HIPAA: AN OVERVIEW

September 2013

Introduction

The Health Insurance Portability and Accountability Act of 1996, known as HIPAA, was enacted on August 21, 1996. The overall 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- A Medical Savings Account demonstration project (which has since been replaced by other programs)
- Expanded enforcement of fraud and abuse
- Administrative Simplification provisions mandating electronic handling of health insurance transactions and information.

It is the Administrative Simplification provisions that have the greatest impact on medical practices. 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.

Developments in technology and the ability to gain easy access to personal health information have driven efforts to streamline diverse state regulations and insurance company requirements into a single regulation. The passage of HIPAA and later the Health Information Technology for Economic and Clinical Health (HITECH) Act occurred, in part, to improve the efficiency and effectiveness of the healthcare system by standardizing the transmission of certain administrative and financial transactions and by protecting the privacy and security of personal health information. However, in January 2013, the U.S. Department of Health and Human Services (DHHS) Office for Civil Rights (OCR) announced a final "omnibus" rule implementing revisions to HITECH Act and to strengthen the privacy and security protections for health information established HIPAA.

This guide summarizes how medical practices are affected by the Administrative Simplification regulations for privacy, security, electronic transactions and code sets, and breach notification. This overview also attempts to address the changes that have occurred since the various rules took effect, including and especially the Omnibus Rule of January 2013.

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, including claims, remittance advice, electronic funds transfer, and so on.
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 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 5010.
- 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, 2014**.
- 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, providers, and health plans which must also be used in all transactions, as required by the standard.

HIPAA Overview

Privacy and Security

Congress recognized the need for patient-record privacy and security 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 treatment, payment, or operations purposes. The final rules established standards for physicians to meet but allowed some flexibility in the design of policies and procedures in order to meet those standards.

The original compliance date for the Privacy Rule was April 14, 2003, and for the Security Rule was April 21, 2005. Since that time, the Office of Civil Rights (OCR), which is in charge of enforcement, has issued clarifications and FAQs regarding how to implement various aspects of the privacy rules. The issuance of HITECH and now the Omnibus rule have resulted in further changes.

The most notable changes to previous privacy and security rules resulting from the Omnibus rules effective September 23, 2013 are as follows:

- Business associates (BA) are now directly responsible for privacy and security of protected health information, especially when it comes to uses and disclosures. BA agreements must be revised accordingly by September 30, 2014, or when the agreement is otherwise renewed or modified prior to that time, whichever is first.
- The definition of marketing for which patient authorization is needed was expanded. While more information can now be used for fundraising, patients may opt out of fundraising activities.
- The omnibus rule changed the definition of what constitutes a breach of personal health information (PHI). Now, any disclosure of PHI that is a violation of the Privacy rule is considered a breach unless it can be demonstrated by a risk assessment that the breach meets certain criteria.
- Patients who pay out of pocket may request that PHI not be sent to their health plan.
- Upon request, practices that store PHI electronically must provide the patient with an electronic copy of the records within a specific time frame and for a "reasonable" cost.
- The Notice of Privacy Practices must be updated to include these changes by September 23, 2013.
- The PHI of deceased patients is protected for 50 years. If the patient wishes are unknown, then family members who were involved in the care and payment are authorized and others are not.

Unique Identifiers

HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services (i.e. 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 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 replaced all other identifiers. Physicians may apply online through NPPES: https://nppes.cms.hhs.gov/NPPES/Welcome.do.

The national Health Plan Identifier (HPID) final rule was released August 24, 2012. This rule establishes a unique identifier for health plans and for other entities that are not providers, health plans, or individuals that need to be identified in standard transactions. Health plans, excluding small health plans, are required to obtain HPIDs by 2 years after the effective date, in **2014**. Small health plans are required to obtain HPIDs 3 years after the effective date, in **2015**. All covered entities are required to use HPIDs where they identify health plans that have HPIDs in standard transactions 4 years after the effective date, in **2016**.

The patient identifier is currently on hold and there is no speculation on when a new rule will be released regarding patient identifiers.

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 included provisions to improve health care quality, safety, and efficiency through the promotion of health information technology (HIT) and the electronic exchange of health information. HITECH included new privacy and security requirements, the most well-known being the EHR incentive programs. For a good summary of these programs, go here: http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Beginners_Guide.pdf.

Affordable Care Act (ACA)

The Administrative Simplification provisions of the Affordable Care Act of 2010 (ACA), build on HIPAA with several new, expanded, or revised provisions, including requirements for:

- Operating rules for each of the HIPAA transactions (including ICD-10)
- Enumeration of a unique, standard Health Plan Identifier (HPID)
- New standards for electronic funds transfer (EFT), electronic remittance advice (ERA), and electronic health care claims attachments. Claims attachment rules are not expected before 2014 or later.
- Health plans to certify compliance with the standards and operating rules.
- Penalties for health plans that fail to comply or to certify their compliance with applicable standards and operating rules.

Eligibility Determination, Electronic Funds Transfer (EFT) and Electronic Remittance

Advice (ERA)

On July 8, 2011, HHS published a regulation, an interim final rule that adopted operating rules for two electronic health care transactions to make it easier for physician practices and hospitals to determine whether a patient is eligible for coverage and the status of a health care claim submitted to a health insurer. The effective date for operating rules for eligibility for health plan and health claims status transactions was January 1, 2013.

On January 10, 2012, HHS published another interim final rule adopting standards for health care claim payments made via EFT and for ERA. The compliance date for the EFT and ERA operating rule is January 1, 2014.

Other Administrative Simplification Rules Still to Come

Future administrative simplification rules will address the adoption of:

- A standard unique identifier for health plans;
- A standard for claims attachments; and
- Requirements that health plans certify compliance with all HIPAA standards and operating rules.