HIPAA in Healthcare

Overview

This in-service provides an overview of what healthcare workers need to know about the Health Insurance Portability and Accountability Act (HIPAA) of 1996, including the implications of the privacy and security rules, and changes made through the enactment of the HITECH Act of 2009.

Purpose

The goal of this in-service is to define HIPAA, provide an overview of its guidelines and requirements, and provide information to help healthcare workers comply with all HIPAA reforms and requirements, including the privacy and security rules.

Introduction

Although the Health Insurance Portability and Accountability Act (HIPAA) has probably already caused many changes in your workplace, it is important to know as much as possible about the legislation itself, as well as its implications regarding privacy and security of patient information. This course provides an overview of what you need to know.

HIPPA: An Overview

In the middle of the 1990s, Congress took up the issue of healthcare reform. With the number of Americans changing jobs, many employees were abruptly finding themselves covered by new and different healthcare plans, often requiring them to choose new providers and transport their records to a new facility. Congress wanted to address the issue of portability, protecting healthcare coverage for employees who change jobs and allow them to carry their existing plans with them to new jobs. But given the great variety of plans in place, including HMOs, PPOs, and indemnity claims plans, it was simply not practical to require immediate portability of the exact same health insurance plan. In terms of full portability, Congress decided on a course of incremental healthcare reform. As its first incremental step, Congress passed the HIPAA act of 1996. This has been further defined and modified in subsequent years, most significantly with enactment of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.

Title I of HIPAA restates federal laws and protections that already exist, and promotes renewability of coverage by prohibiting employee health plans from denying coverage to new employees based on health status, medical history, genetic information, or disability. Title I also regulates the amount of time that coverage for a pre-existing condition can be denied, particularly if there was no significant break in coverage from a previous plan. In some cases, if there was a break in coverage, the pre-existing condition can be excluded from the new plan for as long as 18 months. Title II of HIPAA covers two main areas: preventing healthcare fraud and abuse, and a broad series of rules under the framework of administrative simplification.

The second portion of Title II–administrative simplification–contains five separate rules, most of which have already had a significant impact on virtually everyone working in American health care, including all those working in any way with health information concerning patients or clients.

Under the HITECH Act amendments, Business Associates (including vendors, subcontractors and entities that regularly access a covered entity's electronic health information) are required to comply with the administrative, physical, and technical safeguards mandated by HIPAA Security Rules, as well as the privacy protections of the Privacy Rule. Additionally, Business Associates will need to have written policies and procedures just like covered entities and will be subject to the same civil and criminal penalties for violations.

The Privacy Rule

First is the privacy rule, which applies to all protected health information (PHI). This includes any information–written, spoken or electronic–about the health status, provision of health care, or payment for health care that can be linked to a specific individual. The link could be the patient's name or it could be other identifiers, such as a birth date or medical record number. In practice, you can assume that the entire chart and all its attachments is protected health information.

The privacy rule came about because many healthcare workers have been far too willing to talk casually about their patients without thinking how this violates their confidentiality. Conversations about patients in public areas, on the telephone, in parking lots and even at home with friends and family all violate patient confidentiality. Even if patient names are not used, enough information to identify patients may be revealed. Under HIPAA regulations, you can only discuss this protected health information if it is directly related to treatment, and even then you need to limit the disclosure of any patient information to the minimum necessary for the immediate purpose. Even these legitimate disclosures of PHI must be tracked in some way.

Written Notice

Under HIPAA, the general privacy rule is that patients have to be notified of the institution's and business associates' privacy policies, and you must make a good faith effort to obtain a written acknowledgement of this. Institutions have implemented this in a variety of ways, but generally there is a HIPAA notice presented to every patient. The HIPAA notice explains to patients that their health information may be transmitted to third parties for routine use in treatment decisions, for payment, or for other healthcare processes. The notice also explains the patient's right to see his or her own medical and billing records, make changes to anything that seems inaccurate, and in certain circumstances, learn who has read the records. In general, a facility must disclose protected health information to any patient who requests it within 30 days. In addition, patients can now request that information not be disclosed to an insurance company, and this must be honored as long as the disclosure is not for purposes of treatment and the services at issue have already been paid out of pocket in full.

