Laws and Regulations Governing the Disclosure of Health Information (2002 update)

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: The following information supplants information contained in the May 2001 Practice Brief, "Laws and Regulations Governing the Disclosure of Health Information".

Patients must be assured that the health information they share with healthcare professionals will remain confidential. Without such assurance, patients may withhold critical information that could affect the quality and outcome of care.

To date, the privacy and confidentiality of patient health information has been protected by a patchwork of federal and state laws and regulations, facility policy, professional standards of practice, and codes of ethics. The recently passed *Standards for Privacy of Individually Identifiable Health Information* (45 CFR, parts 160 and 164) under HIPAA establishes requirements for the protection of health information maintained by health plans, healthcare clearinghouses, and healthcare providers who transmit certain transactions electronically. These covered entities will likely need to establish or modify existing policies and procedures to comply with this new legislation.

Legal Requirements

There are a number of laws and regulations at both the federal and state level that govern the confidentiality of health information, as outlined below.

Standards for the Privacy of Individually Identifiable Health Information

The privacy rule:

- Preempts state law contrary to the privacy rule except when one of the following three conditions is met:
    - an exception is made by the secretary of Health and Human Services
    - a provision in state law is more stringent than the rule
    - the state law relates to public health surveillance and reporting
    - the state law relates to reporting for the purpose of management or financial audits, program monitoring and evaluation, and licensure or certification of facilities or individuals
- Establishes requirements for notice and acknowledgment:
    - requires covered health providers and certain health plans to provide a notice of privacy practices
    - requires covered healthcare providers to obtain from individuals an acknowledgment that they received the notice of privacy practices
- Establishes an individual's right to:
    - opt out of the facility directory, or to request restrictions to other uses of his or her health information
    - ask that communications be sent by alternative means or to an alternate address (for example, that correspondence be sent by e-mail or to a post office box)
    - access his health information and limited situations wherein access may be denied
    - request amendment of his health information

    - obtain an accounting of disclosures of his or her health information
- Establishes requirements for use and disclosure:
    - identifies uses and disclosures for which an authorization is required
    - specifies who may authorize disclosure on behalf of an individual
    - provides special protections for psychotherapy notes
    - establishes a standard to limit the amount of information used or disclosed to the "minimum necessary" to accomplish the intended purpose
    - requires that the covered entity identify members or classes of persons within its work force who need access to protected health information (PHI), the categories of information to which access is needed, and the conditions appropriate to such access
    - establishes limitations on the use of PHI for fund raising and procedures wherein individuals must be allowed to opt out
    - establishes requirements for de-identification of health information that can be disclosed without authorization
- Establishes certain administrative requirements:
    - requires that the covered entity designate a privacy official
    - requires that the covered entity designate a contact person who can provide additional information and receive complaints
    - requires that the covered entity train all members of its work force on policies and procedures with respect to PHI
    - requires that covered entities establish appropriate administrative, technical, and physical safeguards to protect health information
    - establishes content or documentation requirements for policies and procedures, notices, authorizations, amendments, accounting of disclosures, complaints, and compliance
    - addresses fees that may be charged for disclosure
    - requires compliance by Apr. 14, 2003, for most covered entities (small health plans have until Apr. 14, 2004 to comply)

The Privacy Act of 1974

The Privacy Act of 1974 (5 USC, section 552A) was designed to give citizens some control over the information collected about them by the federal government and its agencies. It grants people the following rights:

- to find out what information was collected about them
- to see and have a copy of that information
- to correct or amend that information
- to exercise limited control of the disclosure of that information to other parties

Healthcare organizations operated by the federal government, such as Veterans Administration and Indian Health Services, are bound by the act's provisions. The act also applies to record systems operated pursuant to a contract with a federal government agency.

Confidentiality of Alcohol and Drug Abuse Patient Records

This rule (42 CFR, part 2) establishes additional privacy provisions for records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with a federally assisted drug or alcohol abuse program. When these regulations are less stringent than those of the final privacy rule, the final privacy rule would prevail. In general, the rule:

- describes the written summary and communication that must occur at the time of admission or as soon as the patient is capable of rational communication, relative to the confidentiality of alcohol and drug abuse patient records under federal law
- defines circumstances in which an individual's health information can be used and disclosed without patient authorization
- requires that each disclosure of health information be accompanied by specific language prohibiting redisclosure

- does not prohibit patient access
- defines the requirements of a written consent
- addresses who may consent on behalf of the patient

The Medicare Conditions of Participation

The Conditions for Coverage of Specialized Services Furnished by Suppliers (42 CFR, 486.161(a)) require that "clinical record information is recognized as confidential and is safeguarded against loss, destruction, or unauthorized use. Written procedures govern use and removal of records and include conditions for release of information. A patient's written consent is required for release of information not authorized by law."

The Conditions of Participation for Hospitals (42 CFR, 482.24(b)(3)) state, "The hospital must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with federal or state laws, court orders, or subpoenas."

The Conditions of Participation for Home Health Agencies (42 CFR, 484.48(b)) require that "clinical record information is safeguarded against loss or unauthorized use. Written procedures govern use and removal of records and the conditions for release of information. Patient's written consent is required for release of information not authorized by law."

The Requirements For States and Long-term Care Facilities (42 CFR, Part 483, section 483.10(b)(2)) state, "The resident or his or her legal representative has the right upon an oral or written request to access all records pertaining to himself or herself including current clinical records within 24 hours (excluding weekends and holidays) and after receipt of his or her records for inspection, to purchase at a cost not to exceed the community standard, photocopies of the records or any portions of them upon request and two working days advance notice to the facility." In section 483.10 (e), the regulation states, "The resident has the right to personal privacy and confidentiality of his or her personal and clinical records."

