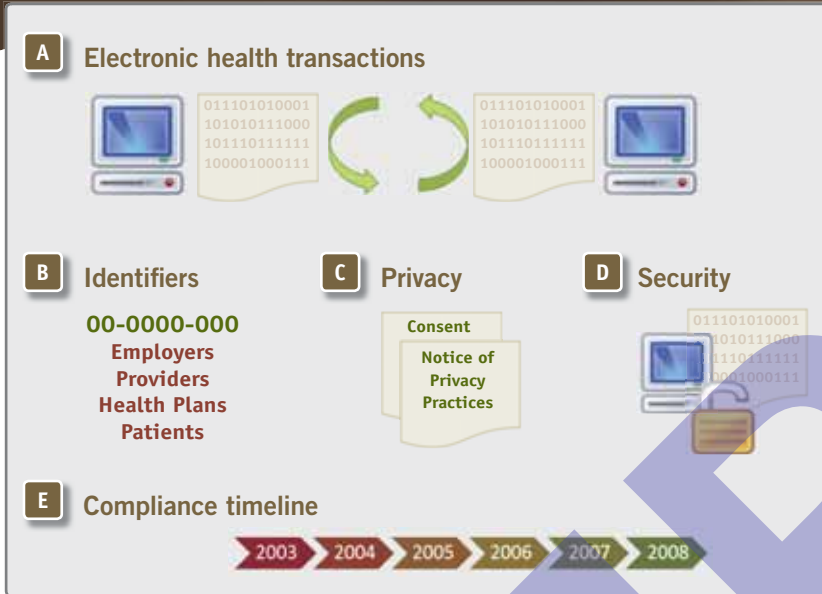


# HIPAA Overview



The Administrative Simplification Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have a major impact on covered entities, as well as on many health care business partners. Some changes involve computer system modifications. Covered entities need to know how to make their practices, health plans, and health care clearinghouses compliant with the HIPAA Administrative Simplification Rules. There are four sets of standards:

- A Standards for electronic transactions**  
Define standards for conducting *electronic data interchange* (EDI) and certain Web-based *direct data entry* (DDE) administrative health transactions.
- B Standards for identifiers**  
Define national identifiers for four categories: employers, providers, health plans, and patients. These are intended to replace all other identifiers used for each category. So far, two of the four identifier categories have been adopted: employers and providers.
- C Standards for privacy**  
Define who is authorized to use and disclose individually identifiable health information (defined by HIPAA as *personal health information* or PHI) and spell out individuals' health care information rights. These rights include access to one's own record, the ability to file privacy complaints, the ability to request health record amendments, and so forth. In addition to privacy, the Privacy Rule also specifies that all PHI, no matter what form it's in, must be protected and secured.
- D Standards for security**  
Define administrative, physical, technical, and organizational safeguards, and define policies and procedures for securing *electronic protected health information* (ePHI).
- E Compliance timeline**
  - **October 16, 2003:** Transactions and Code Sets
  - **April 14, 2003:** Privacy
  - **July 30, 2004:** Employer Identifier
  - **April 21, 2005:** Security
  - **February 16, 2006:** Enforcement Rule finalized
  - **May 23, 2007:** National Provider Identifier (12-month contingency period ending May 22, 2008, approved by the Center for Medicare & Medicaid Services [CMS])

## HIPAA ADMINISTRATIVE SIMPLIFICATION

### HIPAA Basics 2

- DSMOs and related organizations
- Covered entities
- Civil and criminal penalties
- Key terms, such as *individually identifiable health information* (IIHI), *protected health information* (PHI), and *business associate*

### Transaction Standards 3

- Transactions
- ANSI ASC X12N 4010A1 standards
- Code sets
- The National Provider Identifier (NPI) and other identifiers
- TPO

### Privacy Standards 4

- Privacy standards
- Privacy policy documents
- Administrative requirements
- A 16-step privacy solution

### Security Standards 5

- Security standards
- Common security threats
- Security categories
- Key security terms, such as *authentication*
- A 12-step security solution

### Top Productivity Tips and Solutions 6

- Prepare an organization for HIPAA compliance
- Brief executives on the scope of HIPAA
- Prepare for the transaction standards
- Prepare for the national identifier standards

## GETTING HELP

### Additional CourseCARDS

To order additional CourseCARDS, which cover additional HIPAA content that you might find useful, visit [www.axopress.com](http://www.axopress.com).

