Laws and Regulations Governing the Disclosure of Health Information (2014 update)

Save to myBoK

Editor's note: The following information supplants information contained in the May 2001 Practice Brief, "Laws and Regulations Governing the Disclosure of Health Information" and the November 2002 update.

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, safety, and outcome of care.

The HIPAA privacy rule became effective April 14, 2003, and established standards for information disclosure including what constitutes a valid authorization. HIPAA applies to covered entities, defined by the rule to include health plans, healthcare clearinghouses, and healthcare providers that transmit specific information electronically. The rule was amended by the final HITECH Omnibus Rule on January 25, 2013, with an effective date of March 26, 2013, and a compliance date of September 23, 2013. This final rulemaking provides increased protection and control of protected health information (PHI).

The HITECH Omnibus Rule extends disclosure requirements and associated liabilities under HIPAA to business associates. Business associates are required to comply with the same disclosure requirements as a covered entity, and these expectations typically will be addressed in the business associate agreement between the covered entity and the business associate. Refer to the practice brief "Guidelines for a Compliant Business Associate Agreement" for further guidance.

This practice brief provides a general overview of the laws and regulations impacting the timely and appropriate release of PHI. For more detailed information and guidance regarding the overall management and process of releasing PHI, refer to AHIMA's "Release of Information Toolkit."

Legal Requirements

Both state and federal rules and regulations must be considered and accounted for when disclosing PHI. The final HITECH Omnibus Rule finalized the first major changes to privacy and security practices since the HIPAA privacy rule was implemented in 2003. The act strengthened privacy and security requirements and broadened patient rights to accessing and restricting the uses and disclosures of PHI.

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 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/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/her health information except in limited situations wherein access may be denied
    - request amendment of his/her health information
    - obtain an accounting of disclosures of his/her health information
    - restrict disclosure of treatment item or service to health plans if self-paid in full
- 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 persons 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 and business associate 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 and business associates 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

The Health Information Technology for Economic and Clinical Health Act (HITECH) Omnibus Rule

The American Recovery and Reinvestment Act (ARRA) was signed into law in 2009. The Health Information Technology for Economic and Clinical Health Act (HITECH) is a defined section of ARRA that deals exclusively with health information communication and technology. Changes to HITECH, as made in the final rule (now known as the "Omnibus Rule") were effective on March 26, 2013, with a compliance date of September 23, 2013.

The HITECH Omnibus Rule strengthens the privacy rule protections by:

- Extending compliance with HIPAA to business associates and their subcontractors, including the updating of all business associate agreements
- Establishing new limitations on the use and disclosure of protected health information for marketing and fund raising purposes
- Prohibiting the sale of protected health information without appropriate authorization
- Expanding individual rights to electronically access one's protected health information
- Providing easier access by a school to childhood immunization records in states that require it for admissions
- Removing HIPAA privacy rule protections for PHI of an individual deceased for more than 50 years
- Allowing access to PHI for people who were involved in the care OR payment for care of a decedent prior to death, unless doing so is inconsistent with any prior expressed preferences of the individual that is known to the CE prior to death. This does not include past unrelated medical problems. These disclosures are permitted and not required. The ultimate decision still lies with the CE

- Expanding individuals' rights to obtain restrictions on certain disclosures of protected health information to health plans if services are entirely paid for out of pocket
- Expanding the use of compound authorizations for research purposes
    - removes the exception for limited data sets that do not contain any dates of birth and ZIP codes. This can now be considered a breach based on the outcome of the breach risk assessment
- Requiring the update to the notice of privacy practices for all organizations to include the requirements as updated under the Omnibus Rule
- Prohibiting the use of genetic information by health plans for underwriting purposes
- Finalizing breach notification requirements:
    - removes the harm threshold and adds a requirement to determine a potential breach's "risk of compromise" through the use of a breach risk assessment
    - notification of breach to patient within 60 days
- Finalizing the enforcement interim final rule strengthening and increasing penalties for violations

Refer to AHIMA's analysis of the Final Omnibus Rule and HITECH FAQs for further details:

- AHIMA Omnibus Rule Analysis
- HITECH FAQs

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 the 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.

Patriot Act

The "Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act" (USA PATRIOT Act) was signed into law on October 26, 2001. The Patriot Act is primarily a vehicle for the US government to enhance its ability to monitor and detect activities that may indicate the support for terrorism. The act is not necessarily targeted at protected health information (PHI) or systems that create, store, or manage such information. Nonetheless, it is conceivable that in pursuit of investigations being conducted under this act, a demand for PHI may be made of any healthcare provider who would be expected to comply AND who would be prevented from informing the subject of the investigation (that is, the patient).

