's compliance with the regulations.

**Minimum Necessary Standard** [§164.502](#). A covered entity must make reasonable efforts to limit protected health information to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request. The minimum necessary applies when using or disclosing protected health information or when requesting protected health information from another covered entity (see subsection (b)(1) of [§164.502](#)) with some exceptions.

The minimum necessary standard does not apply to the following:

- Disclosures to or requests by a health care provider for treatment;
  - Uses or disclosures made to the individual who is the subject of the information;
  - Uses or disclosures made pursuant to a valid authorization;
  - Disclosures made to the Secretary in accordance with the regulations;
  - Uses or disclosures that are required by law (see [§164.512](#)); and
  - Uses or disclosures that are required for compliance with the HIPAA Privacy Rule
- See Also Minimum Necessary in [Other Requirements \[Link D24\]](#)

The AHIMA has developed two practice briefs that provide excellent guidance in understanding and implementing the Minimum Necessary Standard. These may be accessed at the following links.

**AHIMA Practice Brief: Understanding the Minimum Necessary Standard**  
- < [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_018177.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_018177.hcsp) >

**AHIMA Practice Brief: Implementing the Minimum Necessary Standard**  
- < [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_015785.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_015785.hcsp) >

**Agreed Upon Restriction:** Subsection (c) of [§164.502](#). One of the rights provided to individuals is the right to request restriction on the uses and disclosure of their protected health information. A covered entity that has agreed to a restriction on a use or disclosure of protected health information pursuant to [§164.522](#) may not use or disclose the protected health information covered by the restriction in violation of the agreed upon restriction, except as otherwise provided in the regulation.

The regulations state that a covered entity must permit an individual to request that the covered entity restrict uses or disclosures of PHI about a) the individual to carry out treatment, payment, or health care operations or b) disclosures permitted under subsection (b) §164.510: *Uses and disclosures for involvement in the individual's care and notification purposes.*

While the regulations require the covered entity to provide the right to request a restriction, the regulations also state that the covered entity is not required to agree to a restriction. If the covered entity agrees to a restriction, it may not use or disclose protected health information in violation of such restriction. The exception is if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment. Under those conditions, 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. If the covered entity agrees to a restriction it must document the restriction.

If restricted protected health information is disclosed to a health care provider for emergency treatment, the covered entity must request that health care provider receiving the restricted PHI not further use or disclose the information.

A restriction agreed to by a covered entity is not effective to prevent uses or disclosures permitted or required to assess the covered entities compliance with the regulations [§164.502(a)(2)(ii)], emergency circumstances as defined in section 164.510(a) or when an authorization is not required as stated in section 164.512.

A covered entity may terminate its agreement to a restriction under the following conditions:

- The individual agrees to or requests the termination in writing;
- The individual orally agrees to the termination and the oral agreement is documented; or
- The covered entity informs the individual that it is terminating its agreement to a restriction, with the condition that such termination is only applicable to PHI created or received after it has so informed the individual.

**De-identified Protected Health Information (§164.502(d)).** A covered entity may use protected health information to create information that is not individually identifiable 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. De-identified health information, per §164.514(a) and (b), is not individually identifiable and as such, is not protected. Note, however, that disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information.

**Disclosures to Business Associates (§164.502(e)(1)).** A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive 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 that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of §164.504(e). A covered entity must document the satisfactory assurances required through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).

- This standard does not apply, however, to the following:
  - Disclosures by a covered entity to a health care provider concerning the treatment of the individual;
  - Disclosures by a group health plan or 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) apply and are met; or
  - Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the protected health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually identifiable health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan.

**Deceased Individuals:** Subsection (f) and (g)(4) of [§164.502](#). A covered entity must comply with the requirements of the Privacy Rule with respect to the protected health information of a deceased individual. 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 with respect to protected health information relevant to such personal representation.

**Personal Representatives:** Subsection (g)(1) of [§164.502](#). Except for the exceptions specified below for unemancipated minors and those individuals subject to abuse, neglect and/or endangerment situations, a covered entity must treat a personal representative as the individual.

- **Adults and Emancipated Minors ([§164.502\(g\)\(2\)](#)).** 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 with respect to protected health information relevant to such personal representation.
- **Unemancipated Minors ([§164.502\(g\)\(3\)](#)).** 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 with respect to protected health information relevant to such personal representation. A person may not serve as 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:
  - 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;
  - 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
  - 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.
- **Abuse, Neglect, Endangerment Situations ([§164.502\(g\)\(5\)](#)).** Notwithstanding State law, a covered entity may elect not to treat a person as the personal representative of an individual if the covered entity has a reasonable belief that the individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and 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.

**Confidential Communications:** subsection (h) of [§164.502](#). A covered health care provider or health plan must comply with the requirements of § 164.522(b) in communicating protected health

information. These provisions require that 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. 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. A covered entity may require the individual to make a request for a confidential communication in writing.

A covered entity may condition the provision of a reasonable accommodation on:

- When appropriate, information as to how payment, if any, will be handled; and
- Specification of an alternative address or other method of contact.

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. 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.

**Uses and Disclosures Consistent with Notice** A covered entity that is required to have a notice of privacy practices may not use or disclose protected health information 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 an activity listed in [§164.520\(b\)\(1\)\(iii\)\(A\)-\(C\)](#), may not use or disclose protected health information for such activities, unless the required statement is included in the notice.

**Disclosures by Whistleblowers** ([§164.502\(j\)](#)). A covered entity is not considered to have violated any requirements if a member of its workforce or a business associate discloses protected health information, provided that 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.

The disclosure of the questionable conduct must be to a health oversight agency or public health authority authorized by law to investigate the relevant conduct 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 to 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.

**Disclosures by Workforce Members Who are Victims of Crime** ([§164.502\(j\)\(2\)](#)). A member of a covered entity who is the victim of a criminal act may disclose protected health information to a law enforcement official, provided that the protected health information disclosed is about the suspected perpetrator of the criminal act and the protected health information disclosed is limited to the information listed in [§164.512\(f\)\(2\)\(i\)](#).

**Additional Resources:**

See **AHIMA Practice Brief: Consent for Uses and Disclosures of Information (Updated)**

< [http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1\\_016338.hcsp](http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_016338.hcsp) >