### Additional Solutions

For additional HIPAA compliance solutions, such as training, manuals, consulting, and templates, contact the Supremus Group at [www.training-hipaa.net](http://www.training-hipaa.net).

NOT FOR PRINTING OR INSTRUCTIONAL USE

## DSMOS AND RELATED ORGANIZATIONS

### Designated Standards Maintenance Organizations (DSMOs)

DSMOs are organizations named by the U.S. Department of Health and Human Services (HHS) to maintain standards, using criteria as defined in the published rules. There are six DSMOs:

- **ANSI Accredited Standards Committee (ASC) X12:** An organization that develops electronic-data-exchange standards for multiple business domains, including health care and insurance. Web site: [www.X12.org](http://www.X12.org)
- **Dental Content Committee of the American Dental Association (ADA):** The professional association of dentists that is involved in education, research, and the development of standards. Web site: [www.ada.org](http://www.ada.org)
- **Health Level Seven (HL7):** An ANSI-accredited group that defines standards for the cross-platform exchange of data within and between health care organizations. Web site: [www.hl7.org](http://www.hl7.org)
- **National Council for Prescription Drug Programs (NCPDP):** An ANSI-accredited group that maintains a number of standard formats for use by the retail pharmacy industry. Web site: [www.ncdp.org](http://www.ncdp.org)
- **National Uniform Billing Committee (NUBC):** An organization that works to develop a single billing form and standard data set that could be used nationwide for handling institutional health care claims. Web site: [www.nubc.org](http://www.nubc.org)
- **National Uniform Claim Committee (NUCC):** An organization that works to develop a standardized data set for use by the non-institutional health care community to transmit claims to and from third-party payers. Web site: [www.nucc.org](http://www.nucc.org)

### Related organizations

- **Centers for Medicare and Medicaid Services (CMS):** A division of HHS that is responsible for implementing and enforcing provisions of HIPAA (except the Privacy Rule). Web site: [www.cms.hhs.gov](http://www.cms.hhs.gov)
- **Workgroup for Electronic Data Interchange (WEDI):** An advisory body to HHS. WEDI works to streamline health care administration by standardizing electronic communications, and to improve privacy and security of patient/health-plan data. Web site: [www.wedi.org](http://www.wedi.org)
- **Washington Publishing Company (WPC):** The official publisher of the X12N HIPAA Implementation Guides and the X12N HIPAA Data Dictionary (current approved version: ASC X12 4010A1). Web site: [www.wpc-edi.com](http://www.wpc-edi.com)
- **National Committee on Vital and Health Statistics (NCVHS):** An advisory committee to HHS. The NCVHS identifies common problems that are complicating compliance activities and submits recommendations to HHS for solving identified problems. Web site: [www.ncvhs.hhs.gov](http://www.ncvhs.hhs.gov)

## COVERED ENTITIES

### Health plan

An individual or group plan that provides, or pays the cost of, medical care. This includes public health plans such as Medicare and Medicaid; private health plans; and employer-sponsored group health plans.

### Health care clearinghouse

An entity that processes HIPAA-covered transactions on behalf of health plans and providers. The information may be received in a non-standard format and translated into a standard one, and vice versa, or may represent the exchange of standard transactions between two covered entities.

### Health care provider

A provider of health care (as defined by HIPAA and the Social Security Act), and any other person or organization who furnishes, bills for, or is paid for health care and who sends and/or receives HIPAA-defined electronic transactions directly or indirectly. Includes, but is not limited to:

- Physicians
- Laboratories
- Hospitals
- Behavioral health specialists
- Dentists
- Alcohol and drug abuse dependency treatment providers
- Clinics
- Certain long-term-care providers
- Pharmacies

## PENALTIES

### Civil

FINE	PRISON TIME	OFFENSES
\$100	NA	Single violation of a provision (multiple penalties for violating multiple provisions).
\$25,000	NA	Multiple violations of an identical requirement made during a calendar year.

