

HIPAA

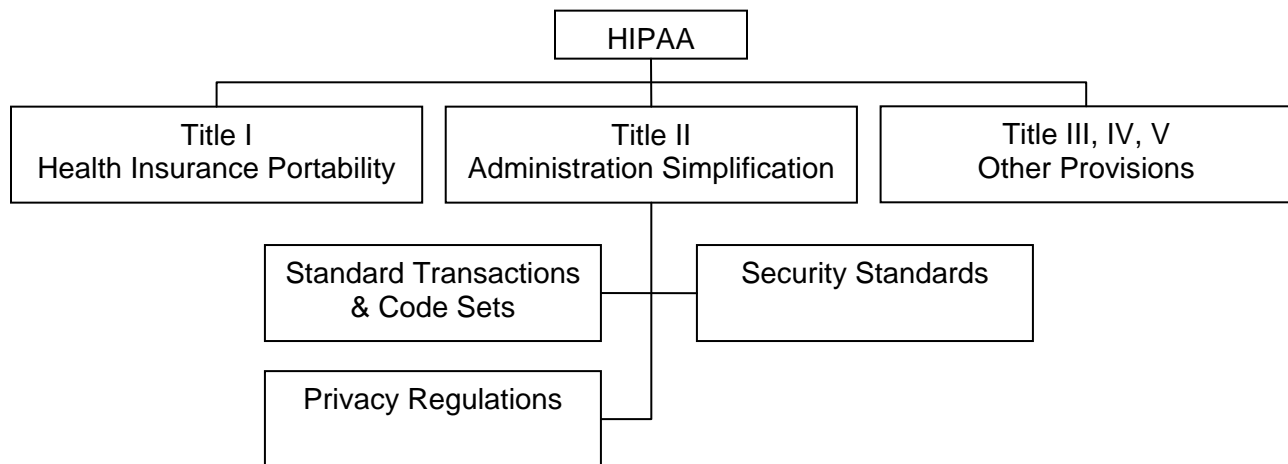
I. Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) A. Background: Administrative Simplification

Despite the many current state and federal requirements that health information be held in confidence, few laws, regulations, or professional standards have existed to govern the details of how confidentiality and security of health information should be maintained. Federal regulations have now been issued under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) that provide such details.

HIPAA was enacted on August 21, 1996 as part of a broad-ranging congressional attempt at incremental health care reform. Among the main purposes of HIPAA were

- to promote the portability and continuity of health insurance coverage
- to combat waste, fraud and abuse; and
- administration simplification of health insurance

The purpose of “administration simplification” is to improve the Medicare and Medicaid programs, and the efficiency and effectiveness of the health care system generally. HIPAA requires the United States Department of Health & Human Services (“DHHS”) to develop and implement standards for the electronic transmission of certain health information. HIPAA further requires federal legislation or regulations to protect the privacy and security of individually identifiable health information.



The Administrative Simplification regulations fall in to three categories:

1. Transactions: Standards for the content and format of certain electronic transactions.
2. Privacy: Regulations safeguarding the privacy of an individual's healthcare information, and establishing certain individual rights with respect to that information.
3. Security: Standards for assuring the confidentiality, integrity and accessibility of electronic health information.

B. Penalties

Civil Penalties: Noncompliance with the Administrative Simplification regulations may result in maximum penalties of \$100 per violation and a maximum of \$25,000 per person for all identical violations in a calendar year.

Criminal Penalties: HIPAA also establishes a fine of up to \$50,000 and/or imprisonment for up to one year for any person who knowingly obtains or discloses individually identifiable health information. For such offenses committed under false pretenses, the penalty is a fine of up to \$100,000 and/or imprisonment for up to five years. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm the penalty is a fine of up to \$250,000 and/or imprisonment for a maximum of ten years.

II. Electronic Transactions, Identifiers and Code Sets Regulations

The core of HIPAA Administrative Simplification is the standardization of common electronic transactions, and related identifiers and code sets. A "transaction," according to HIPAA, is the "exchange of information between two parties to carry out financial and administrative activities related to health care." At present, hundreds of formats are used for these transactions, usually custom designed by each payor. By October 16, 2002 (or October 16, 2003 for a small health plan, or if an extension is requested), Health Plans and Clearinghouses must be prepared to accept certain electronic transactions in new standardized formats. Health care providers may continue to conduct such transactions on paper, but if the transactions are conducted electronically, the standards must be followed beginning October 16, 2002 (or October 16, 2003 if an extension is requested).

In August 2000, final regulations for the content and format of eight transactions (the first "Standard Transactions") were published; 65 Federal Register 50311. (In proposed regulations issued in May 2002, changes in the standard code set for drugs and certain technical changes were proposed.) The Standard Transactions are

1. Health claims and equivalent encounter information
2. Health Plan enrollments and disenrollments
3. Health Plan eligibility

4. Health care payment and remittance advice
5. Health Plan premium payments
6. Health claim status
7. Referral certification and authorization
8. Coordination of benefits

Standards for additional transactions are expected to be issued at a later date.

HIPAA also requires the development of unique identifiers for individuals, employers, health plans, and health care providers. Congress has put the individual identifier on hold; the other identifiers are in various stages of development at this time. The regulations also establish code sets, which are standard codes to be used in the Standard Transactions to convey key information. Generally, these code sets are those already adopted by the health care system, such as ICD9-CM diagnosis codes and HCPCS service codes.

The Transaction Standards, including the identifiers and code sets, may not be modified by the Covered Entity engaged in the transaction. Covered Entities may exchange data electronically only in the standard formats and with the standard content; no “local codes” or customized variations are permitted.

