

GETTING STARTED WITH HIPAA

An Instructional Document Written by WorkSmart MD, Inc.

Extracted from the HIPAA Rx™ Compliance Software

In the early 1990s, the Bush Administration called health care industry leaders together to discuss how health care administrative costs could be reduced. This group concluded that this could best be accomplished by increasing the use of electronic data interchange (EDI), or electronic transactions, within the healthcare industry. This advisory group later organized as the Workgroup for Electronic Data Interchange (WEDI).

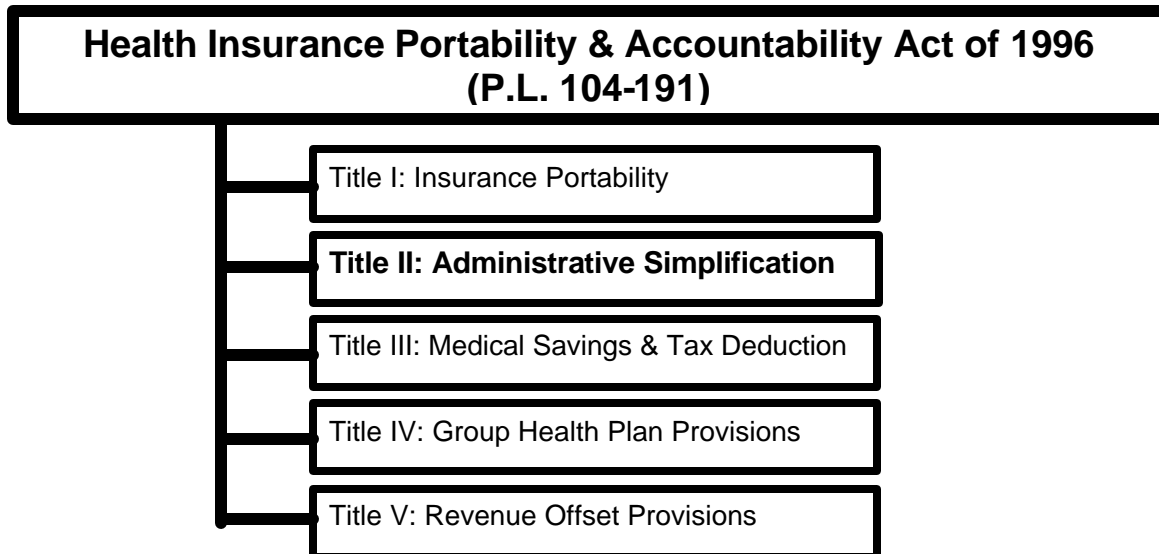
WEDI conducted a number of studies to determine how electronic transactions could improve the efficiency of America's healthcare system. Upon completing its analysis it identified more than four hundred (400) various formats being utilized for sending and receiving health information. WEDI estimated that providers would save \$9 billion annually, and the healthcare industry at large would save \$26 billion annually through the implementation of EDI for certain financial and administrative healthcare transactions.

WEDI recommended that Federal legislation be passed to ensure that a consistent set of standards could be used across the country.

WEDI's recommendations were incorporated in the Clinton Health Plan, which failed to pass. Its recommendations were again proposed and incorporated in The Health Insurance Portability and Accountability Act (HIPAA) which was signed into law on August 21, 1996.

HIPAA was written and signed into law with the objectives of

1. Improving portability of health insurance
2. Combating waste, fraud, and abuse in health insurance
3. Promoting the use of medical savings accounts
4. Simplifying the administration of health insurance.