*NOTE: The Secretary may reduce the fine if a violation is not due to willful neglect and is corrected within 30 days.*

### Criminal (maximum penalties)

FINE	PRISON TIME	OFFENSES
Up to \$50,000	Up to one year	Wrongful disclosure of individually identifiable health information (IIHI).
Up to \$100,000	Up to five years	Wrongful disclosure of IIHI committed under false pretenses.
Up to \$250,000	Up to ten years	Wrongful disclosure of IIHI committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.

## KEY TERMS

### Individually identifiable health information (IIHI)

Information that is created by a health care organization; relates to the past, present, or future diagnosis, treatment, or condition of an individual; and could be used to identify that individual.

### Protected health information (PHI)

Any patient/health plan member identifiable information, regardless of the form it is in (electronic, paper, or verbal) and whether it is or isn't active.

### Patient/health plan member identifiable information

Identifiers, within health information, that could be used to identify an individual. Examples: name, address, Social Security number, e-mail address, photographic images, phone numbers, and rare health conditions.

### De-identified information (DII)

Health information that has had all personal identifiers removed from the data set. May be disclosed without consent of the individual.

### Business associate

An individual or entity who, on behalf of the covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of PHI. May include but is not limited to legal, actuarial, accounting, consulting, IT vendors, third-party administrators, collection companies, and auditors. Doesn't include the covered entity's workforce.

### Workforce

Employees, volunteers, trainees, contractors, and other people under the direct control of a covered entity.

### Agents

Business associates, employees, volunteers, trainees, contractors, and other people under the direct control of a covered entity. For purposes of rule enforcement, a business associate is not an agent of the covered entity as long as the appropriate Business Associate Contract has been executed and the covered entity has developed a due diligence regarding compliance with HIPAA privacy and security requirements. Covered entities are considered responsible for the actions of all of their agents.

## TRANSACTION STANDARDS

## Transactions

Health care administrative transactions, which include patient scheduling, registration, billing, and payment. Health care business applications are involved in the storage and movement of health records and transactions. Health care transactions are varied. Some health care administrative transactions are covered by HIPAA, and some others are not.

## Transaction set

A group of logically related data in units. The smallest meaningful set of data exchanged between trading partners, including health plans, health care providers, health care clearinghouses, and business associates.

## Functional group

A grouping that adds relevance to two or more data segments. Introduced by a group start segment; concluded by a group end segment.

## National Provider and Payer Enumeration System (NPPES)

A central electronic system that will identify and uniquely enumerate health care providers (individual and organizational) and health plans at the national level.

## Enumerator

The organization that will assign unique health care provider and health plan identifiers and maintain the NPPES database.

## ANSI ASC X12N 4010A1 standards

All of the transactions adopted by this rule are from the ANSI ASC X12N, except the standards for retail pharmacy transactions, which are from the National Council for Prescription Drug Programs (NCPDP).

REGULATED TRANSACTION TYPE	X12 TRANSACTION SET IDENTIFIER
Eligibility, Coverage, or Benefit Inquiry	ASC X12N 270 (004010A1 X092)
Eligibility, Coverage, or Benefit Information Inquiry Response	ASC X12N 271 (004010A1 X092)
Health Care Claim Status Request	ASC X12N 276 (004010A1 X093)
Health Care Claim Status Response	ASC X12N 277 (004010A1 X093)
Health Care Services Review: Request for Review	ASC X12N 278 (004010A1 X094)
Health Care Services Review: Response	ASC X12N 278 (004010A1 X094)
Payment Order/Remittance Advice	ASC X12N 820 (004010A1 X061)
Benefit Enrollment and Maintenance	ASC X12N 834 (004010A1 X095)
Health Care Claim Payment/Advice	ASC X12N 835 (004010A1 X091)
Health Care Claim: Institutional	ASC X12N 837I (004010A1 X096)
Health Care Claim: Dental	ASC X12N 837D (004010A1 X097)
Health Care Claim: Professional	ASC X12N 837P (004010A1 X098)

## Scope

Transaction standards apply only to EDI sent directly or indirectly between health care providers and health plans as part of a standard transaction.

*EXCEPTION: Web-based transactions (DDE transactions) that include the same content as the defined ASC and NCPDP transactions are also considered standard or covered transactions.*

## Compliance

All covered entities that choose to transmit any transactions in electronic form (including DDE) should have complied with the final rule by October 16, 2003. All health plans are required to accept all covered transactions from providers and cannot finalize the provider in the health plans required to employ a health care clearinghouse to translate HIPAA standard transactions into proprietary transactions.

