

MEDICAL TRAVELERS, INC.

Review of HIPAA Regulations

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), one purpose of HIPAA is to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information. HIPAA applies to health plans, health care clearing houses and health care providers.

The administrative simplification provision of HIPAA has three major requirements:

- 1 - Protection for the privacy of Protected Health Information
- 2 - Protection for the security of Protected Health Information
- 3 - Standardization of electronic data interchange in health care transactions

Privacy Requirements

Rules Concerning the Use and Disclosure of Protected Health Information

HIPAA contains detailed requirements for the use or disclosure of protected health information. Covered entities may only use and disclose PHI as permitted by HIPAA or more protective state rules.

In general, covered entities may use PHI for the purposes of treatment, payment and health care operations (TPO) without any special permission from patients. Health care operations include activities such as quality assurance, peer review, training and business planning activities. Prior to the compliance date, covered entities must furnish patients a Notice of Privacy Practices that explains how the covered entity may use the patient's health information for TPO purpose and what rights the patient has with respect to his or her PHI.

Special permission, called an authorization, must be obtained for uses and disclosures other than for TPO. For example, an authorization may be required for the use of protected health information for research purposes (discussed below) or for marketing activities.

Covered entities need not obtain an authorization for some uses and disclosures, but must give the patient the opportunity to agree or object. An important example is the disclosure of health information to family or friends involved in the patient's care. Finally, in some situations, such as reporting to public health authorities, emergencies, or in research studies in which a waiver has been obtained from an Institutional Review Board ("IRB"), MMCC does not need to obtain an authorization or provide an opportunity to agree or object.

Covered entities must keep a record, or an "accounting," of disclosures made and, if

requested, provide that accounting to the patient. Covered entities do not need to account for disclosures made in connection with TPO, or made pursuant to an authorization.

Minimum Necessary

Covered entities must make reasonable efforts to ensure that it uses, discloses, or requests only the minimum necessary information. For routine disclosures, this has been achieved by the development of policies and procedures that limit the protected health information disclosed. For other disclosures, an individualized review is required. To ensure that only the minimum necessary PHI is used or disclosed, covered entities have defined role-based access to PHI to ensure that the right people are handling PHI in the appropriate way. The minimum necessary standard does not apply to sharing PHI for treatment purposes.

Research

HIPAA also addresses use of protected health information for research purposes. HIPAA requires either a patient authorization or a waiver of the authorization requirement for the use, disclosure or creation of identifiable health information for research.

An authorization is not required for research using only "de-identified" data. If a researcher uses health information from which direct identifiers have been removed, then no authorization is required but the researcher must enter a data use agreement covered with the entity that holds the records.

Marketing

The final Rule requires a covered entity to obtain an individual's prior written authorization to use his or her protected health information for marketing purposes except for a face-to-face encounter or a communication involving a promotional gift of nominal value. The Department defines marketing to distinguish between the types of communication that are and are not marketing, and makes clear that a covered entity is prohibited from selling lists of patients and enrollees to third parties or from disclosing protected health information to a third party for the marketing activities of the third party, without the individual's authorization. The Rule clarifies that doctors and other covered entities communicating with patients about treatment options or the covered entity's own health-related products and services are not considered marketing. For example, health care plans can inform patients of additional health plan coverage and value-added items and services, such as discounts for prescription drugs or eyeglasses.

Business Associates

Contractors that handle protected health information while providing a function or activity for a covered entity must satisfy certain HIPAA requirements. All contracts must require that contractors, called business associates in the regulations, use appropriate safeguards to prevent use or disclosure of the information other than as permitted by the contract. Covered entities may be held responsible for the actions of its business associates if (1) it knew of a pattern of activity of the business associate that violated the contract and (2) failed to take reasonable steps to correct the problem.

Individual Rights

The privacy rule creates five individual rights. Covered entities must furnish patients the following information about their rights.

Right to a notice of the covered entity privacy practices.

Right to request restrictions and confidential communications concerning protected health information.

Right to obtain access to protected health information for inspection and copying.

Right to obtain an accounting of certain disclosures

Right to request amendment of protected health information

Administrative Requirements

Covered entities are required to comply with a number of administrative requirements, including the following:

-Designation of a privacy official responsible for development of policies and procedures for the use and disclosure of protected health information.

-Implementation of an internal complaint process to handle complaints relating to privacy rules and to explain privacy procedures.

-Workforce training by the compliance date (for privacy standards, this is April 14, 2003).

-Implementation of administrative, technical and physical safeguards to protect the confidentiality and integrity of PHI.

-Development and enforcement of sanctions for failure to comply with policies and procedures.

-Development of procedures to mitigate adverse effects of a prohibited use or disclosure.

-Development and enforcement of policy prohibiting retaliation against a person for exercising individual rights or filing a complaint.

General Security Requirements

Covered entities are required to apply the security standard to all health information pertaining to an individual that is electronically maintained or transmitted. The Security Regulation outlines the general security measures, including administrative, technical and physical safeguards. Under the regulation, covered entities must:

-Assign responsibility for security to a person or organization.

-Assess security risks and determine the major threats to the security and privacy of protected health information.

-Establish a program to address physical security, personnel security, technical security

controls, and security incident response and disaster recovery.

-Certify the effectiveness of security controls.

-Develop policies, procedures and guidelines for use of personal computing devices (workstations, laptops, hand-held devices), and for ensuring mechanisms are in place that allow, restrict and terminate access (access control lists, user accounts, etc.) appropriate to an individual's status, change of status or termination.

-Implement access controls that may include encryption, context-based access, role-based access, or user-based access; audit control mechanisms, data authentication, and entity authentication.

Penalties

HIPAA establishes both civil monetary penalties and criminal penalties for the knowing use or disclosure of individually identifiable health information in violation of HIPAA.