



HIPAA: AN OVERVIEW

January 2010

Table of Contents

INTRODUCTION.....	2
ADMINISTRATIVE SIMPLIFICATION	2
ELECTRONIC TRANSACTIONS AND CODE SETS.....	2
PRIVACY	3
SECURITY.....	4
UNIQUE IDENTIFIERS.....	5
HITECH ACT AND HIT INCENTIVES	5

25 Massachusetts Ave, NW · Suite 700 · Washington, DC 20001
(800) 338-2746 · Fax (202) 835-0442 · www.acponline.org/running_practice
© ACP

HIPAA Overview

Introduction

The Health Insurance Portability and Accountability Act of 1996, known as HIPAA, was enacted on August 21, 1996, as an attempt to incrementally reform the healthcare system. The goal was to simplify and streamline the burdens of healthcare.

The original law had four key components:

- Insurance market reforms to limit exclusions for pre-existing conditions and to guarantee the renewal of group and individual insurance
- A Medical Savings Account demonstration project
- Expanded enforcement of fraud and abuse
- Administrative Simplification provisions mandating electronic handling of health insurance transactions

This guide addresses how medical practices are affected by the administrative simplification regulations for privacy, security, and electronic transactions and code sets. The Administrative Simplification provisions of HIPAA established national standards for electronic health care transactions and national identifiers for providers and employers. It also addresses the security and privacy of health data. This guide also attempts to address the changes that have occurred since the various rules took effect.

Administrative Simplification

Although the administrative simplification provisions appear in the last section of HIPAA (Title II, Section F), they are the most widely known portion of the law. The Department of Health and Human Services (DHHS) is responsible for the development of the following administrative simplification regulations:

1. Standardization of electronic patient health, administrative and financial data
2. Unique health identifiers for individuals, employers, health plans and health care providers
3. Security standards protecting the confidentiality and integrity of individually identifiable health information

The requirements outlined by the HIPAA law and supporting regulations produced by the DHHS require compliance from all healthcare organizations that maintain or transmit electronic health information. This includes physician offices, as well as hospitals, health plans, and healthcare clearinghouses.

The Office of Civil Rights (OCR) is responsible for enforcement of the Privacy and Security Rules while CMS is responsible for the Transactions and Codes Sets and Identifier Rules. Non-compliance can be costly so it is important for practices to understand their responsibilities under HIPAA.

Electronic Transactions and Code Sets

Before the enactment of HIPAA, there was no common standard for the transfer of information

HIPAA Overview

between healthcare providers and payers. Consequently over 400 electronic data interchange (EDI) formats were used by various payers. The HIPAA electronic transactions regulations were an effort to reduce paper work and increase efficiency and accuracy through the use of standardized financial and administrative transactions and data elements for transactions.

The electronic transactions regulation requires that whatever information is transmitted electronically, specifically health claims and encounter information, enrollment and disenrollment information, eligibility information, payment and remittance advice, health plan premium payments, claim status, eligibility, and referrals and authorizations, must use a standard format and code sets. Providers may still submit paper claims, but all electronic submissions must be compliant, even if submitted through a clearinghouse.

HIPAA requires all payers to accept the following transaction standards for EDI:

- Claims/encounters, eligibility verification, enrollment, and related transactions: *American National Standards Institute (ANSI) X12N* version 4010A1. However, on **January 1, 2012**, entities must use X12 version 5010. For those practices that are ready sooner, Medicare will conduct both the current 4010A1 standard and the new 5010 standards from Jan. 1, 2011, until Jan. 1, 2012, when the new version will be required.
- Physician services: *Current Procedural Terminology (CPT-4)*
- Diagnoses and inpatient hospital services: *International Classification of Diseases, 9th edition, Clinical Modification (ICD-9-CM)*. However, ICD10 CM (diagnosis) and PCS (inpatient hospital procedures) will replace ICD9 on **October 1, 2013**.
- Ancillary services/procedures: *HCFA Common Procedural Coding System (HCPCS)*
- Pharmacy transactions: *National Council for Prescription Drug Programs (NCPDP)*
- Dental services: *Current Dental Terminology (CDT)*

HIPAA adopted standards for unique identifiers for Employers and Providers, which must also be used in all transactions, as required by the standard (see below for more information on the identifiers).

Privacy

Congress recognized the need for patient-record privacy standards when they enacted HIPAA. The information protected by this section of the law includes all medical records and other individually identifiable health information whether electronic, written, or oral. With few exceptions, an individual's health information may only be used for health purposes. The final rule establishes privacy standards for physicians to meet but allows some flexibility in the design of policies and procedures in order to meet those standards.

