HIPAA inSight

Health Insurance Portability and Accountability Act

November 2002• No. 6
PHC 1919

The information in *HIPAA inSight* applies to billing vendors, Medicaid HMOs and other managed care programs, as well as providers participating in the following Wisconsin health care programs administered by the Division of Health Care Financing (DHCF):

- Medicaid and BadgerCare.
- Health Insurance Risk Sharing Plan (HIRSP).

The HIPAA privacy standards

This document provides preliminary general summary information about the HIPAA privacy standards and does not purport to be a comprehensive restatement of all the requirements of the standards; moreover, nothing in this document should be construed as legal advice. Do not rely on this document to ensure or determine compliance with the privacy standards. Always consult the standards and/or your privacy lawyer when making decisions about privacy for your organization.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy regulation, officially titled "Standards for Privacy of Individually Identifiable Health Information," provides the first comprehensive federal protection for the privacy of health information.

Why were the HIPAA privacy standards enacted?

Congress recognized the need for national patient health information privacy standards when it enacted HIPAA. Federal privacy regulations issued pursuant to the final HIPAA enactment were published in the Federal Register on December 28, 2000, and amended on August 14, 2002, with an implementation deadline of April 14, 2003 (April 14, 2004, for small health plans). Those regulations are created in 45 CFR Part 160 and 164. They provide the first comprehensive federal protection for the privacy and confidentiality of health information. The requirements specify who has the right to access individually identifiable health information (IIHI) and covers all IIHI used or disclosed by a covered entity in any form, whether electronically, on paper, or orally.

What does the privacy regulation do?

The privacy rule defines protected health information (PHI) and establishes certain individual rights regarding this information. The rule also:

- Gives patients more control over their health information.
- Sets boundaries on the use and release of health records.
- Establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- Holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- Strikes a balance when public responsibility requires disclosure of some forms of data, for example, to protect public health.

For patients, the privacy standards:

- Enable them to find out how their information may be used and what disclosures of their information have been made by the covered health provider or health plan.
- Generally limit the release of information to the minimum reasonably needed for the purpose of the disclosure.
- Give them the right to examine and obtain a copy of their own protected health information that is maintained in a designated record set and to request corrections of PHI made by the covered health care provider or health plan.

Who must comply?

Covered entities and their business associates must comply with the privacy standards.

When will covered entities have to meet these standards?

Most covered entities have until April 14, 2003, to become compliant with the privacy standards. Under the law, small health plans have until April 14, 2004, to achieve compliance.

Which federal department has responsibility for enforcement of the HIPAA privacy standards?

The federal Department of Health and Human Services (HHS) Office for Civil Rights (OCR) will enforce the standards. The OCR has provided some guidance for covered entities in meeting the requirements of the regulation. For further information, consult the OCR Web site at *www.hhs.gov/ocr/hipaa/*. The OCR is in the process of updating its Web site to reflect final revisions to the rule.

In general, what must covered entities and their business associates do to achieve compliance?

Under the privacy standards, covered entities and their business associates are required to develop and implement the following points to ensure the privacy of IIHI and PHI:

1. Appoint a privacy officer.
   The privacy officer is responsible for the development and implementation of policies and procedures required by the privacy standards, may receive complaints, and may provide further information about matters covered by the privacy notice. (Refer to Number 14 of this list for information about the privacy notice.)

2. Develop minimum necessary policies.
   Covered entities must make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary. For routine disclosures, covered entities must implement policies and procedures that limit the amount of PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

3. Amend business associate contracts.
   - A covered entity may disclose PHI to a business associate if it receives satisfactory assurance that the business associate will appropriately safeguard the information.
   - Satisfactory assurances must be obtained in a contract or other written arrangement.
   - If the covered entity and the business associate are both governmental entities, a memorandum of understanding may provide satisfactory assurances.

Most covered entities have until April 14, 2003, to become compliant with the privacy standards. Under the law, small health plans have until April 14, 2004, to achieve compliance.

