HIPAA Primer

Updated July 2005

- **Learn more about HIPAA with our audio conferences, books, and other compliance tools.**
- **How Did We Get HIPAA?** Health Data Management magazine's March 2003 10th anniversary issue includes a history of HIPAA, explaining how the mandates now before the industry came to be.

WHAT IS HIPAA?

"HIPAA" is an acronym for the Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring:

1. Improved efficiency in healthcare delivery by standardizing electronic data interchange, and
2. Protection of confidentiality and security of health data through setting and enforcing standards.

More specifically, HIPAA called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure:

1. Standardization of electronic patient health, administrative and financial data
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," past, present or future.

- The bottom line: sweeping changes in most healthcare transaction and administrative information systems.

Who is affected?

Virtually all healthcare organizations – including all healthcare providers, health plans, public health authorities, healthcare clearinghouses, and self-ensured employers – as well as life insurers, information systems vendors, various service organizations, and universities.

Are there penalties?

HIPAA calls for severe civil and criminal penalties for non-compliance, including:

– fines up to $25K for multiple violations of the same standard in a calendar year

– fines up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information

Compliance deadlines?

Most entities have 24 months from the effective date of the final rules to achieve compliance. Normally, the effective date is 60 days after a rule is published. The Transactions Rule was published on August 17, 2000; the compliance date for that rule was October 16, 2003. The Privacy Rule was published on December 28, 2000, but due to a minor glitch didn't become effective until April 14, 2001. Compliance with the Privacy Rule was required as of April 14, 2003. The final Security Rule was published April 21, 2003, with compliance required as of April 21, 2005. The final Standard Unique Employer Identifier was published on May 31, 2002. Compliance was required by July 30, 2004. The final rule establishing the National Provider Identifier (NPI) rule was published January 23, 2004. The compliance date is May 23, 2007 for most covered entities. Healthcare providers may begin applying for NPIs beginning May 23, 2005. A final standard for a Health Plan Identifier has not yet been published.

- For more information, see our Compliance Calendar on the Status of HIPAA Regulations.

How are healthcare organizations affected?

Broadly and deeply. Required compliance responses aren't standard, because organizations aren't. For example, an organization with a computer network will be required to implement one or more security authentication access mechanisms – "user-based," "role-based," and/or "context-based" access – depending on its network environment.

Effective compliance requires organization-wide implementation.

Compliance requirements include:

- Building initial organizational awareness of HIPAA
- Comprehensive assessment of the organization's privacy practices, information security systems and procedures, and use of electronic transactions
- Developing an action plan for compliance with each rule
- Developing a technical and management infrastructure to implement the plans
- Implementing a comprehensive implementation action plan, including
    - Developing new policies, processes, and procedures to ensure privacy, security and patients' rights
    - Building business associate agreements with business partners to support HIPAA objectives
    - Developing a secure technical and physical information infrastructure
    - Updating information systems to safeguard protected health information (PHI) and enable use of standard claims and related transactions
    - Training of all workforce members
    - Developing and maintaining an internal privacy and security management and enforcement infrastructure, including providing a Privacy Officer and a Security Officer

The Rules Under HIPAA

HIPAA's **"Administrative Simplification"** provision is composed of four parts, each of which have generated a variety of "rules" promulgated by the Department of Health and Human Services. 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

The term **"Electronic Health Transactions"** includes health claims, health plan eligibility, enrollment and disenrollment, payments for care and health plan premiums, claim status, first injury reports, 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. Implementing a national standard is intended to result in the use of one format, thereby "simplifying" and improving transactions efficiency nationwide.

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.

- More about the Transactions Standards.

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. The NPI, published in 2004, requires hospitals, doctors, nursing homes, and other healthcare providers to obtain a unique identifier when filing electronic claims with public and private insurance programs. Providers can apply for an identifier once and keep it if they relocate or change specialties. A final standard for a Health Plan identifier has not yet been published.

- More about the Employer ID.
- More about the National Provider ID.

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.

- More about the Security Rule.

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”. 65 Fed. Reg. at 82464The 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 parteners 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

- More about the Privacy Rule.

Go to TOP