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

Occupational Health Records

Further guidance on the management and release of occupational health records can be found in the following AHIMA resources:

- "The Privacy and Security of Occupational Health Records"
- "The Privacy and Security of Non-Traditional Occupational Health Services"

Genetic Information Nondiscrimination Act (GINA)

In 2008, the president signed into law the GINA, which expands the provisions in HIPAA to protect Americans against discrimination based on their genetic information when it comes to health insurance and employment. In the final rule, health information includes genetic information. Health plans and insurers are prohibited from imposing a preexisting condition exclusion based solely on genetic information and from discriminating in individual eligibility, benefits, or premiums based on any health factor, including genetic information.

The Medicare Conditions of Participation

PART 485 — CONDITIONS OF PARTICIPATION: SPECIALIZED PROVIDERS
485.60 Condition of participation: Clinical records states, "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 safe-guarded 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- (i) 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 (ii) after receipt of his/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/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/her 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

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. The best practice is to always follow the more restrictive regulatory guidelines when releasing information.

Accreditation Standards

In standard IM.02.01.01: The Joint Commission on Accreditation of Healthcare Organizations requires that "the hospital protect the privacy of information." Elements of performance include:

- The hospital has a written policy addressing the privacy of health information.
- The hospital implements its policy on the privacy of health information.
- The hospital uses health information only for purposes permitted by law and regulation or as further limited by its policy on privacy.
- The hospital discloses health information only as authorized by the patient or as otherwise consistent with law and regulation.
- The hospital monitors compliance with its policy on the privacy of health information.

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, the date an authorization expires is ultimately left up to the policy of the individual organization. Recommended expiration date for authorizations is no more than one year from date the authorization was signed by the appropriate party.

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. 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 all 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 laws and regulations.
10. Review contracts with any business associates to whom information is disclosed and make sure the language contained therein is in compliance with the state and federal laws.
11. Monitor compliance and implement corrective action where indicated.

12. Non-covered entities that 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 organization's information practices
    - provided access to their own health information
    - 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 (2013)

Judi Hofman, BCRT, CHPS, CAP, CHP, CHSS
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA

Acknowledgments (2013)

Becky Buegel, RHIA, CHP, CHC
Marlisa Coloso, RHIA, CCS
Dana DeMasters, MN, RN, CHPS
Kathy Downing, MA, RHIA, CHPS, PMP
Kim Turtle Dudgeon, RHIT, CHTS-IS/TS, CMT
Rose T. Dunn, MBA, RHIA, CPA, FACHE
Elisa R. Gorton, MAHSM, RHIA, CHPS
Lesley Kadlec, MA, RHIA
Michele Kruse, MBA, RHIA, CHPS
Kelly McLendon, RHIA, CHPS
Nancy Prade, MBA, RHIA, CHPS
Diana Warner, MS, RHIA, CHPS, FAHIMA

Prepared by (Original)

Gwen Hughes, RHIA

Acknowledgments (Original)

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

References

AHIMA. "Guidelines for a Compliant Business Associate Agreement." *Journal of AHIMA* 84, no.11 (November–December 2013): expanded web version.

AHIMA. "The Privacy and Security of Occupational Health Records." *Journal of AHIMA* 84, no.4 (April 2013): 52-56.

AHIMA. "Requirements for the Disclosure of Protected Health Information (Updated)." *Journal of AHIMA* 84, no.11 (November–December 2013)

AHIMA. "Release of Information Toolkit." May 2013.

"Confidentiality of Alcohol and Drug Abuse Patient Records." 42 e-CFR part 2.

Dunn, Rose, and Godwin Odia. "The Privacy and Security of Non-Traditional Occupational Health Services." *Journal of AHIMA* 84, no.11 (November–December 2013): expanded web version.

Food and Drug Administration, Department of Health and Human Services. "Institutional Review Board." *Code of Federal Regulations*, 2013. 21 CFR, Chapter I, Part 56.

Code of Federal Regulations. Title 42 Subpart B – Administration § 484.10 Conditions of participation: Patient rights (5)(d).

Code of Federal Regulations, Department of Health and Human Services. "Conditions of Participation for Home Health Agencies." *Code of Federal Regulations*, 2013. 42 CFR, Chapter IV, Part 484.

Code of Federal Regulations, Department of Health and Human Services. "Conditions of Participation for Hospitals." *Code of Federal Regulations*, 2013]. 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*, 2013. 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, 2013.

"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." 45 CFR Parts 160 and 164. *Federal Register* 78, no.17 (January 25, 2013)

Department of Health and Human Services. "New rule protects patient privacy, secures health information." Press release, January 17, 2013.

Public Law 107-56, 107th Cong. (Oct. 26, 2001), Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001.

The Privacy Act of 1974. 5 USC, Section 552A.

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).

Article citation:
AHIMA Practice Brief. "Laws and Regulations Governing the Disclosure of Health Information (2014 update)" (Updated January 2014)