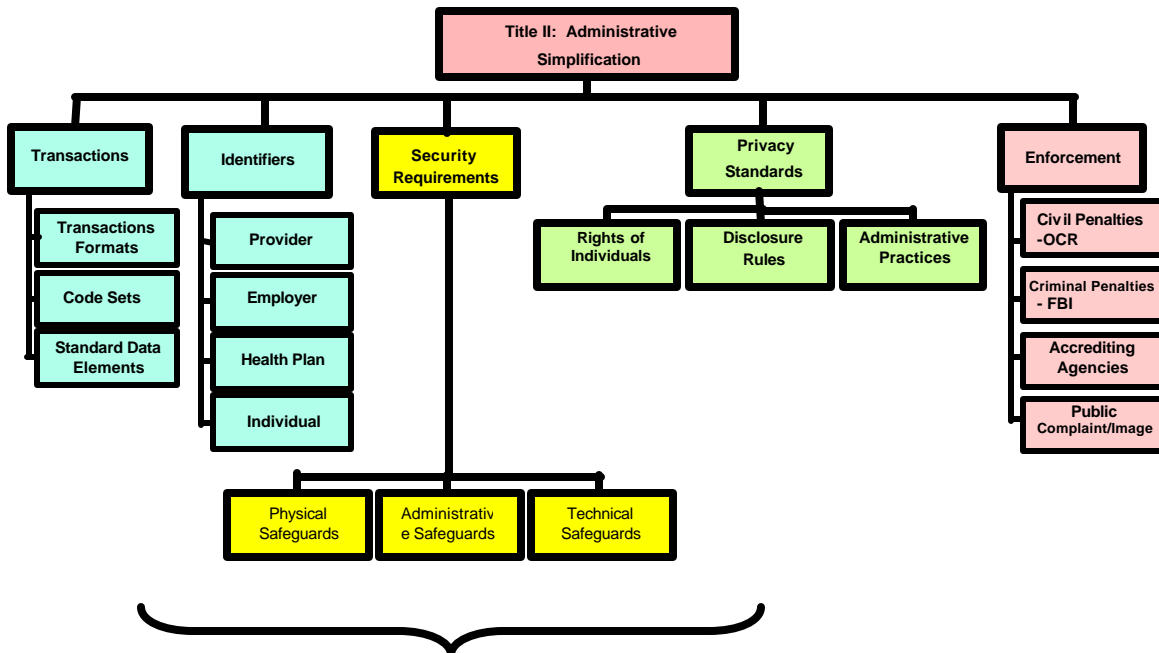


The portion of HIPAA that affects the majority of healthcare providers, insurance companies, hospitals, and clearinghouses is Section II, subtitle F, Administrative Simplification. Throughout the HIPAA compliance process when you see “**HIPAA**” it refers specifically to the Administrative Simplification section of the Health Insurance Portability and Accountability Act.

Most of the HIPAA mandates were supposed to become effective in February, 1998, with compliance required by February, 2000. This didn't happen. The government has had repeated delays in the completion of the draft rules, or Notices of Proposed Rulemaking (NPRMs). Once finalized and published in the Federal Register, the final regulations become effective 60 days after their publication and compliance is required within 24 months of the effective date.

The Administrative Simplification section requires that the US Department of Health and Human Services (DHHS) mandate the use of specific electronic formats for a number of business purposes, and specify what administrative and medical coding schemes can be used within those formats. It also mandates the development and implementation of national identifiers for patients, providers, payers, and employers, and the adoption of security and privacy standards appropriate for the protection of individually identifiable health care information.

Administrative Simplification



Administrative Simplification Summary

The General Accounting Office (GAO) estimated that at least twenty cents of every healthcare dollar is spent on administrative overhead. The objective of the Administrative Simplification portions of HIPAA is not just to ease the additional administrative burden resulting from the new HIPAA regulations, but also, and more importantly, to reduce costs through electronic data interchange (EDI) and to increase efficiency. The final outcome of the EDI standards should be a seamlessly integrated network of healthcare systems that operates comparably to the banking industry.

When the administrative simplification standards are in place, a healthcare provider will be able to submit a standard transaction for eligibility, an authorization, a referral, a claim, or an attachment containing the same standard data content to any health plan and that health plan must accept and process the transaction. This will simplify many clinical billing, and other financial applications.

As a result of the HIPAA transactional standards, both healthcare providers and insurance carriers will be able to interactively exchange standard transactions for eligibility verification, authorization, and referral information. The approximately 403 proprietary formats used in the past will be replaced by one (1) national standard for each identified transaction.

Administrative Simplification includes:

1. Standardization of electronic formats for transmission of nine specific transactions including claims, electronic remittance advice, eligibility, authorization, pharmacy, enrollment, coordination of benefits, attachments and first notice of claim
2. Unique Identifying Codes for Providers, Health Plans, Employers and Individuals
3. Security of electronic health information
4. Privacy of individually identifiable health information
5. Enforcement of the Administrative Simplification provisions

Electronic Transactions

Today, health providers use many different electronic formats. The HIPAA Transactional and Code Set Standards will result in one format, thereby "simplifying" and improving transaction efficiency nationwide. The transactional standards require the use of specific electronic formats developed by ANSI, the American National Standards Institute. The HIPAA Standards for Electronic Transactions include 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.

