

HIPAA “Privacy Primer”

Overview:

All health plans and health care clearinghouses must comply with [federal HIPAA Privacy Rules and Security Rules](#). Health care providers that conduct any of the HIPAA administrative transactions electronically must also comply with the HIPAA Privacy and Security Rules. Many providers are currently complying with the HIPAA Privacy and Security Rules as a result of already exchanging electronic HIPAA transactions.

Minnesota Statutes, section 62J.536, requires health care providers and group purchasers to exchange standard, electronic HIPAA-compliant transactions in 2009. As a result of exchanging these electronic transactions, providers must also comply with HIPAA privacy and security rules. The HIPAA “privacy primer” below is provided to help providers and payers better understand and comply with the HIPAA Privacy Rule.

What is the HIPAA Privacy Rule?

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes such as to protect public health.

The HIPAA Privacy Rule created national standards to protect individuals’ medical records and other personal health information by giving patients more control over their health information, settings boundaries on when, how, by whom and for what purpose health records can be used and disclosed, and holding covered entities accountable with civil and criminal penalties, if they violate patients’ privacy rights or other provisions of the Rule.

The HIPAA Privacy Rule was enacted to address the gaps that existed across the nation due to an uneven patchwork of federal and state privacy laws. Under this patchwork of laws, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. It establishes a Federal floor of safeguards and conditions to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

Resource:

- *Overview of HIPAA Privacy: Office for Civil Rights, Department of Health and Human Services* - <http://www.hhs.gov/ocr/privacy/index.html>

Who is Subject to Comply with the HIPAA Privacy Rule?

The overall HIPAA law (and all its administrative simplification regulations issued thereof by the Secretary of Health and Human Services) applies to three groups of entities (known as “Covered Entities”):

- All health plans, including HMOs, PPOs, health insurance companies, company health plans and government programs such as Medicare and Medicaid;

- All health care clearinghouses (vendors contracted by covered entities to process nonstandard health information and convert it into a standard electronic transaction, and vice-versa);
- Health care providers (such as hospitals, doctors, clinics, psychologists, dentists, pharmacists, chiropractors, nursing homes, etc) that conduct one of the administrative transactions named by HIPAA electronically;

This means that if a provider submits claims electronically (whether directly or via a contracted vendor), checks eligibility of a patient electronically, looks-up the status of a claim, or conducts via electronic means any of the other transactions named by HIPAA, then the provider is subject to all the HIPAA regulations, including the HIPAA Privacy Rule and the HIPAA Security Rule. "Electronic means" includes the use of internet/web-based systems such as those offered by health plans for providers to check eligibility, file claims, check the status of a claim, and request referral authorizations. Electronic means do not include fax or voice-based phone systems.

In Minnesota all health care providers will be subject to comply with the HIPAA Privacy and Security Rules since conducting transactions electronically will be required starting July 15, 2009 under Minnesota Statutes § 62J.563.

Covered entities are required to include on agreements with business associates the same privacy and security requirements they are subject to.

Resource:

- *Are You a HIPAA Covered Entity? - Centers for Medicare & Medicaid Services, Department of Health and Human Services - http://www.cms.hhs.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp#TopOfPage*

What Information is Protected by the HIPAA Privacy Rule?

The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral communication. This information is called "Protected Health Information" or PHI.

Resource:

- *Overview of HIPAA Privacy: Office for Civil Rights, Department of Health and Human Services - <http://www.hhs.gov/ocr/privacy/index.html>*

When did Compliance with the HIPAA Privacy Rule Start?

Compliance with the HIPAA Privacy Rule started April 14, 2003. In the event entities become subject to the HIPAA Privacy Rule after April 14, 2003, they will be required to comply with all provisions of the Rule immediately upon the date they become a covered entity.

What are the Core Requirements of the HIPAA Privacy Rule?

The basic principle of the HIPAA Privacy Rule is that a covered entity may not use or disclose protected health information, except when the Privacy Rule explicitly permits it or the individual subject of the information authorizes it.

The HIPAA Privacy Rule does not require the disclosure of health information, except in two instances: 1) to the individual subject to the information; and 2) to HHS when conducting a compliance investigation.

Requirements of the HIPAA Privacy Rule can be grouped into three areas:

A. Consumer Controls Over Health Information, including the rights to:

- Receive a Notice of Privacy Practices describing how covered entities will use and disclose individual's health information;
- Prohibit sharing of the individual's health information except as allowed for by laws or regulations;
- Request a restriction on the uses or disclosures of individual's health information;
- Inspect and obtain copies of the individual's health information;
- Request and amendment of the individual's health information;
- Receive an accounting of certain disclosures of the individual's health information; and
- File a complain with the covered entity or the Office for Civil Rights.