The compliance date for the Privacy Rule was April 14, 2003. The privacy regulations outline specific rights for individuals regarding protected health information and obligations of healthcare providers, health plans, and health care clearinghouses. These standards grant healthcare consumers a greater level of control over the use and disclosure of personally identifiable health information. In general, healthcare providers, health plans, and clearinghouses are prohibited from using or disclosing health information except as authorized by the patient or specifically permitted by the regulation. The final rule's applicability was expanded to include

HIPAA Overview

all personally identifiable health information, irrespective of form. The regulations are applicable to all health information held or created by the covered entity. This expanded coverage was intended to eliminate potential confusion from treating various categories of records differently.

The rule established requirements for covered entities and specific rights for patients. For instance, providers and health plans must inform their patients/beneficiaries of their business practices concerning the use and disclosure of health information. Direct healthcare providers need not obtain written consent from a patient for use and disclosure of health information if the use or disclosure is related to routine purposes such as treatment or payment. A separate, specific authorization is required for non-routine disclosures.

Healthcare providers and health plans are required to create privacy-conscious business practices, which include the requirement that only the minimum amount of health information necessary is disclosed. In addition, business practices should ensure the internal protection of medical records, employee privacy training and education, creation of mechanisms for addressing patient privacy complaints, and designation of a privacy officer. Overall, covered entities are encouraged to use de-identifiable information whenever possible. Once information is de-identified, it is no longer subject to the privacy regulation restrictions.

Security

Despite years of work by standards development organizations (SDO's), there was no recognized single standard for the security of health information that includes all of the components required by HIPAA. So DHHS developed a security standard with input from these SDO's and business interests. The security standards are generally technology neutral and scaleable for the size and complexity of healthcare organizations. The compliance deadline was April 21, 2005.

There are 18 standards with which practices must comply. However, the standards have "implementation specifications" that are either "required" or "addressable," thus making the Rule scalable, flexible, and technologically neutral. If the implementation specification is "addressable," the practice must assess whether it is reasonable and appropriate to implement. If it is reasonable and appropriate, then the practice must implement. If not, the practice must document why it would not be reasonable and appropriate and implement an equivalent alternative measure that is reasonable and appropriate.

The standards are divided into three areas: administrative, physical, and technical safeguards of all electronic protected health information (EPHI). Electronic means any PHI stored in or transmitted by electronic media. In summary, the Security Rule requires the following:

1. Administrative safeguards are policies, procedures and other administrative actions that implement or maintain security measures to protect electronic health information and manage the conduct of employees to protect that information.
2. Physical safeguards are physical measures, policies, and procedures that protect the practice's information systems and related buildings and equipment from natural or environmental hazards and unauthorized intrusion.

HIPAA Overview

3. Technical safeguards are technology, policies, and procedures that protect and control access to EPHI.

Unique Identifiers

HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services (patients).

The National Employer Identifier has been in use since July 30, 2004. The employer identifier is based on the de facto standard, the Internal Revenue Service assigned Employer Identification Number (EIN), which has nine numeric positions.

The National Provider Identifier (NPI) has been in effect since May 23, 2007. A new unit of CMS, the National Plan and Provider Enumeration System (NPPES), issues the unique 10-digit numeric NPI for all health care providers, including physicians, group practices, hospitals, and other providers of healthcare services designated as covered entities under HIPAA. The NPI has no identifying features and replaces all other identifiers (e.g., UPIN and insurance provider IDs). Physicians may apply online through NPPES:

<https://nppes.cms.hhs.gov/NPPES/Welcome.do>.

The patient identifier is currently on hold. However, industry experts speculate that the identifier will consist of approximately ten numeric digits with a check digit.

HITECH Act and HIT Incentives

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) of the American Recovery and Reinvestment Act of 2009 (ARRA) (Pub. L. 111–5), was enacted on February 17, 2009. The HITECH Act amended the Public Health Service Act (PHSA) and created “Title XXX – Health Information Technology and Quality” to improve health care quality, safety, and efficiency through the promotion of health information technology (HIT) and the electronic exchange of health information. HITECH includes massive new privacy and security requirements, and the resulting regulations really must be digested thoroughly by practices of all sizes. In addition, HHS Office of the National Coordinator of HIT (ONC) published preliminary rules on December 30, 2009 about what qualifies as “meaningful use” and about the proposed certification process for EHR systems.

For more information on these rules, see

http://www.acponline.org/running_practice/technology/faq.pdf.