III. Privacy Regulations

A. General Information

The HIPAA privacy regulations provide the first comprehensive federal protection for the privacy of health care information.

1. The Main Principle

Covered Entities may not use or disclose protected health information without permission of the individual, except as permitted by the regulation. Covered Entities must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the regulations. “Reasonable safeguards” does not mean protection from any and all potential risks; the determination is based on the particular facts and circumstances, including the financial and administrative burdens of any safeguard. (For example, a hospital is not required to remodel its facility to eliminate semi-private rooms.)

2. What is Protected Health Information (PHI)?

Protected health information (“PHI”) is individually identifiable information related to an individual’s health or physical/mental condition, health care, or payment for health care, regardless of its form – including electronic information, paper records, and oral communications.

De-identified information is not PHI. Information may be de-identified by removing certain specified data elements (the “safe harbor”) or by hiring an expert who can apply statistical analysis to certify that the data is de-identified.

3. Designation of Privacy Official and Contact Person

A Covered Entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the Covered Entity. In the addition, the Covered Entity must designate a contact person or office to be responsible for receiving complaints relating to the Privacy Regulations and to provide further information about matters covered by the Covered Entity’s Notice. These designations must be documented; 45 C.F.R. § 164.530(a). The contact person may, but need not be, the privacy official. Implementation is expected to vary widely, depending on the size and nature of the Covered Entity. Small entities may have a part-time privacy official, or may assign this as an additional duty to an existing staff person. In contrast, large organizations may have a full-time, dedicated privacy official; see 65 Fed. Reg. 82561.

4. Minimum Necessary

Reasonable steps must be taken to limit uses and disclosures to the minimum amount of PHI required to accomplish the intended purpose. The idea is to avoid using or disclosing the individual’s entire health record unless this is truly necessary, and to make Covered Entities evaluate their practices and enhance protections as appropriate. There are exceptions to the minimum necessary rule; for example, the requirement does not apply to *disclosures* for treatment. The minimum necessary rule does apply to *uses* for treatment within the organization.

A Covered Entity must develop policies and procedures for routine uses and disclosures which identify the amount of information that is required. For example, a hospital may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record. When Access to the entire medical record is necessary, the policy should state this explicitly and provide the justification.

For routine or recurring disclosure situations, the policies and procedures may be standard protocols. For non-routine uses and disclosures, the Covered Entity must develop reasonable criteria for making the determination as to what will be considered the minimum necessary information for the specific purpose. Non-routine disclosures must be reviewed on an individual basis in accordance with these criteria.

5. Business Associates

The privacy rules create a sphere of privacy protection that includes both Covered Entities and the “Business Associates” they engage. A Business Associate is a person or entity who provides certain functions on behalf of the Covered Entity which involve the use of disclosure of PHI; 45 C.F.R §164.504(e). An example of a Business Associate could be a third party administrator (TPA) providing plan administration services to an employer’s self-insured Health Plan, a Provider’s billing or practice management service, legal counsel, collection service, etc. Employees of the Covered Entity are never Business Associates. In addition, the Business Associate requirements do not apply to Covered Entities who disclose PHI to Providers for treatment purposes (e.g., a hospital disclosing PHI to a member of the medical staff).

IV. Security Regulations

A. Overview of Requirements

The proposed HIPAA security Regulations require reasonable and appropriate administrative, technical, and physical safeguards that insure the integrity and confidentiality of health care information, and protect against reasonably foreseeable threats to the security or integrity of the information; 64 Fed. Reg. 43249. The proposed regulations include technical guidance as well as administrative requirements for those who maintain or transmit electronic health information.

Like the HIPAA Privacy Regulations, the Security Regulations are intended to be scalable and flexible. No specific technologies are required. Covered Entities are expected to have different security needs, depending on their size and complexity. The Security Regulations require each Covered Entity to assess its potential risks and vulnerabilities and its own security needs. The scalability and flexibility of the regulations allow Covered Entities to adopt security plans that fit their organizations; yet, that scalability and flexibility also leaves Covered Entities at risk for making an erroneous judgment about their vulnerabilities, or making the wrong business decision in their investment in technology and development of their security management plan. There are no pre-determined “safe harbors” to illustrate the “right” level of security protections for a particular organization. Fortunately, the proposed regulations are consistent with common sense and good information systems practices that most organizations should be following anyway.

The standards are divided into four (somewhat overlapping) categories. The number of requirements in each category is noted in the parentheses.

<p style="text-align: center;">Administrative procedures (12 standards)</p> <p>To guard data integrity, confidentiality, and availability. These are documented, formal practices for selecting and executing information security measures to protect data, and staff responsibilities for the protection of data.</p>	<p style="text-align: center;">Physical safeguards (6 standards)</p> <p>To guard data integrity, confidentiality, and availability. These safeguards relate to the protection of the actual physical computer system, and related buildings and equipment, from fire and other environmental hazards. Also included are the use of locks, keys, and administrative measures to control access to computer systems and facilities.</p>
<p style="text-align: center;">Technical data security services (5 standards)</p> <p>To guard data integrity, confidentiality, and availability. These include the processes used to protect, control and monitor information access.</p>	<p style="text-align: center;">Technical security mechanisms (1 standard)</p> <p>To prevent unauthorized access to data transmitted over a communication network.</p>

Additional Information:

CRHC's Privacy Officer is Alan Palo CFO.

The CMS website (<http://www.cms.hhs.gov/>) has the regulations in their entirety, as well as FAQ's and a hotline number.