Axian
Software Consulting and Training

HIPAA AND THE ADMINISTRATIVE SIMPLIFICATION PROVISIONS

The law known as "HIPAA" stands for the Health Insurance Portability & Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Congress passed this landmark law to provide consumers with greater access to health care insurance, to protect the privacy of health care data, and to promote more standardization and efficiency in the health care industry. The law applies directly to three groups referred to as "covered entities."

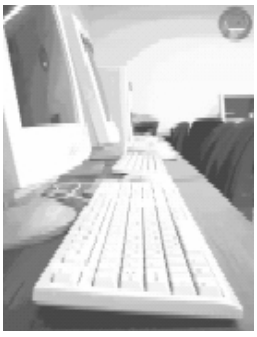
- **Health Care Providers:** Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which standard requirements have been adopted.
- **Health Plans:** Any individual or group plan that provides or pays the cost of health care.
- **Health Care Clearinghouses:** A public or private entity that transforms health care transactions from one format to another.

Section 262 of HIPAA, also known as the ***Administrative Simplification Provisions***, established standards and regulations for the **electronic exchange and maintenance of certain health information**.

HIPAA's "Administrative Simplification" provision is composed of four parts, each of which has generated a variety of "rules" promulgated by the Department of Health and Human Services (DHHS). The four parts of Administrative Simplification are:

1. Standards for Electronic Transactions
2. Unique Identifiers Standards
3. Security Rule
4. Privacy Rule

1. STANDARDS FOR ELECTRONIC TRANSACTIONS AND CODE SETS



"Electronic Health Transactions" include health claims, health plan eligibility, referrals and authorizations, enrollment and disenrollment, payments for care and health plan premiums, claim status, coordination of benefits, and related transactions.

In the past, health providers and plans have used many different electronic formats to transact medical claims and related business. HIPAA requires every covered entity that does business electronically to use the same health care transactions, code sets, and identifiers. HIPAA has identified ten National Standards for Electronic Data Interchange (EDI) for the transmission of health care data. Claims and encounter information, payment and remittance advice, and claims status and inquiry are several of the Electronic Transactions Standards.

Virtually all health plans must adopt these standards. Providers using non-electronic transactions are not required to adopt the standards for use with commercial healthcare payers. However, electronic transactions are required by Medicare, and all Medicare providers must adopt the standards for these transactions. If they don't, they will have to contract with a clearinghouse to provide translation services.

Health organizations also must adopt standard code sets to be used in all health transactions. For example, coding systems that describe diseases, injuries, and other health problems, as well as their causes, symptoms and actions taken must become uniform. All parties to any transaction will have to use and accept the same coding, for the purpose of reducing errors and duplication of effort. Fortunately, the code sets proposed as HIPAA standards are already used by many health plans, clearinghouses and providers, which should ease transition to them. The codes mandated by HIPAA are given below:

International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 1 and 2	**Diseases, Injuries, Impairments, Causes of injury, diseases, impairment, or other health-related problems.**
International Classification of Diseases, 9th Edition, Clinical Modification, (ICD-9-CM), Volumes 3	**Procedures or other actions taken for diseases, injuries, and impairments on hospital inpatients, encompassing Prevention, Diagnosis and Treatment.**
National Drug Codes (NDC)	**Drugs and Biologics**
Code on Dental Procedure and Nomenclature	**Dental services**
Healthcare Financing Administration Common Procedure Coding System (HCPCS) and Current Procedural Terminology, Fourth Edition (CPT-4)	**Combination of Physician Services, Physical and Occupational therapy, Radiological and Clinical laboratory procedures, Hearing and Vision services, and Transportation services including ambulances.**

All covered entities must be in compliance with the electronic transaction and code set standards by Oct.16, 2003. However, HHS' Centers for Medicare & Medicaid Services (CMS) -- the agency charged with overseeing the implementation of these standards -- issued guidance in July 2003 regarding the enforcement of the HIPAA transactions and code set standards after Oct.16, 2003. The guidance clarified that covered entities, which make a good faith effort to comply with the standards, may implement contingency plans to maintain operations and cash flow. Specifically, as long as a covered entity demonstrates a good-faith effort to come into compliance through active outreach and testing efforts, it can continue processing payments and claims using non-standard transactions.

CMS will focus on obtaining voluntary compliance and use a complaint-driven approach for the enforcement of the electronic transactions and code sets provisions. Detailed information about the transactions and code sets rule is available at http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/default.asp.

.

2. UNIQUE IDENTIFIERS FOR PROVIDERS, EMPLOYERS, AND HEALTH PLANS

In the past, healthcare organizations have used multiple identification formats when conducting business with each other -- a confusing, error-prone and costly approach. It is expected that standard identifiers will reduce these problems. The **Employer Identifer Standard**, published in 2002, adopts an employer's tax ID number or Employer Identification Number (EIN) as the standard for electronic transactions. Final standards for Provider and Health Plan identifiers have not yet been published.

3. SECURITY RULE

The final Security Rule was published on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual. The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce. Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices.

