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.

HIPAA Overview

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)*

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.

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

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.