## CODE SETS AND IDENTIFIERS

## Code sets

Code sets are used for encoding data elements.

- **ICD-9-CM Volumes 1 and 2:** International Classification of Diseases, 9th Revision, Clinical Modification, must be used to identify diseases, injuries, impairments, and other health problems. Updated by the Department of Health and Human Services (HHS).
- **ICD-9-CM, Volume 3:** Must be used to describe/identify inpatient hospital services and surgical procedures. Updated by HHS.
- **CPT-4:** Current Procedural Terminology, 4th Revision, must be used to identify physician services or procedures. Owned by the American Medical Association (AMA).
- **CDT:** Code on Dental Procedures and Nomenclature must be used to describe dentist services or procedures. Owned by the ADA.
- **NDC:** National Drug Code must be used to identify drugs. Updated by HHS and the Food and Drug Administration (FDA).
- **HCPCS:** Health Care Common Procedure Coding System must be used to describe health-related services that are not physician, dentist, or hospital services or procedures. Examples include radiological procedures and hearing and vision services. Updated by CMS.

## National Provider Identifier (NPI)

All HIPAA-covered providers are required to obtain an NPI associated with:

- Individual providers
- Organizational providers (known as subpart NPIs)
- Notes to keep in mind on NPIs:
  - Individual providers keep their NPIs for life.
  - Organizations can get multiple subpart NPIs.
  - Individual NPIs are just now being linked to subpart NPIs in the National Provider and Payer Enumeration System (NPPES).
  - Organizations and health care providers must apply for an NPI through the national enumerator designated by CMS.
  - Non-health-care providers (those who provide health-related services, but the services provided are not specifically defined as "health care" under HIPAA and the Social Security Act) are not eligible to apply for an NPI.
  - Non-covered health care providers may apply for an NPI.
  - The NPI must be shared with any entity or individual who needs the number for health care administrative and clinical purposes.

## Other identifiers

- **National Health Plan Identifier (NHPI):** A standard and uniform identifier that would apply to health plans. No date set by CMS for publication of the draft rule defining the NHPI.
- **National Employer Identifier for Health Care (NEI):** A standard for a national employer identifier and requirements concerning its use. The IRS Employer Identification Number (EIN) is the standard for NEI.
- **National Health Identifier for Individuals:** A standard for a national health care identifier for individuals. Currently on hold and not likely to be defined in the rule.

## TPO

## TPO (Treatment, Payment, or Health care operations)

- **Treatment:** Refers to using PHI to diagnose, provide, coordinate, or manage health care and related services.
- **Payment:** Refers to using PHI to obtain payment for health care services provided. May include claim validation, pre-authorization requirements, and requests for additional health information related to a claim that a health plan needs additional information before a payment can be made.
- **Health care operations:** Refers to using PHI to support the business activities for a provider or health plan. May include quality assessment, employee review, training of medical students, licensing, credentialing, limited marketing activity, and fund-raising activities.

## PRIVACY STANDARDS AND DOCUMENTS

### Privacy standards

Policies that define who may use and disclose PHI; clearly define patient/health plan member rights; define special uses of PHI (such as research, marketing, or fund-raising); define PHI authorization requirements; and define when PHI may be released without authorization.

#### Individual rights:

- Allowed access to health record
- Request amendment of health record
- Request restriction of information
- Request alternative communications
- Allowed accounting of PHI disclosures (except for TPO or if specifically authorized by patient/health plan member)
- Allowed avenue to report privacy complaints to the organization and the HHS Office of Civil Rights (OCR)
- Verbally deny access to or communication of PHI to friends or family
- Excluded from hospital directory
- Opt out of fund-raising mailings
- Notice of organizational or joint (organized health care arrangement) privacy practices

• **Use:** Refers to sharing, employing, applying, utilizing, examining, or analyzing PHI by members of an organization's workforce and business associates. Also, use includes the sharing or disclosing of PHI to other authorized individuals or entities.

• **Disclosure:** Releasing, transferring, providing access to, or divulging in any manner, information outside the entity responsible for maintaining the information. The disclosure must only be made to an authorized individual or entity. Disclosures for TPO and limited exceptions may be made to another covered entity or business associate of the covered entity without authorization. Any other disclosure requires an authorization from the patient/health plan member or his/her personal representative. Other state and federal laws may have more stringent requirements.

