DISCOVER THE DIFFERENCE

TEOCO Healthcare Solutions

HIPAA OVERVIEW

TEOCO
CORPORATION

TEOCO HEALTHCARE SOLUTIONS
Delivering Optimal Healthcare Decisions by Merging the Business of Healthcare with the Intelligent Application of Technology ™

TABLE OF CONTENTS

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into effect by President Clinton to protect health insurance coverage for workers and their families when they change or lose their jobs (Portability) and to protect health data integrity, confidentiality, and availability (Accountability).

It consists of Titles I-V and places various legal requirements on the health care industry. Title II will have the biggest impact on business partners exchanging electronic transaction data, specifically: Preventing Health Care Fraud and Abuse, Administrative Simplification, and Medical Liability Reform.

Administrative Simplification Provision

HIPAA Title II, Subtitle F contains the provisions that pose the greatest challenge to healthcare organizations today and is called Administrative Simplification. Its goal is to reduce the costs and administrative burdens of healthcare through standardization, improved security standards and contains provisions related to patient confidentiality and privacy. Electronic signature is also addressed. The Administrative Simplification provisions of HIPAA (HIPAA-AS) establish various protections, standards and requirements for the transmission, storage and handling of electronic health care transactions. Organizations effected include all entities that maintain or transmit electronic "health information"; health care payers including insurance companies, government agencies, private health plans, hospitals, nursing homes; physicians and other health care providers, and health care clearinghouses. The business partners of these entities are also covered including third party administrators, practice management system vendors, billing agents and other health care service organizations. HIPAA provisions may also require changes in state statutes, rules, regulations, and reimbursement policies. States must look closely at the requirements and determine the overall impact of HIPAA on their agencies.

The goals of HIPAA-AS provisions

- Enhance the flow of information by creating unique identifiers for the constituents in healthcare; patients, providers, payers and employers.
- Secure the healthcare environment and confidentiality of healthcare information through establishing security and privacy standards.
- Reduce administrative costs through standardization of transaction formats and code sets.

Key provisions of the law

- Monetary penalties for violations of the standards ranging from $50,000 to $250,000 and up to ten years in prison for violations of the proposed privacy standards.
- Monetary penalties of not more than $100 per violation on any person who fails to comply with a standard other than the privacy standard, except that the total amount imposed on any one person in each calendar year may not exceed $25,000 for violations of one requirement.
- Standards can not be changed during the first year of implementation and not more frequently than every 12 months thereafter.
- Standards supersede contrary state law, with the exception of privacy law.
- Most organizations have two (2) years from the effective date in which to implement standards. Effective date is 60 days after final rule, unless otherwise specified. To date, only the transaction standards have been finalized.

HIPAA is not just an information technology issue. The provisions result in operational issues that will modify the day-to-day routine of every health care organization. Managing the significant changes in business processes and cultural values will equal in importance managing the technical challenges that are associated with each category of standards.

Transaction Standards

[http://aspe.os.dhhs.gov/admnsimp/faqtx.htm].

Currently, there is no common standard for the transfer of information between constituents in healthcare. This has resulted in some providers and payers supporting hundreds of formats at great administrative expense. Under HIPAA, one common format will be employed by all constituents for each transaction type (i.e., claims/encounters, eligibility verification, enrollment, etc.) The law applies to all named transactions between covered entities and their "business partners" and other covered entities.
Covered Transactions -- For the purpose of HIPAA, a "transaction" means any of the following:

- Health claims or equivalent encounter data.
- Health care payment and remittance advises.
- Coordination of benefits.
- Health claim status inquiries.
- Enrollment and disenrollment transactions.
- Eligibility verification inquiry.
- Health plan premium payment transactions.
- Referral certification and authorizations.
- First report of injury.
- Health claims attachments.
- Other transactions as the Secretary may prescribe by regulation.

In the proposed rule HHS provided that certain technologies- telephone voice response, "faxback", and Hyper Text Markup Language (HTML) interactions - would not be required to follow the standard. HHS reevaluated this position in light of the many comments on this position and on developments in the EDI industry, which continue to expand the options in this area. HHS has decided that, instead of creating an exception for these transmissions, the final rule will recognize that there are certain transmission modes in which use of the format portion of the standard is inappropriate. However, the transaction must conform to the data content portion of the standard. The "direct data entry" process, using dumb terminals or computer browser screens, where the data is directly keyed by a health care provider into a health plan's computer, would not have to use the format portion of the standard, but the data content must conform. If the data is directly entered into a system that is outside of the health plan's system, to be transmitted later to the health plan, the transaction must be sent using the full standard (format and content). HHS has included this clarification in §162.923 (Requirements for Covered Entities).

