

HIPAA-Compliant Data Systems



Laws for the secure and private transfer of individual's medical information.

The nearly instantaneous flow of information is a defining variable of the information age. Many leading companies have established a benchmark of implementing flexible and effective new technologies into their business plan, and just now many small businesses have been able to get out ahead of this trend and implement their own solutions. While it's true some companies can use this technology better than others, in regards to healthcare information, the seamless flow of information can literally be the difference between life and death.

In August of 1996, United States President Bill Clinton, in an effort to promote secure transfer of patient information, signed into law the Health Insurance Portability and Accountability Act (HIPAA). At that time, HIPAA stated that the Secretary of Health and Human Services had to publicize official standards for the electronic exchange, privacy, and security of health-related information. It also stated that the Secretary of HHS had the responsibility of issuing regulations if the U.S. Congress didn't enact privacy and security standards by 1999. Three years later, HHS unveiled the official rules.

Table of Contents

1. [HIPAA Privacy Rule](#)

2. [HIPAA Security Rule](#)
3. [Electronic Transaction & Code Sets Standards](#)
4. [National Identifier Requirements](#)
5. [Enforcement & Penalties](#)

HIPAA Privacy Rule

The HIPAA Privacy Rule, or the *Standards for Privacy of Individually Identifiable Health Information*, established protocols for many healthcare providers in regards to who has access to patient information. The privacy rule applies to health plans, health care agencies, and to any healthcare provider that transmits patient information electronically.

Individual and group medical plans that provide or pay the cost of medical care are covered by HIPAA. These plans include health, dental, vision, prescription drug insurers, health maintenance organizations (HMO), Medicare, Medicaid, and other healthcare insurance providers.

The following information is protected under HIPAA's Privacy rule:

- An individual's complete history of their physical and mental health conditions.
- The treatment or provision the individual has access to.
- An individual's payment information for said health care.

The Privacy Rule is administered by the Office for Civil Rights.

HIPAA Security Rule

The more seamless the transfer of data is, the better it works for business. Unfortunately, there are entities out there looking for opportunities to intercept this information for their own, often nefarious, purposes. No where is data more personal, than in the health care industry.

HIPAA's Security Rule, or *Security Standards for the Protection of Electronic Protected Health Information*, specifies a series of administered, physical, and technical safeguards for covered parties to guarantee the integrity, real-time availability, and confidentiality of protected electronic healthcare information.

The Security Rule is administered by the Centers for Medicare and Medicaid Services (CMS).

Electronic Transaction & Code Sets Standards

The standardization of electronic transactions is important for the efficiency of the care being provided to patients. With the standardization rules set forth by HIPAA, each health care provider has to adhere to the same set of protocols as other providers do to ensure the transferred financial and medical information is easily deciphered by the health care provider. HIPAA sets a standard and the operating rules for electronic funds transfer (EFT) and electronic remittance advice (ERA) and attachments for claims.

This section of HIPAA is administered by the Centers for Medicare and Medicaid Services.

National Identifier Requirements

As a part of the HIPAA law, health care providers are mandated to use unique Health Plan Identifiers (HPID). These are identifying numbers assigned to specific medical transactions. For example, the numeric code for an allergy test is the same from one provider to another. This level of standardization allows providers to avoid the pitfalls that come with deciphering what care is to be provided as well as the act of billing the services that have been received.

Like the transaction code standardization, the identifiers are administered by the Centers for Medicare and Medicaid Services.

Enforcement & Penalties

Every law needs a ruling entity. HIPAA is no different. In order rules of the HIPAA law to work, the Enforcement Rule is in place for dedicated checks and balances. Currently the Centers for Medicare and Medicaid Services enforces the HIPAA Security Rule and the Rules covering the standardization of information, while the Privacy concern is handled by The Office of Civil Rights.

To date, the implementation of Health Insurance Portability and Accountability Act standards have substantially increased the use of electronic data interchange within the medical industry. Provisions in play under the Affordable Care Act of 2010 will increase these electronic interchanges and include further requirements to take into account the basics of the initial act.

Additionally, as a part of the Affordable Care Act of 2010, health plans will be required to certify their compliance. The Act provides for crippling penalties for failures to certify or comply with the new standards and operating rules. These penalties include:

Penalties for General Violations of HIPAA:

- Each violation: A \$100 penalty per violation, with no more than \$25,000 in one year for all violations of identical requirements.

Penalties for the Wrongful Disclosure of Individually Identifiable Health Information:

- For wrongful disclosure: \$50,000 penalty, imprisonment for not more than one year, or both.
- For wrongful disclosure made under false pretenses: \$100,000 penalty, imprisonment for not more than five years, or both.
- For wrongful disclosure made with the intent to sell information: \$250,000 penalty, imprisonment of not more than 10 years, or both.

As well as the penalties listed above, covered entities that fail to comply with HIPAA regulations will likely be subject to a loss of credibility, which will likely result in the loss of public trust and revenue.

For more information about HIPAA or our role in your data security, call us today at 703-270-1007. We can clarify about the specifics for HIPAA compliance and present secure data transfers for your medical practice.