Standards for Electronic Transactions	
Health Care Claim (COB)	X12 837
Health Care Eligibility/Benefit Inquiry	X12 270
Health Care Eligibility/Benefit Information	X12 271
Health Care Services Review Information (Referral)	X12 278
Health Claim Status Inquiry	X12 276
Health Claim Status Response	X12 277
Benefit Enrollment and Maintenance	X12 834
Claim Payment and Remittance Advice	X12 835
Premium Payments	X12 820
First Report of Injury	(Not Available)
Health Claim Attachments	(Not Available)

Under the provisions of the HIPAA Transactional Standards, healthcare organizations 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. The objective being to reduce mistakes and costs.

Standards for Code Sets	
Institutional-Based Procedures	ICD-9 codes
Non-Institutional or Ambulatory Department Procedures	CPT-4 and HCFA Common Procedure Coding System (HCPCS) codes
Drug Payment Claims	National Council for Prescription Drug Programs (NCPDP) codes

Unique Identifiers

Healthcare claims are often delayed or rejected due to processing errors, including incorrect identifier codes for parties to transactions. The majority of healthcare providers find themselves with different identifier codes assigned by different health plans. The same identifier may be issued to multiple providers. Millions of employers are subject to similar inconsistencies, along with health plans and patients themselves. Employers,

providers, insurers, clearinghouses, patients and vendors are faced with extra work, processing delays, and high costs created by this lack of standardization. Under the administrative simplification provisions of HIPAA, unique identifiers will be established for healthcare providers, health plans, employers and patients thereby reducing errors and increasing the efficiency of electronic transactions.

Security

The security standards mandate safeguards for physical storage and maintenance, transmission, and access to individual health information. The final security rule was published on February 20, 2003 and provides a uniform level of protection of all health information, pertaining to an individual that is maintained or transmitted electronically. The security standard does mandate or require specific technology or equipment.

There are four main security provisions included in HIPAA. These are:

1. Administrative Procedures (security practices and procedures)
2. Physical Safeguards (protection from intrusion)
3. Technical Safeguards (security over data at rest)

Privacy

The HIPAA privacy standards were designed to protect health information that is individually identifiable to a patient and provide the patient with increased access and information about their health record. The standards protect individually identifiable health information in written, oral or electronic formats. These regulations were published on December 28, 2001 and became a law April 14, 2003.

The privacy rule outlines who has the right to access individually identifiable health information, establishes guidelines for when health information can be used and disclosed, provides patients new rights to access their health information and know who else has accessed the information, and establishes criminal and civil penalties for improper use or disclosure of health information.

The HIPAA privacy rule is composed of the following key requirements:

- Healthcare providers must obtain written authorization for use and disclosures of health information for purposes other than treatment, payment, or healthcare operations.
- Healthcare providers must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- Healthcare providers must implement policies and procedures, with respect to protected health information, that are designed to comply with the standards, implementation specifications, or other requirements of the HIPAA privacy rule.
- Healthcare providers must create a Notice of Privacy Practices to inform individuals of their legal rights and how their information is used and disclosed. Healthcare providers must obtain written acknowledgement that the individual has received a copy of the notice.

- Healthcare providers must train members of its workforce on the organization’s policies and procedures.
- Healthcare providers must retain all documentation developed in the process of complying with the HIPAA privacy rule. Documentation must be retained for six years.

Compliance Schedule and Penalties

Compliance Schedule			
Standard	Proposed Rule Published	Final Rule Publication	Compliance Deadline
Transactions and Code Sets	5/07/1998	8/17/2000	10/16/2003
Security	8/12/1998	2/20/2003	4/21/2005
Privacy	11/3/1999	12/28/00	4/14/2003

HIPAA is a Federal Mandate. Although its objective is to save the healthcare industry money, there will be costs associated with compliance. It is estimated by the General Accounting Office (GAO) that HIPAA will cost 17.6 billion dollars to implement over the next ten years, a figure which is more than offset by the 29.9 billion dollars in estimated savings.

Organizations that do not comply with the HIPAA Administrative Simplification Standards could face civil and criminal penalties. The penalties include monetary fines and possible imprisonment.