The Security Standard is intended to be scalable; in other words, it does not require specific technologies to be used. Covered entities may elect solutions that are appropriate to their operations, as long as the selected solutions are supported by a thorough security assessment and risk analysis. (For a complete summary analysis of the Final Security Rule, see the next section of this report.)

4. PRIVACY RULE

The Privacy Rule is intended to protect the privacy of all individually identifiable health information in the hands of covered entities, regardless of whether the information is or has been in electronic form. The rule establishes the first "set of basic national privacy standards and fair information practices that provides all Americans with a basic level of protection and peace of mind that is essential to their full participation in their care." The Privacy standards:

- Give patients new rights to access their medical records, restrict access by others, request changes, and to learn how they have been accessed
- Restrict most disclosures of protected health information to the minimum needed for healthcare treatment and business operations
- Provide that all patients are formally notified of covered entities' privacy practices,
- Enable patients to decide if they will authorize disclosure of their protected health information (PHI) for uses other than treatment or healthcare business operations
- Establish new criminal and civil sanctions for improper use or disclosure of PHI
- Establish new requirements for access to records by researchers and others
- Establish business associate agreements with business partners that safeguard their use and disclosure of PHI.
- Implement a comprehensive compliance program, including
    - Conducting an impact assessment to determine gaps between existing information practices and policies and HIPAA requirements
    - Reviewing functions and activities of the organization's business partners to determine where Business Associate Agreements are required
    - Developing and implementing enterprise-wise privacy policies and procedures to implement the Rule
    - Assigning a Privacy officer who will administer the organizational privacy program and enforce compliance

- Training all members of the workforce on HIPAA and organizational privacy policies
- Updating systems to ensure they provide adequate protection of patient data

HIPAA Deadlines

April 14, 2003
Privacy

Deadline for compliance with privacy requirements (except small health plans who must comply by 4/14/04)

April 16, 2003
Software

Start testing software no later than April 16, 2003.

October 16, 2003
Electronic Transactions & Code Sets Requirements

Deadline for compliance

(Note: CMS announced on Sept. 23, 2003 that it will implement a contingency plan to accept noncompliant transactions after the Oct. 16th deadline.)

July 30, 2004
Standard Unique Identifier for Employers

Deadline for compliance for most covered entities (except small health plans who have until 8/1/05)

April 21, 2005
Security

Deadline for compliance (except small health plans who have until 4/21/06)

Most covered entities were required to comply with the privacy rule by April 14, 2003; small health plans (annual revenue receipts of under $5 million) have until April 14, 2004 to come into compliance, as required under the law. Detailed information about the privacy rule is available at http://www.cms.gov/hipaa/hipaa2/enforcement.

The Final HIPAA Security Rule – Major Themes and Highlights

The final rule adopts standards as required under title II subtitle F, sections 261 through 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191.

- **Effective Date:** These regulations are effective on April 21, 2003.
- **Compliance Date:** Covered entities, with the exception of small health plans, must comply with the requirements of this final rule by April 21, 2005. Small health plans (i.e., annual receipts of $5 million or less) must comply with the requirements of this final rule by April 21, 2006.

On February 20, 2003, the Department of Health and Human Services (HHS) issued final security standards to complement the health privacy standards that protect individually identifiable health information from unauthorized disclosure. Because many of the security standards work in concert with the already finalized HIPAA Privacy Rule that took effect on April 14, 2003, health care providers, payers and clearinghouses have anxiously awaited the final version of the Rules. The following are key highlights of the final rule.

Covers Only Electronic Protected Health Information

The Final Security Rule requires covered entities to safeguard and protect individually identifiable health information (called "protected health information") maintained or transmitted in electronic form only. Additionally, as part of the Final Security Rule, HHS updated the definition of PHI to clarify that PHI includes information that is transmitted by electronic media, maintained in electronic media or maintained in any other form or medium. The term "electronic media" is defined as:

1. electronic storage media including computer hard drives and any removable/transportable digital memory medium such as magnetic tape or disk, or digital memory card;

2. transmission media used to exchange information already in electronic storage media, for example extranet, leased lines, dial-up lines, private networks; and

3. the physical movement of removable/transportable electronic storage media.

Further, the Final Security Rule clarifies that certain transmissions such as paper-to-paper faxes, person-to-person telephone calls, video teleconferencing and/or messages left on voice-mail are not "electronic media" and, accordingly are not subject to the safeguards required under the Final Security Rule.

By contrast, the final privacy standards issued by HHS protect medical records and other confidential health information that identifies (or could reasonably be used to identify) an individual and relates to past, present, or future physical or mental condition of the individual or the payment of health care for that individual. The privacy standards protect PHI in all forms (including electronic, written, or oral) created or received by a covered entity.

Privacy vs. Security Standards

A stated goal of the Final Security Rule was to create greater coordination between the security and privacy rules – a clear acknowledgement that that the concepts of security and privacy are inextricably linked.