B. Restrictions on the Use and Disclosure of Health Information, including:

- *Permitted* uses and disclosures (without an individual's authorization) including
 - *To the Individual* (unless required for access or accounting of disclosures);
 - *For Treatment, Payment, and Health Care Operations* purposes;
 - When giving the individual the *opportunity to agree or object*;
 - *As an incident to an otherwise permitted use and disclosure*;
 - When done for *public interest and benefit activities*; and
 - When the information is on a *Limited Data Set* for the purposes of research, public health or health care operations
- Authorized uses and disclosures (with written authorization from individual)
 - Psychotherapy notes
 - Marketing

C. Administrative Requirements Related to the Protection of Health Information

- Establish written internal privacy policies and procedures to address all HIPAA requirements
- Designate a privacy official

- Train all workforce members on the organization's privacy policies and procedures
- Limit the use and disclosures to the minimum necessary
- Provide a Notice of Privacy Practices to consumers
- Establish and administer all consumer controls, including request for restrictions, request for amendments, request to access and obtain copies, request an accounting of disclosure, and file a complain
- Mitigate, to the extent practicable, any harmful effect to the individual of uses and disclosures done in violation to the Privacy Rule
- Maintain, at least for six year, its privacy policies and procedures, privacy practices notices, disposition of complaints, and other actions and activities required to be documented by the Privacy Rule
- Do not retaliate against a person for exercising privacy rights, reporting an act or practice it believes in good faith violates the Privacy Rule, or assist HHS in an investigation of a possible violation

What are the New Privacy Requirements Contained in the American Reinvestment and Recovery Act (ARRA) of 2009?

The recently enacted American Reinvestment and Recovery Act of 2009 (ARRA) makes important modifications and extensions to the current HIPAA Privacy Rule, including applying the HIPAA Rule directly to business associates and other non-HIPAA covered entities; allowing patients to pay out of pocket for a health care service and request non-disclosure of the rendered service; authorizing increased civil monetary penalties for HIPAA violations; defining which actions constitute a breach (including some inadvertent disclosures) and requiring breach notification; requiring an accounting of all disclosures when using an electronic health record system; and granting authority to state attorneys general to enforce HIPAA. Unless otherwise specified, the privacy provisions become effective on February 17, 2010.

More information about the HIPAA Privacy Rule can be obtained from <http://www.hhs.gov/ocr/privacy/index.html>.

What do You Have to do to Comply with the HIPAA Privacy Rule?

() Note: the following information is provided to assist entities organize their work toward HIPAA compliance, and do not constitute legal advice. Organizations should consult with legal counsel prior to taking any actions prompted by the information provided herein.*

The most important first step that you can take is to read and understand the requirements under the HIPAA Privacy Rule.

With respect to the HIPAA Privacy Rule, the following ten steps will assist you organize your compliance tasks.

1. Organize your privacy compliance plan: Prepare a formal plan for achieving compliance, document current privacy practices and prescribed requirements from the HIPAA Privacy Rule, and develop a working timeline for compliance.

2. Appoint a Privacy Official: The privacy official is responsible for the development and implementation of the policies and procedures required by the HIPAA Privacy regulations. The privacy official may also serve as the person designated to receive complaints and provide further information about matters covered by the privacy notice.

3. Develop and plan the dissemination of a Notice of Privacy Practices including: the standard notice introductory information; individual privacy rights; how information can be used and disclosed; your privacy official's contact information; a reference describing how consumers can file a complaint; and a acknowledgment of receipt. Make the Notice available to consumers at the first (or next) delivery of service. Make a good faith effort to obtain the individual's acknowledgement of receipt.

4. Develop written policies and procedures regarding the uses and disclosures of personal health information: Adopt or develop required forms to implement your privacy policies and procedures. Policies and procedures related to the use and disclosure of protected health information should cover:

- Uses and Disclosures for Treatment, Payment and Health Care Operations
- Uses and Disclosures with the Individual's Opportunity to Agree or Object
- Uses and Disclosures that Require Individual Authorization
- Uses and Disclosures that Do Not Require Individual Consent, Authorization or the Opportunity to Agree or Object

5. Establish procedures for minimum necessary uses and disclosures: Only use or disclose the information that is needed to accomplish the intended purpose, when applicable.

6. Establish Procedures to document and account for disclosures: Certain disclosure of health information must be accounted for, such as disclosures to public health, for research purposes, and others, in case a consumer wants to request an accounting of disclosures of their health information.

7. Plan for the Implementation of Individual Privacy Rights: Under HIPAA, individuals have rights to:

- Receive a Notice of Privacy Practices
- Access and copy the health information
- Request an amendment of their health information
- Request an accounting of certain disclosures of their health information
- Request restrictions on the use and disclosure of their health information
- Request communication by alternative means and to alternative locations
- File complaints regarding the handling of their health information

8. Evaluate Your Business Associate Relationships: Evaluate all your business relationships and determine which require a Business Associate agreement. You will need a Business Associate agreement with one of your vendors if the answer to all three of the following questions is “Yes”: 1) does your organization have a contractual relationship with the vendor to perform services or activities on behalf of your organization?; 2) does your organization need to supply the vendor with personal health information or access to personal health information in order for the vendor to perform its service or activity on your behalf? and 3) is the service or activity a service or activity other than treatment?

9. Implement appropriate use and disclosure restrictions in certain circumstances: Strict restrictions apply if the use and disclosure of protected health information relates to marketing activities, fundraising activities and psychotherapy notes.

10. Plan and Conduct Privacy Training of Workforce: Train your workforce about your privacy policies and procedures; establish and designate a contact person and a process to receive complaints.

Additional guidelines and resources to assist you with implementing the HIPAA Privacy Rule can be found at <http://www.hhs.gov/ocr/privacy/>.