Standards

In compliance with the provisions of HIPAA, the Secretary of HHS issued the final regulation -- Standards for Electronic Transactions on August 17, 2000. It adopts the standards set forth below as implemented through the appropriate implementation guides, data content and data conditions specifications, and data dictionary:

Health Care Claim and equivalent Encounter:	Retail prescription drug claim: Dental claim Professional claim Institutional claim	NCPDP Telecommunication Claim Version 5.1 or equivalent NCPDP Batch Standard Version 1.0 ASC X12N 837 - Health Care Claim: Dental ASC X12N 837 - Health Care Claim: Professional ASC X12N 837 - Health Care Claim: Institutional
Health care payment and remittance advice:		ASC X12N 835 - Health Care Payment/Advice. The final rule named NCPDP for remittance advice, but HHS has publicly stated at the Phoenix SNIP meeting and October X12 meeting that this is incorrect and will be changed to the 835.
Coordination of Benefits	Retail prescription drug claim Dental claim Professional claim Institutional claim	NCPDP Telecommunication Standard Version 5.1 or equivalent NCPDP Batch Standard Version 1.0 ASC X12N 837 - Health Care Claim: Dental ASC X12N 837 - Health Care Claim: Professional ASC X12N 837 - Health Care Claim: Institutional
Health Claim Status		ASC X12N 276/277 - Health Care Claim Status Request and Response
Enrollment and disenrollment in a health plan:		ASC X12 834 - Benefit Enrollment and Maintenance
Eligibility:		ASC X12N 270/271 - Health Care Eligibility Benefit Inquiry and Response
Health insurance premium payments		ASC X12 820 - Payment Order/Remittance Advice
Referral certification and authorization		ASC X12N 278 - Health Care Services Review - Request for Review and Response. The final rule did name the 278 for all entities, but HHS has publicly stated at the Phoenix SNIP meeting and October X12 meeting that this is incorrect and will be changed to the NCPDP Version 5.1.

Effective Dates

[http://aspe.os.dhhs.gov/admnsimp/pubsched.htm]

Most constituents will have to comply with transaction and code set standards by October 16, 2002. A small health plan has an additional 12 months to complete implementation. HHS defines a "small health plan" as a group health plan with annual receipts of $5 million or less.

Code Set Standards

[http://aspe.os.dhhs.gov/admnsimp/faqcode.htm]

- International Classification of Diseases - 9th Revision - Clinical Modification (ICD-9-CM) Volumes 1,2 and 3.
- Physician Current Procedural Terminology (CPT-4) which are HCPCS level 1.
- Health Care Financing Administration (HCFA) Common Procedure Coding System (HCPCS) level 2
- National Drug Codes (NDC) for prescription drugs
- Current Dental Terminology (CDT-2) codes for dental services.

While most organizations utilize these code sets, many use them with some kind of local customization. Local codes will be eliminated as will J-codes and other alpha-numeric HCPCS that refer to drugs. In addition, knowing which version is applicable at any given time can be difficult. HHS indicated that all HCPCS identifying drugs will be eliminated.

There are no separately named codes for behavioral health diagnosis or procedures and behavioral health entities will need to work together to get their codes added as a separate standard code set or added to the currently named standards.

Organizations can meet the requirements either by transmitting and receiving standard data elements or by submitting non-standard data elements to a clearinghouse for transmission and receiving non-standard data elements through the clearinghouse.

Unique Health Identifiers

Standards for unique health identifiers include identifiers for payers, providers, employers and individuals. These standards are meant to ease the administrative challenge of maintaining and transmitting clinical data across disparate episodes of patient care. HHS has proposed standards for payers and providers, the National Health PlanID [http://www.hcfa.gov/hcfainit.htm], formerly known as the PAYERID and the National Provider Identifier (NPI) respectfully. Also, the widely used Employer Identification Number (EIN) is specified for use as the unique employer health identifier. Due to privacy concerns, the standard identifier for individuals has been delayed. All these standards are subject to change resulting from the NPRM process.

Organizations will need to translate existing identifiers into the new identifiers and applications and workflow will need to be modified. In addition, new standard identifiers will be released on an incremental basis.

National Provider Identifier (NPI)

[http://www.hcfa.gov/stats/npi/overview.htm]

Each provider will be issued a single NPI that will remain unchanged over time. The NPI will contain no embedded intelligence, to identify location or specialty, for example. It has recently been modified and will probably consist of a ten character numeric, rather than the initial eight character alpha-numeric identifier.

Employer Identifiers (EIN)

[http://aspe.os.dhhs.gov/admnsimp/faqemp.htm]

DHHS has proposed a nine position numeric, the Tax ID Number, administered by the Internal Revenue Service.

National Nealth PlanID

[http://www.hcfa.gov/hcfainit.htm]

The anticipated standard is a nine position numeric, including one check digit. DHHS is likely to announce the proposed National Health PlanID, formerly the PAYERID rule soon.

Patient Identifiers

This is clearly the most controversial. Announcement of a universal patient identifier is not expected until patient privacy protections have been put forth.

Security & Electronic Signature Standards

[http://aspe.os.dhhs.gov/admnsimp/nprm/seclist.htm].

