HIPAA: Understanding the Requirements (HIPAA on the Job)

by Bonnie Cassidy, MPA, RHIA, FHIMSS

(Editor's note: This is the first in a series of special inserts intended to help HIM professionals educate themselves about the Health Insurance Portability and Accountability Act [HIPAA] of 1996. In this installment, we take a look at this groundbreaking legislation from a nuts-and-bolts perspective. In future inserts, we'll look at more complex issues related to HIPAA.)

The primary intent of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (also known as Public Law 104-191) is to protect health insurance coverage for workers who change or lose their jobs. The **administrative simplification** provisions of HIPAA are found in **Title II, subtitle F** of this legislation.

What is Administrative Simplification?

The administrative simplification provisions aim to:

- improve the efficiency and effectiveness of the healthcare system by **standardizing** the electronic transmission of certain administrative and financial transactions
- protect the security and privacy of transmitted information

HIM Impact—What Does This Mean to Me?

National standards aim to achieve administrative savings and reduce the administrative burden on healthcare providers and health plans. Today, most providers and plans use many different electronic formats, with many different data requirements, to exchange claims, remittance advices, and other transactions. **A national standard means one format for electronic transactions.**

Once the standards are in place, providers will be able to submit a standard transaction containing standard content to any health plan and that plan will have to accept it. Furthermore, plans will be able to send one standard transaction (remittance advice or claim) to providers. National standards will make electronic data interchange (EDI) a viable alternative to paper processing.

A Look at the Provisions

HIPAA requires the Secretary of Health and Human Services (HHS) to adopt **standards for nine administrative and financial healthcare transactions.** These are:

1. health claims or equivalent encounter information
2. health claims attachments
3. enrollment and disenrollment in a health plan
4. eligibility for a health plan
5. healthcare payment and remittance advice
6. health plan premium payments
7. first report of injury

8. health claim status
9. referral certification and authorization

HIM Impact—What Does This Mean to Me?

To begin, understand that "HIPAA compliance" refers to all electronic claims transactions—not just for Medicare or Medicaid. These nine areas must be in compliance if you work at a physician's office, hospital, healthcare plan, fiscal intermediary, outsourced or consolidated business office, vendor, payer, or data clearinghouse. Healthcare providers who elect to conduct the administrative and financial transactions electronically must comply with the standards.

When Does My Employer Need to Be in Compliance?

Once HIPAA regulations are finalized, there will be a 24-month implementation or grace period. Small health plans will have 36 months to comply. There are specific penalties for failure to comply with the requirements and standards and wrongful disclosure of individually identifiable information.

Who Will Monitor Compliance?

We don't know yet. Every HIM director should anticipate self-reporting or surveys of compliance in the next two years. At a minimum, every healthcare organization dealing with electronic claims transactions should be preparing for HIPAA compliance. The first step is to understand the regulations, standards, and proposed rules.

Identifiers

HIPAA also directs the Secretary of HHS to adopt standards for unique health identifiers for:

- individuals
- employers
- health plans or payers
- healthcare providers

HIM Impact—What Should I Know About Unique Identifiers?

HHS published the notice of proposed rule-making for a **national provider identifier** in 1998. The proposed standard for national provider identifier is an eight-position alphanumeric identifier that includes a check digit in the last position. The identifier would be implemented through a central electronic enumerating system and would be managed by HCFA. Identifiers would be issued by one or more organizations known as "enumerators."

Currently, there is no specific information on the **payer ID for payers/health plans**.

The proposed standard for **employer identifiers** would be the employer identification number assigned by the Internal Revenue Service.

Individual health identifiers do not have a standard and will not until legislation is enacted specifically approving the standard. Individual identifiers have been controversial because of the perception that "access" to all information on an individual could be obtained through a single identifier. As a result, Vice President Al Gore put a hold on this standard until a federal privacy law that offers recourse to individuals is created.

The whole concept of privacy versus wrongful disclosure is truly at stake here. Two different task forces have been created to investigate possible identifiers.

Other Standards to Know About

HIPAA also mandates standards for:

- code sets
- security
- electronic signatures
- coordination of benefits

HIM Impact—What Are Code Sets?

Under HIPAA, a code set is any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes, procedure codes, etc. Code sets for medical data are required for data elements in the administrative and financial transaction standards adopted under HIPAA for diagnoses, procedures, and drugs. ICD-9-CM is an example of a code set.

What Do We Need to Know About Security Standards?

HIPAA mandates the adoption of **new** security standards to protect an individual's health information while permitting the appropriate access and use of that information by providers, clearinghouses, and health plans. The law also mandates that a new electronic signature standard be used where an electronic signature is employed in the transmission of a HIPAA standard transaction.

The proposed standard for **security of health information and electronic signatures** was published in 1998. The proposed standard requires healthcare entities that engage in electronic maintenance or transmission of health information to **assess** their own security needs and risks and **devise, implement, and maintain** appropriate security to address their business requirements. These required measures, which must be documented and maintained regularly, are:

- administrative procedures
- physical safeguards
- technical security services
- technical security mechanisms

What Are the Requirements for Each of These Categories?

