



HIPAA Primer

HIPAA BACKGROUND:

The Health Insurance Portability and Accountability Act (HIPAA) requires the Secretary of Health and Human Services (HHS) to promulgate standards to comply with the administrative simplification provisions of the law to improve Medicare and Medicaid programs, and the efficiency and effectiveness of the health care system.

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.

WHO IS AFFECTED?

All healthcare organizations, which include health care providers, physician offices, health plans, employers, public health authorities, insurance companies, clearinghouses, billing agencies, information systems vendors, service organizations, and universities.

ARE THERE PENALTIES?

Fines:

- a.) Up to \$25K for multiple violations of the same standard in a calendar year
- b.) 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.

The Transactions Rule was published on August 17, 2000. The compliance date for that rule is October 16, 2002.

The Privacy Rule was published on December 28, 2000, but the effective date is April 14, 2001. Required compliance for the Privacy Rule is on April 14, 2003.



More specifically, HIPAA calls for:

- **Compliance** with HIPAA privacy Standards for gathering, handling and storing personal health information
- **Train** (and monitor) employees on these privacy standards
- **Audit** compliance with HIPAA privacy practices on a regular basis
- **Secure** all computer equipment and network on which personal health information is stored or transmitted

Effective compliance will require the following recommended steps:

- a.) Organizational awareness training of HIPAA regulatory requirements
- b.) Assessment of your organization's information security systems, and your policies and procedures
- c.) Develop a HIPAA compliance action plan with deadlines and timetables
- d.) Implement the aforementioned action plan
- e.) Build a HIPAA Chain of Command for effective information flow and problem resolution
- f.) Purchasing new, or adapting current information systems to meet security standards
- g.) Training and enforcement of the action plan and policies

I. ELECTRONIC HEALTH TRANSACTIONS STANDARDS

Electronic Health Transactions includes those companies who deal with;

- Health claims
- Health plan eligibility
- Health plan enrollment and un-enrollment
- Payments for care and health plan premiums
- Health claim status
- Injury reports
- Coordination of benefits
- Related transactions

This 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.

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;

Housed or transmitted electronically as it pertains to an individual(s).

Electronic Signatures will have to:

- Ensure message integrity
- Verify user authentication(note: is verify the right word here? Something needs to be put before user)
- Have Non-repudiation. (same note as above)

Electronic Signature standard applies only to the transactions adopted under HIPAA.

IV. PRIVACY AND CONFIDENTIALITY

Compliance will be required on **April 14, 2003** for most covered entities.

The HIPAA Privacy standards will:

- 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:

- 1.) **Consumer Control:** This regulation provides consumers with the right to control the release of their medical information
- 2.) **Boundaries:** With few exceptions, individual health care information should be used for health purposes only.
- 3.) **Accountability:** Under HIPAA, for the first time, there will be specific federal penalties if a patient's right to privacy is violated.
- 4.) **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.
- 5.) **Security:** Will be the responsibility of organizations that are entrusted with health information to protect it against deliberate or inadvertent misuse or disclosure.