Institutional Review Boards

Within the provisions of the institutional review board (IRB) rules (21 CFR, part 56) are requirements that the IRB ensure informed consent is sought from each research subject or his legally authorized representative, that the consent be appropriately documented, and that where appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

State Laws and Regulations

With the exception of Montana and Washington, which passed a version of the Uniform Health Information Act, state laws relative to the privacy and confidentiality of patient health information vary widely.

States may have special privacy requirements for patients tested, diagnosed, or treated for alcohol and drug abuse, sexually transmitted diseases, or mental health disorders. There may also be privacy and confidentiality requirements within state legislation or regulation related to insurance, workers compensation, public health, or research.

Accreditation Standards

In standard IM2, the Joint Commission on Accreditation of Healthcare Organizations requires that the confidentiality, security, and integrity of data and information be maintained.

Standards of Practice

Except where a consent or authorization clearly indicates otherwise, disclosures of information made pursuant to a valid authorization will be for information originated on or before the authorization was signed.

Except as otherwise required by federal or state law or regulation, or specified in the authorization itself, an authorization will expire no later than six months after it is signed.

Recommendations

To ensure compliance with federal and state laws and regulations that protect the confidentiality of health information and govern its disclosure, HIM professionals should:

1. Study the HIPAA standards for the privacy of individually identifiable health information.
2. Identify policies, procedures, and processes that must be developed or revised to comply with these standards.
3. Become knowledgeable about other applicable federal laws and regulations relative to privacy, confidentiality, and disclosure of patient health information.
4. Become knowledgeable about state laws and regulations relative to privacy, confidentiality, and disclosure of health information. To this end, links to state laws and regulations provided on state health information management association Web sites may prove helpful. State privacy law summaries maintained on the Health Privacy Project Web site (www.healthprivacy.org) may also prove of assistance. Consider performing a key word search of state laws by accessing AllLaw.com (www.alllaw.com/state_resources) or a similar state law Web site. Other resources worth consulting include component state health information management associations' confidentiality or release of information manuals, legal counsel, and the organization's malpractice insurer.
5. Develop an understanding about which rule prevails or how various requirements can be combined procedurally. For example, how can a health information manager combine the requirements for the notice of information practices in the privacy rule with those in the Confidentiality of Alcohol and Drug Abuse Patient Records rule and any requirements in state law. As another example, consider the necessary modifications to the release of information fee schedule to comply with both federal and state regulations insofar as reasonable charges.
6. Establish policies and procedures that comply with federal and state laws and regulations.
7. Ask legal counsel to ensure that new and revised policies and procedures comply with both federal and state laws and regulations.
8. Train members of the work force on policies and procedures with respect to protected health information.
9. Maintain appropriate documentation to demonstrate compliance with federal and state privacy law and regulation.
10. Review contracts with any business associates to whom information is disclosed and make sure the language contained therein is in compliance with the privacy rule.
11. Monitor compliance and implement corrective action where indicated.
12. Non-covered entities who maintain individually identifiable health information are encouraged to construct policies and procedures in which information obtained or disclosed is the minimum necessary, the work force is trained about the importance of privacy and confidentiality, and consumers are:

    - informed about the organizations' information practices
    - provided access to health information about them
    - provided a mechanism to make amendments
    - asked for an authorization for disclosures not otherwise allowed by law
    - allowed access to and copies of disclosure logs

Prepared by

Gwen Hughes, RHIA

Acknowledgments

Mary Brandt, MBA, RHIA, CHE
Jill Burrington-Brown, MS, RHIA
Jill Callahan Dennis, JD, RHIA
Cheryl Smith, BS, RHIT, CPHQ

References

Food and Drug Administration, Department of Health and Human Services. "Institutional Review Board." *Code of Federal Regulations*, 2002. 21 CFR, Chapter I, Part 56.

Health Care Financing Administration, Department of Health and Human Services. "Conditions for Coverage of Specialized Services Furnished by Suppliers." *Code of Federal Regulations*, 2001. 42 CFR, Chapter IV, Part 486.

Health Care Financing Administration, Department of Health and Human Services. "Conditions of Participation for Home Health Agencies." *Code of Federal Regulations*, 2001. 42 CFR, Chapter IV, Part 484.

Health Care Financing Administration, Department of Health and Human Services. "Conditions of Participation for Hospitals." *Code of Federal Regulations*, 2001. 42 CFR, Chapter IV, Part 482.

Health Care Financing Administration, Department of Health and Human Services. "Requirements For States and Long Term Care Facilities." *Code of Federal Regulations*, 2001. 42 CFR, Chapter IV, Part 483.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals*. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations, 2002.

The Privacy Act of 1974. 5 USC, Section 552A. Available at www.usdoj.gov/foia/privstat.htm.

Public Health Service, Department of Health and Human Services. "Confidentiality of Alcohol and Drug Abuse Patient Records." *Code of Federal Regulations*, 2001. 42 CFR, Chapter I, Part 2.

"Standards for Privacy of Individually Identifiable Health Information; Final Rule." 45 CFR, Parts 160 and 164. *Federal Register* 67, no. 157 (August 14, 2002). Available online at http://aspe.os.dhhs.gov/admnsimp/.

Source: Hughes, Gwen. "Laws and Regulations Governing the Disclosure of Health Information" (AHIMA Practice Brief, Updated November 2002)