Administrative procedures—there must be formal, documented practices to manage the selection and execution of security measures to protect data as well as the conduct of personnel in relation to the protection of data

Physical safeguards—physical computer systems and related buildings and equipment must be protected from fire and other natural and environmental hazards, as well as from intrusion

Technical security services—these processes must be implemented to protect information and control and monitor individual access to information. Services include access control, audit controls, authorization control, data authentication, and entity authentication

Technical security mechanisms—processes to prevent unauthorized access to data that is transmitted over a communications network should be implemented

What Are the Requirements for Electronic Signatures?

If an entity elects to use an electronic signature in a HIPAA-specified transaction, the entity must apply the electronic signature standard. The standard for an electronic signature is a **digital** signature based on cryptographic methods of originator authentication, computed with a set of rules and parameters that allow for the verification of the identity of the signer and the integrity of the data.

What Features Must Be Present as We Build Our Electronic Signature System?

The signature method must assure message integrity, nonrepudiation, and user authentication.

The entity may also use, among others, any of the following implementation features:

- ability to add attributes
- continuity of signature capability
- countersignatures
- independent verifiability
- interoperability
- multiple signatures

How Are the Security and Privacy Rules Different?

In the world of HIPAA, privacy and security are different. While the security standards are specifically mentioned in Subtitle F, the privacy regulations come from a different section of the law.

In a nutshell, security encompasses the measures healthcare organizations must take to protect the information within their possession from internal and external threats. Privacy is the consumer's view of the way his/her information is treated.

As noted above, the proposed privacy rule was published at the end of 1999. At press time, no date for a final rule had been scheduled.

Understanding the Standards Adoption Process

In general, standards that are adopted are developed, adopted, or modified by a standards development organization (SDO) accredited by the American National Standards Institute (ANSI). ANSI includes organizations such as X12N, HL7, and the American Society for Testing and Materials (ASTM). The secretary of HHS will rely on the National Committee on Vital and Health Statistics to provide input on all proposed standards. The HHS Data Council, an internal advisory committee to the secretary, also plays an important role in addressing issues related to the proposed standards.

Currently, X12N standards exist for the majority of administrative and financial transactions mandated under HIPAA.

A standard may **not** be adopted unless the SDO has consulted with the:

- National Uniform Billing Committee
- National Uniform Claims Committee
- Workgroup for Electronic Data Interchange
- American Dental Association

HIM Impact—Where Can I Get More Information on Any of These Standards?

The Implementation Guides for the X12N Standards are available at no cost from the Washington Publishing Company web site at www.wpc-edi.com/hipaa/. Bound copies may be purchased as well.

Will Any Diagnostic Coding Requirements Change?

It is recommended that the industry continue with the current systems for diagnosis (ICD-9-CM); procedure (ICD-9-CM and CPT-4); dental (CDT); drug codes (NDC); and other health-related services (HCPCS).

It is anticipated that the industry will move forward with ICD-10 and that we will make some changes in time. Health plans, clearinghouses, and providers must use the proposed code sets in all electronic transactions. Official coding guidelines must be followed, as always.

From the payers' perspective, one of the biggest issues about HIPAA is that the transactions and code set standards are **mandatory** for them, but providers still have a choice. So for at least some period of time, payers will need the capability to handle both electronic and manual transactions while providers can submit either one.

Similarly, from a code set standpoint, while we currently use ICD-9, ICD-10 will probably become final some time during the two-year implementation period. Payer systems again will need the capability to handle both code sets, in stages. Everyone will have to follow the code sets, but the implementation, from a timing perspective, will be different.

Resources

Useful Web sites to obtain HIPAA information include:

- Washington Publishing Company Web site. Available at www.wpc-edi.com/hipaa/.
- The HHS administrative simplification Web site. Available at http://aspe.os.dhhs.gov/admnsimp/.

HIPAA Regulations: Current Time Frames

Time frames for implementation of HIPAA regulations are subject to change. As of February 2000, this was the most recent timetable. Check the HHS Web site at http://aspe.os.dhhs.gov/admnsimp/pubsched.htm for continuous updates.

Regulation	Proposed rule published	Final rule expected
Transactions	May 1998	March 2000
Code Sets	May 1998	March 2000
Unique Identifiers		
Plan	expected April 2000	April 2001
Provider	May 1998	June 2000
Employer	June 1998	March 2000
Individual	On hold	On hold
Security	August 1998	May 2000
Electronic Signatures	August 1998	2Q 2000
Information Between Health Plans	May 1998	1Q 2000
Privacy	November 1999	Unknown

What Key Transaction Standards Do I Need To Know?

Type of Claim	Standard
All transactions except claims	X12N Version 4010
Pharmacy Claims	National Council for Prescription Drug Programs Telecommunication Standard 3.2
Medical, dental and institutional claims	X12N 837
Claims attachment	No standards
First report of injury	No standards

Bonnie Cassidy *is principal of the North Highland Company, Atlanta, GA. She can be reached at bcassidy@north-highland.com.*

Article citation:
Cassidy, Bonnie. "HIPAA: Understanding the Requirements (HIPAA on the Job)." *Journal of AHIMA* 71, no.4 (2000): 16A-D.