The privacy standards essentially say that a covered entity cannot use or disclose Protected Health Information (PHI) except as authorized by the individual or by HHS regulations. The security standards go a step further to say a health plan must adopt safeguards to prevent unauthorized electronic access (e.g., by hackers breaking into a health plan's claims records) or unauthorized destruction of the information.

Flexibility in Implementation

The Final Security Rule does not provide specific instruction on how covered entities should safeguard PHI in oral, written or non-electronic form. However, it does provide a process of evaluation that covered entities could use to determine what would constitute "appropriate safeguards" under the Privacy Rule.

Specifically, covered entities are permitted to "use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications" of the security rule.

To provide flexibility, the implementation specifications are divided into two categories:

- ***Required*** specifications that must be implemented as described in the regulations. (As shown in Appendix A, *Security Standards Matrix*, 20 of the implementation specifications are required.)

- ***Addressable*** specifications that need not be implemented as described in the regulations but may be addressed in some other manner. (As shown in Appendix A, *Security Standards Matrix*, 22 of the implementation specifications are addressable.)

  Addressable means a covered entity must:

  - Assess whether the specification is reasonable and appropriate based on an analysis of the risks involved.
  - If the specification is assessed as unreasonable or inappropriate, document the rationale for the assessment.
  - Implement an alternative safeguard, or none at all, if that is reasonable and appropriate for the covered entity.

It is important to note that **compliance with all the standards in the final rule are required irrespective of whether required, addressable, or no implementation specifications exist for the standard.**

Scalable

The regulations require that a covered entity "reasonably and appropriately implement" the specifications taking into account the size, complexity, and capability of the covered entity, its technical infrastructure, cost, and probability/criticality of risk. For example, a solution deemed appropriate for a small health plan may not be adequate for a large health plan nor would a large plan's solution be cost-effective for a small plan.

Technology-Neutral

With the rapid rate of change in available technologies, any regulation requiring the use of a particular technology would become rapidly obsolete. To avoid the obsolescence problem, the regulation does not require specific implementation measures or technologies. The choice of appropriate technology is left to the covered entity. However, the **covered entity must periodically review and evaluate its technology**.

Security Risk Assessment

The Final Security Rule requires all covered entities to **"conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."** All covered entities must then implement security measures to reduce the risks and vulnerabilities identified to a "reasonable and appropriate level."

This is similar to a gap analysis that many covered entities have conducted with regard to implementing the Privacy Rule; however, this assessment will identify potential security risks and vulnerabilities in electronic information systems rather than a gap in compliance.

Security Policies and Procedures and Training

Similar to the privacy rule, the security rule requires that covered entities implement reasonable and appropriate security policies and procedures. In addition, a covered entity is required to "implement a security awareness and training program for all members of its workforce (including management)." Although these requirements mirror the privacy rule, covered entities will be required to develop and implement additional policies and procedures and train all workforce on such policies and procedures.

Business Associate Agreements

The Final Security Rule mandates that covered entities must pass on information security requirements to their "business associates." The term "business associate" is defined the same for the Privacy Rule as for the Final Security Rule. It is a person or organization to whom a covered entity provides Protected Health Information so that the person or organization can provide a service to the covered entity (e.g., transcription service, disease management services). Pursuant to the April 2005 compliance date for the Final Security Rule, covered entities will need to make sure that their business associate agreements contain all of the required elements for protecting electronic PHI.

Ongoing Compliance Process

The Final Security Rule provides that the security measures implemented to comply with the requirements of the Rule "must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information." Thus, compliance with the security rule is an ongoing process of reevaluation and assessment to ensure that the covered entity's security measures are still reasonable and appropriate in light of new security threats and technological capabilities.

Who Is Affected by the Security Standards?

The final security standards apply to health plans, health care clearinghouses, and to health care providers that maintain or transmit health information electronically.

- **Health Plans** that provide or pay the cost of medical care (e.g., HMO, insurance company, employer-sponsored plan, Medicare and Medicaid program, Medicare supplemental plan). A health plan that conducts transactions through an agent is responsible for ensuring that the agent satisfies all applicable regulations.
- **Health Care Providers** that transmit any health information in electronic form in connection with a transaction covered by the security rule.
- **Health Care Clearinghouses** that process or facilitate the processing of health information for health plans, employers and providers. (Note: The HIPAA definition of clearinghouses includes some billing services and "repricing companies." A repricing company aggregates smaller health care providers into a larger group for the purpose of providing services to a health plan. Billing services have a more complex definition. If billing is provided by a financial institution as a pure financial transaction, such as processing a credit or debit card payment, HIPAA excludes the transaction. If, in the course of billing for services, an organization processes any information that is specifically covered under HIPAA standards, then all of the billing for those services is subject to HIPAA standards, as HIPAA considers these organizations health care clearinghouses.)

What Are the Primary Compliance Obligations of a Covered Entity?

The final rule specifies that covered entities must meet **four general security requirements**. They are to:

1. Ensure the confidentiality, integrity and availability of all electronic PHI the covered entity creates, receives, maintains or transmits.

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Final Security Rule.

4. Ensure compliance by the workforce. (Note: The security rule also extends to the covered entity's at-home workers.)