4. Develop an authorization form.
   - In general, covered entities must obtain an individual's authorization before using or disclosing the individual's PHI for any purpose other than treatment, payment, or health care operations.
   - In general, covered entities may not condition treatment, enrollment, or eligibility for benefits upon the provision of an authorization.
   - An authorization form must contain certain elements specified in the privacy regulations.

5. Develop verification procedures.
   Before disclosing PHI, the covered entity must verify the identity of the person requesting PHI and the authority of that person to have access.

6. Develop accounting of disclosures capabilities.
   The covered entity must give an individual up to a six-year accounting of disclosures made of the individual's PHI, including disclosures to or by business associates, except for disclosures:
   - To carry out treatment, payment, or health care operations.
   - To the individual.
   - To providers or for facility directory.

- For national security or intelligence purposes.
- To corrections officials or law enforcement personnel.
- Made before the compliance date.

7. Develop a procedure to request alternative means of communication.
   A health plan or covered health care provider must permit individuals to request and must accommodate reasonable requests to receive communication of PHI by alternative means or at an alternative location.

8. Develop a procedure to request restricted use of PHI.
   A covered entity must allow an individual to request that the covered entity restrict its use and disclosure of the individual's PHI for treatment, payment, or health care operations. The covered entity is not required to agree to the restriction. If the covered entity agrees to the restriction, it may not violate that agreement except for emergency treatment.

9. Develop a complaint procedure.
   A covered entity must provide a process for individuals to make complaints to the covered entity concerning its privacy standards policies and procedures, its compliance with those policies or procedures or its compliance with the privacy standards itself. A covered entity must document all complaints received and the complaints' disposition.

Terms and definitions

Business associate
A person or entity who is *not* a member of the covered entity's workforce, but performs a function for the covered entity which requires it to use, disclose, create, or receive PHI. A business associate can also be a covered entity in its own right.

Designated record set
Records by or for a covered entity from which information is retrieved, which is used by the covered entity to make decisions about an individual.

Covered entity
Is one of the following: a health plan, health care clearinghouse, or health care provider who transmits PHI in electronic form to carry out financial or administrative activities related to health care.

IIHI
Individually identifiable health information. Information that is a subset of health information, including demographic information collected from an individual that:
- Is created by or received from a health care provider, health plan, employer, or health care clearinghouse.
- Relates to the past, present, or future physical or mental health 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.
- Identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.

Refer to s.160.103 of the privacy regulations for a complete definition of IIHI.

PHI
Protected health information is IIHI that is one or more of the following:
- Transmitted by electronic media.
- Maintained in any medium described in the definition of electronic media (s.162.103 of the privacy regulations).
- Transmitted or maintained in any other form or medium.

Refer to s.164.501 of the privacy regulations for exceptions to this definition.

10. Develop a procedure to request amendment of PHI.
    A covered entity must permit an individual to request that the covered entity amend the individual's PHI. The covered entity may require that the request be in writing and state a reason for the amendment, as long as it informs individuals in advance of that requirement. The covered entity must act on the request within 60 days. One 30-day extension is allowed.

11. Develop a procedure for individual access to PHI.
    A covered entity must provide access to an individual to inspect or copy his or her PHI. The covered entity may require that the request be in writing, as long as it informs individuals in advance of that requirement.

12. Develop an anti-retaliation policy.
    A covered entity may not retaliate against any person for exercising a right under the privacy standards, or for filing a complaint, participating in an investigation, or opposing any unlawful act relating to the privacy standards.

13. Train workforce.
    The covered entity must provide training to each member of the workforce by the compliance date; thereafter, training must be provided to each new member of the workforce within a reasonable period of time after joining the workforce and to each member of the workforce whose functions are affected by a material change in the required policies or procedures.

14. Develop and disseminate a privacy notice.
    A covered entity must disseminate a notice of its privacy practices to individuals.

A covered entity must provide access to an individual to inspect or copy his or her PHI. The covered entity may require that the request be in writing, as long as it informs individuals in advance of that requirement.