Security Standards are to protect the confidentiality and availability of health care information. They apply to all health care organizations and their business partners that transmit or maintain electronic health information, not just those that solely transmit electronic data as with other provisions of HIPAA-AS. Administrative, physical and technical controls are to be established. The proposed security standards are subject to change through the NPRM process and include a comprehensive schedule of security requirements. HIPAA's proposals are technology neutral by design partly due to the fact that security technology is changing rapidly. The measures that may be employed are varied and scalable and it is up to the organization to deploy the appropriate measures commensurate with their exposure and risk levels.

The proposed standards cover both organizational and technical practices. DHHS divides proposed security requirements into the following five areas of compliance.

- ***Administrative Procedures*** - Documented practices for establishing and enforcing security policies that guard data integrity, availability and confidentiality. These also must address staff responsibilities for protecting data. Requirements such as training, information access control, security management, incident and termination procedures are covered in this section of the regulation. Chain of Trust agreements must be put in place in order to protect data exchanged between covered entities and their business partners. This section of the regulation also addresses contingency planning including data backups, alternate processing options and disaster recovery procedures. Covered entities must develop formal mechanisms for the processing of records that contain health information including receipt, manipulation, storage and transmission of those records.
-
- ***Physical Safeguards*** - There must be documented processes to protect data integrity, availability and confidentiality. Safeguards protect physical computer systems, buildings, equipment from fire and other environmental hazards as well as intrusion. A security officer or department must be assigned the responsibility for security. Policies on workstation use and security are addressed as well as the use of physical locks, security systems, and administrative measures.
-
- ***Technical Security Mechanisms*** - Mechanisms, including business processes, to prevent unauthorized access to data or information transmitted over a communications network (data in transit). The following implementation features must be implemented over an open network: access controls, encryption. In addition alarm, audit trail, entity authentication and event reporting must be implemented.
-
- ***Technical Security Services*** - These are services or processes to guard the integrity of data integrity, availability and confidentiality within a system. These include the use of passwords and other means to monitor, control and protect access. There must be audit controls that record and examine system activity related to data authentication and entity authentication.
-
- ***Electronic Signature Standards*** - If a digital signature is employed, the following three implementation features must be implemented: (1) message integrity, (2) non-repudiation, and (3) user authentication. There are other optional features. HHS has indicated that the final security regulations will be published without the standard for electronic signature and that this part of the regulation will be delayed for some time.

Implementing security standards will result in many changes to business policy and processes, physical facilities, workflow and culture. Meeting the technical requirements may require redesign of existing systems as each user must be individually identifiable and each data access must be uniquely associated with an authenticated identity.

Privacy Protections

[http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=228]

Security and privacy provisions are sometimes confused. Privacy protections protect the confidentiality of the patient's individual medical information. It is an individual right. Security relates to the protective measures put in place to enforce policy regarding confidential information.

HIPAA privacy standards will apply to all forms of protected information (e.g. paper, oral, electronic) once any patient identifiable health information has been electronically stored or transmitted. Since it can be hard to know whether information has ever been electronically stored or transmitted, many health care organizations plan on treating all paper and oral information as protected information.

HIPAA defines individual information as "any information, including demographic information collected from an individual that:

1. is created or received by a health care provider, health plan, employer or health care clearinghouse; and
2. is related to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and;
   a. Identifies the individual; or
   b. b. With respect to which there is a reasonable basis to believe that the information can be used to identify the individual."

The privacy NPRM was published on November 3, 1999. Comments were accepted through February 3, 2000. A final privacy standard has not been announced as of this date. but is expected before the end of the Clinton administration. Privacy provisions do not pre-empt State laws unless the State law is weaker.

Proposed Privacy Regulation

- **Consumer Control** - providing consumers with new rights regarding access to their health information.
- **Accountability** - A violation carries civil and criminal penalties of up to $250,000 in fines and 10 years imprisonment.
- **Public Responsibility** - privacy protections must be balanced with research, public health, quality of care monitoring and fraud and abuse control.
- **Boundaries** - health information can for the most part only be used for health purposes.
- **Security** - organizations must protect such information against misuse or disclosure, whether inadvertent or purposeful.

Complying with privacy regulations are expected to cause healthcare organizations to invest significant resources.

Next Steps

In order to comply with HIPAA provisions, organizations must do the following:

- Establish a framework for stakeholder buy-in. Conduct an executive awareness session to provide an overview of HIPAA rules and regulations. Senior management must understand HIPAA in order to drive the process and understand the resources required.
- Conduct enterprise wide HIPAA training for departmental managers and those that must participate in the assessment process.
- Designate a security and privacy official (CSO) and establish a HIPAA Implementation Team.
- Perform an organization-wide risk/readiness assessment to define your organization's current ability to comply with HIPAA mandates. Inventory applications, security systems, and policies/procedures. Identify areas of high risk and gaps in readiness.
- Develop a comprehensive HIPAA Compliance Plan containing what changes are needed, remediation recommendations and an estimate of resources required.
- Develop and execute project plans for individual technical solution designs and areas where business process and policy changes are required.
- Revise or create new "Chain of Trust" and Business Partners agreements and information notices.
- Perform ongoing review, monitoring and audits of processes and systems.