Under HIPAA, if health information is disclosed for purposes other than treatment, payment or operations, without a patient’s permission, the penalties are as follows:

- Up to \$50,000 and one year in prison for obtaining or disclosing protected information
- Up to \$100,000 and five years in prison for obtaining protected information under “false pretenses”
- Up to \$250,000 and ten years in prison for obtaining or disclosing protected information with intent to sell, for personal gain, or with malicious intent

There are extremely limited circumstances when health information can be disclosed without the patient’s permission. These instances include emergency circumstances, identification of a deceased person, determining cause of death, public health needs, judicial proceedings, research, oversight of the health care system, law enforcement proceedings, and activities related to national security.

COMMON HIPAA COMPLIANCE ISSUES TO WATCH FOR

If you are unsure about any of these items they will be explained in more detail as you complete compliance steps within the HIPAA Rx™ software.

Privacy and Security

- Are computer screens with protected health information in plain view?
- Do workforce members leave their computers unattended with protected health information on the screen?
- Are medical records, lab reports, and faxed information easily accessible to those who have no “need-to-know”?
- Are there safeguards that are documented regarding the transfer of health information as paper medical records, orders, images, and lab specimens?
- Are there documented policies and procedures when an employment is terminated?

Security

- Do workforce members regularly change their passwords and safeguard access to their work areas?
- Is PHI stored electronically? Are there system safeguards in place?
- If health care information is transmitted on the Internet or via phone lines, are these secure transmissions?
- Does this include any e-mail communications that contain PHI?
- Is there access to health information on a web site? What safeguards are in place?
- Is there remote access to any internal networks? If so, what kind? (e.g. dial-up modem.)
- Is there a current inventory of all computer systems and software?
- Is there a regular virus check and mitigation program in place?
- What system of password maintenance is in use? Is there a formal policy that is documented?
- What other types of computer security are in place? (Examples are: a firewall, VPN, SSL, or encryption.)
- Is there a disaster plan in place that could be reviewed and expanded to include contingency plans in the event of critical systems failure?
- Do termination policies include the return of all keys, cards, and change codes and locks, as necessary?

Contracts, Policies and Procedures

- Is there an employee handbook or other human resources documentation that can be expanded to cover HIPAA requirements for security training, termination policies and procedures, etc.?
- Are there privacy/security policies and procedures as well as training to cover special functions that may be handled off-site, i.e. transcription, medical reviews, and some accounting or claims filing?

Definitions

Throughout the HIPAA compliance project you will see the following key-terms used frequently:

PHI, Protected Health Information – Individually identifiable health information

CE, Covered Entity – A healthcare provider, healthcare clearinghouse, or health plan

Business Associates – An organization that provides a service on behalf of a healthcare provider involving use or disclosure of health information.

Authorization – A document signed by an individual, or the individual's personal representative, that permits a covered entity to use or disclose certain protected health information.

Accounting of Disclosures – A detailed report showing any uses or disclosures of PHI.

Minimum Necessary – The limitation of protected health information to the minimum necessary to accomplish the intended purpose.

The following terminology appears in the HIPAA regulations and the HIPAA Rx software. The definitions have been extracted directly from the HIPAA regulations:

Business associate:

Business associate means, with respect to a covered entity, a person who:

- (i) On behalf of such covered entity or of an organized health care arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
 - (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 - (B) Any other function or activity regulated by this subchapter; or
 - (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
- (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as

described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

Covered entity means:

- (1) A health plan.
- (2) A health care clearinghouse.
- (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

HHS stands for the Department of Health and Human Services.

Health care means care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Secretary means the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services or practices:

- (i) Classification of components.
 - (ii) Specification of materials, performance, or operations; or
 - (iii) Delineation of procedures; or
- (2) With respect to the privacy of individually identifiable health information.

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- (1) Health care claims or equivalent encounter information.
- (2) Health care payment and remittance advice.
- (3) Coordination of benefits.
- (4) Health care claim status.
- (5) Enrollment and disenrollment in a health plan.
- (6) Eligibility for a health plan.
- (7) Health plan premium payments.
- (8) Referral certification and authorization.
- (9) First report of injury.
- (10) Health claims attachments.
- (11) Other transactions that the Secretary may prescribe by regulation.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.