HIPAA primer

WHAT IS HIPAA?

The Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.

Title II includes a section, 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 calls for:

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? All healthcare organizations. This includes all health care providers, even 1-physician offices, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

ARE THERE PENALTIES? HIPAA calls for severe civil and criminal penalties for noncompliance, 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. So the compliance date for that rule is October 16, 2002. The Privacy Rule was published on December 28, 2000, but due to minor glitch didn't become effective until April 14, 2001. Compliance is required for the Privacy Rule on April 14, 2003.

For more information, see the Tentative Schedule for Publication of the regulations.

HOW WILL WE BE 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. Steps include:

- Building initial organizational awareness of HIPAA

- Comprehensive assessing of the organization's information security systems, policies and procedures
- Developing an action plan with deadlines and timetables
- Developing a technical and management infrastructure to implement the plan
- Implementing a comprehensive action plan, including
    - Developing new policies, processes, and procedures
    - Building "chain of trust" agreements with service organization
    - Redesigning a compliant technical information infrastructure
    - Purchasing new, or adapting, information systems
    - Developing new internal communications
    - Training and enforcement

Now, we'll explore the next level of HIPAA - specifics that, for many of us, cause more confusion than clarity. Let's try to make "Administrative Simplification" simple!

HIPAA's "Administrative Simplification" provision is composed of four parts, each of which have generated a variety of "rules" and "standards." Many of the rules and standards are still in the "proposed" (by HHS) stage; however, most were expected to become "final" rules within the year 2000. Even more confusing, the rules, when final, will often have different compliance deadlines.

The four parts of Administrative Simplification are:

I. ELECTRONIC HEALTH TRANSACTIONS STANDARDS
II. UNIQUE IDENTIFIERS
III. SECURITY & ELECTRONIC SIGNATURE STANDARDS
IV. PRIVACY & CONFIDENTIALITY STANDARDS

I. ELECTRONIC HEALTH TRANSACTIONS STANDARDS

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.

Today, health providers and plans use many different electronic formats. Implementing a national standard will mean we will all use one format, thereby "simplifying" and improving transaction efficiency nationwide. The proposed rule requires use of specific electronic formats developed by ANSI, the American National Standards Institute, for most transactions except claims attachments and first reports of injury. Proposed regulations for these exceptions are not yet out.

Virtually all health plans will have to adopt these standards, even if a transaction is on paper or by phone or fax. Providers using non-electronic transactions are not required to adopt the standards; although 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. Again, in the long run, this is intended to reduce mistakes, duplication of effort and costs. Fortunately, the code sets proposed as HIPAA standards are already used by many health plans, clearinghouses and providers, which should ease the transition.

More about Transactions.
Read the Final Transactions Rule.

II. UNIQUE IDENTIFIERS FOR PROVIDERS, EMPLOYERS, HEALTH PLANS and PATIENTS

The current system allows us to have multiple ID numbers when dealing with each other, which HIPAA sees as confusing, conducive to error and costly. It is expected that standard identifiers will reduce these problems.

III. SECURITY OF HEALTH INFORMATION & ELECTRONIC SIGNATURE STANDARDS

The new Security Standard will provide a uniform level of protection of all health information that is

1. housed or transmitted electronically and that
2. pertains to an individual.

In addition, organizations who use Electronic Signatures will have to meet a standard ensuring message integrity, user authentication, and non-repudiation.

The Security standard mandates safeguards for physical storage and maintenance, transmission, and access to individual health information. It applies not only to the transactions adopted under HIPAA, but to all individual health information that is maintained or transmitted. However, the Electronic Signature standard applies only to the transactions adopted under HIPAA.

The Security Standard does not require specific technologies to be used; solutions will vary from business to business, depending on the needs and technologies in place. Also, no transactions adopted under HIPAA currently require an electronic signature.

IV. PRIVACY AND CONFIDENTIALITY

The Final Rule for Privacy was published just as President Clinton was leaving office, on December 28, 2001. A paperwork glitch delayed notification of Congress, so the Congressional Review period didn't begin until February, pushing the effective date of the rule until April 14, 2001. HHS Secretary Tommy Thompson used the time to solicit additional comments during March. HHS received over 11,000 comments and plans to issue guidelines and clarification of the final rule in response. Compliance will be required on April 14, 2003 for most covered entities.

In general, privacy is about who has the right to access personally identifiable health information. The rule covers all individually identifiable health information in the hands of covered entities, regardless of whether the information is or has been in electronic form.

The Privacy standards:

- limit the non-consensual use and release of private health information;
- give patients new rights to access their medical records and to know who else has accessed them;
- restrict most disclosure of health information to the minimum needed for the intended purpose;
- establish new criminal and civil sanctions for improper use or disclosure;
- establish new requirements for access to records by researchers and others.

The new regulation reflects the five basic principles outlined at that time:

- **Consumer Control:** The regulation provides consumers with critical new rights to control the release of their medical information
- **Boundaries:** With few exceptions, an individual's health care information should be used for health purposes only, including treatment and payment.
- **Accountability:** Under HIPAA, for the first time, there will be specific federal penalties if a patient's right to privacy is violated.
- **Public Responsibility:** The new standards reflect the need to balance privacy protections with the public responsibility to support such national priorities as protecting public health, conducting medical research, improving the quality of care, and fighting health care fraud and abuse.
- **Security:** It is the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.