HIPAA allows exceptions to the requirement for a privacy notice and a written acknowledgement, in situations when it might prevent or delay timely care–for example, when you are providing emergency care. There are also some disclosures permitted under HIPAA, but they require that the patient be given an opportunity to object before the disclosure can be made. An example is disclosures made to family and friends. Other permitted disclosures that do not require patient permission include practices considered beneficial to the public. Examples include reporting vital statistics, reporting communicable diseases, and reporting adverse reactions to drugs or medical devices to the FDA.

Public announcements of patients' names are considered to be "incidental uses or disclosures" that are not violations of the privacy rule, provided that the facility has reasonable safeguards that prevent revealing any further information. In addition, the use of devices such as pagers, can be used as a way to call patients or family members in a way that maintains confidentiality.

Privacy Violations

The HITECH Act amendments to HIPAA state that if a breach of privacy occurs, the individual must be notified, and if a business associate discovers a breach he or she must notify the covered entity. If contact information for the individual is unavailable, and the breach involved more than 10 people, the covered entity must put a notice on its website or in the media with a toll-free number for information. The covered entity must also maintain a log of breaches that affect less than 500 individuals. This log is submitted to the Secretary of the HHS on an annual basis. For breaches affecting greater than 500 individuals, covered entities will be required to give notice to prominent media outlets and alert the Secretary of HHS immediately.

Bear in mind there can also be substantial civil and criminal penalties for violating patient privacy, and these penalties were increased in 2009 with enactment of the HITECH Act. Since HIPAA came into effect, OCR has referred more than 400 of the most serious cases to the Department of Justice for possible prosecution. At the extreme, anyone caught selling private healthcare information can be fined up to $250,000 and sentenced to up to 10 years in prison. Civil penalties have been increased to $1,000 per violation for a violation due to "reasonable cause and not to willful neglect" (with a maximum penalty of $100,000); $10,000 for each violation that was due to willful neglect and is corrected (subject to a $250,000 maximum penalty); and $50,000 for each violation if the violation is not corrected (subject to a maximum penalty of $1,500,000 during a calendar year). In addition, within 3 years there will be a system established that will allow individuals who were harmed by a disclosure will be able to share in civil monetary penalties collected by HHS.

Transactions and Code Set Rules

The second rule of administrative simplification is the Transactions and Code Sets Rule. To lay the groundwork for portability, this rule set standardized codes and formats for the interchange of medical data and for administrative purposes. HIPAA mandates two types of codes for the transfer of data. First and most importantly, uniform codes are needed to describe diseases and injuries, describe the causes of the diseases and injuries, and to describe the preventions and treatments used. Secondly, there are smaller sets of codes for many administrative purposes–for describing ethnicity, the type of facility or the type of unit where care was performed. As much as possible, the major codes have been chosen based on code sets that are already in use, known as "legacy codes." For example the standard coding for diagnoses is based on the International Classification of Diseases, 10th edition (ICD-10-CM). Most physician offices have been using this code source, and its predecessor, the ICD-9-CM, for years for documenting the visit and for billing.

The Security Rule

The third rule of the administrative simplification portion of Title II covers the security of healthcare data. The Security Rule applies to all electronic protected health information (PHI). This includes any information about the health status, provision of health care, or payment for health care that can be

linked to a specific individual. The link could be the patient's name or another identifier, such as a birth date, social security number, or medical record number. The HIPAA regulations laid out three types of data security safeguards: administrative, physical, and technical. Some of the provisions were required to be implemented in a specific way and others have been implemented by facilities in ways that are most suited to their situation, their physical layout and their staffing.

The Unique Identifier Rule

The fourth rule covers the use of a unique provider identifier. All healthcare providers, hospitals, physicians, healthcare clearinghouses and large health plans are now using a unique identifier in their standard transmissions of data. This unique ten-digit alphanumeric is known as the National Provider Identifier (NPI), and it replaces all previous identification numbers such as the UPIN that was used for Medicare and other similar identification numbers. The NPI does not contain any embedded information, such as the state or type of provider or specialty. It is simply a unique number identifying the provider that is used on all transmission of standard healthcare-related transactions.

The Enforcement Rule

The fifth rule covers enforcement of the HIPAA act. The Enforcement Rule sets penalties for violating HIPAA rules. It establishes procedures for investigations and hearings for HIPAA violations. Bear in mind that HIPAA regulations provide serious civil and criminal penalties for violations.

Conclusion

You should be aware of what HIPAA requires in order to help your patients' privacy and the security of their protected health information. Maintaining this confidentiality is an important underlying part of maintaining the relationship between the patient and healthcare provider.