### Privacy policy documents

- **Notice of Privacy Practices (NPP):** Describes the use and disclosure of PHI for carrying out TPO and other circumstances where PHI may be released without authorization. Describes the privacy policies of the covered entity. Describes a patient or health plan member's rights as outlined in the HIPAA Privacy Rule. A written acknowledgement of receipt must be requested of new patients by direct care providers (patients are not required to sign). If the covered entity has a Web site, the NPP must be prominently displayed on it.
- **Authorization:** Authorization to use or disclosure of PHI where specific authorization is not required. State and federal laws may require authorization for TPO.
- **Consent:** Consent, for purposes of releasing PHI, is optional and applies only to the exchange of PHI for TPO.
- **Business Associate Contract (BAC):** Addresses the requirements related to protecting the privacy and security of a patient or health plan member's PHI when using and disclosing PHI on behalf of the covered entity. Creates a requirement to comply with HIPAA privacy and security rules "by contract."
- **Data Use Agreement:** An agreement with a recipient of the PHI data that limits their use of the PHI and the method of PHI exchange.
- **Designated Record Set (DRS):** A specifically defined set of documents, data, films, and claim reports that are included in the patient's medical record or the health plan member's claims record. The patient/health plan member has the right to request to view, request a copy of, or request a summary of his/her DRS.
- **Document Retention:** The requirement that covered entities or any of its agents retain documentation related to HIPAA defined activities for a minimum of six years (or the maximum required by state or other federal laws).
- **Privacy Officer Position Description:** Description of the Privacy Officer's responsibilities.
- **Security Officer Position Description:** Description of the Security Officer's responsibilities.

## REQUIREMENTS AND SOLUTION

### Administrative requirements

1. **Personnel:** Assign a Privacy Officer and a Security Officer (can be the same workforce member).
2. **Complaints:** Identify how to address complaints within the organization, and clearly communicate a patient or health plan member's right to complain to the OCR.
3. **Policies and procedures:** Documented policies and procedures that clearly indicate the covered entity's program for complying with the HIPAA Administrative Simplification Rules and other applicable federal and state privacy/security laws. Must be periodically reviewed, current, accurate, enforceable, communicated to affected workforce members, and easily understood. *Policies* are high-level statements. *Procedures* are detailed instructions regarding policy compliance.
4. **Documentation:** Create and maintain documentation related to the HIPAA Administrative Simplification Rules. Must be retained for a minimum of six years.
5. **Training:** Provide training for new workforce members and existing workforce. Specialize training as needed (for example, IT security, health records management, and patient rights management). Training should cover:
  - Privacy and security requirements (all state and federal laws)
  - Policies, procedures, and practices that ensure compliance with the HIPAA Administrative Simplification Rules
6. **Security safeguards:** Implement administrative, physical, technical, and organizational security safeguards (all PHI, in any form).
7. **Sanctions:** Create a policy that describes specific actions against members of the workforce who fail to comply with HIPAA, other federal law, state law, and the covered entity's established privacy and security policies and procedures.
8. **Mitigation:** Create a policy that includes steps to remedy any harm caused by a disaster, inappropriate disclosure of PHI, theft of data or hardware, and so forth, and to prevent such from re-occurring.
9. **No intimidating or retaliatory acts:** An organization cannot intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient or health plan member for exercising any right under the Privacy or Security Rule, including filing a complaint.
10. **No waiver of rights:** An organization cannot require, as a condition of TPO or eligibility of benefits, that an individual waive his/her privacy rights or the right to file a complaint with OCR (privacy) or CMS (security).

### HIPAA privacy solution: 16 steps

1. Assign privacy responsibility.
2. Inventory and assess an organization's PHI (including, but not limited to, points of access, who has access, and sensitivity of data).
3. Conduct risk analysis.
4. Assess privacy policies, procedures, and practices.
5. Analyze gaps in current policies, procedures, and practices.
6. Adjust organizational policies, procedures, practices, and documents.
7. Develop/implement periodic targeted and annual compliance audits.
8. Develop/implement disaster-recovery/emergency-mode operations plans.
9. Develop and provide workforce training.
10. Identify business associates.
  - Does the entity provide services for your organization?
  - Is the entity exempted from business associate requirements?
  - Is the service a part of treatment, payment, or health care operations for individuals served by your organization?
  - Does any such service performed require access to PHI?
11. Develop a template for BACs and negotiate BACs.
12. Develop privacy documents, templates, and forms.
13. Develop and distribute a notice of privacy practices.
14. Enforce privacy policies, procedures, and practices and patient rights.
15. Sanction workforce members for violation of privacy laws, policies, procedures, and practices.
16. Conduct privacy audits (include reviews of risk analysis, policies, training, privacy incidents, workforce compliance, and disclosure).

NOT FOR PRINTING OR INSTRUCTIONAL USE

## SECURITY STANDARDS

### Security standards

The controls, countermeasures, and procedures that reasonably ensure an appropriate level of protection for information assets and that minimize the vulnerability of and threats to information assets.

### Protect the confidentiality, integrity, and availability of PHI

- **Confidentiality** is the prevention of unauthorized use or disclosure of data.
- **Integrity** is the prevention of unauthorized modification of data or corruption of data.
- **Availability** is the prevention of loss of access by authorized individuals or entities (physical and technical) to resources and data.

### Some common security threats

- Inadequately trained workforce members
- Failure to create an incident response team
- Inadequate or weak authentication methods
- Failure to create an accurate, complete, and tested disaster-recovery plan and an associated emergency-mode operations plan
- Failure to catch malicious code (for example, viruses, spyware, Trojans, and worms) before it destroys or damages data
- Unauthorized remote or local access to the network, databases, applications, and other IT assets
- Unauthorized physical access to systems, facilities, and other physical assets
- Failure to secure wireless networks
- Failure to prevent data tampering while in transit
- Sending unencrypted PHI data over the Internet
- Theft of portable devices (laptops, hand-held computers, smart phones) and removable media (floppy disks, flash drives, CD-ROMs)
- Intentional or inadvertent loss of electric power
- Violation of security policies, procedures, and practices (intentional or inadvertent; administrative, physical, and technical and operational)
- Failure to terminate access (technical and physical) after an employee is fired or laid off
- Failure to enforce a sanctions policy
- Failure to back up data regularly and test the data-recovery process
- Failure to apply security patches and updates
- Failure to update signature files for anti-virus and anti-spyware software
- Failure to adequately protect the internal network through the use of items such as firewalls, hubs, and secure Web sites
- Failure to regularly conduct risk analysis and regularly conduct audits (targeted and compliance)

### HIPAA security categories

#### Administrative safeguards

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation

#### Technical safeguards

- Access controls
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security

#### Organizational safeguards

- Business Associate Contracts and other arrangements
- Group health plan management requirements
- Policies, procedures, and document retention

#### Physical safeguards

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

## KEY TERMS AND SOLUTION

### Key terms

- **Authentication:** Verification that an individual or entity is the one claimed. Typing a user name and a password is an example of authenticating yourself as a user on a system. Authentication is required within the organization and to authenticate external parties. A system needs to authenticate users to a degree appropriate for the level of risk or threat that an authenticated user represents. This means that multi-factor authentication may be necessary. Multi-factor authentication might include:
  - Something you know, like a password, PIN, or secret answer
  - Something you have, such as a smart card, security token, or security USB drive
  - Physical traits you have, like a fingerprint or iris recognition pattern
- **Access control:** A method of restricting access to resources, allowing only authorized individuals or entities to have access. Types of access control include:
  - Mandatory access control
  - Discretionary access control
  - Time-of-day
  - Role-based
- **Non-repudiation:** To prevent one of the entities involved in a communication from denying that he/she/it participated in all or part of the communication.
- **Evaluation:** To perform a periodic technical and non-technical evaluation (audit). The scope of the initial evaluation is to verify compliance with the HIPAA Security Rule. Subsequent evaluations should account for such items as infrastructure changes that affect the security of electronic PHI; business changes such as mergers and expansion; needed policy changes; repeated risk analysis reports; and new internal and external threats.
- **Business Associate Contract (BAC):** A contract between a covered entity and a business associate that permits the business associate to use and disclose electronic PHI on the covered entity's behalf. The covered entity must obtain satisfactory assurances that the business associate will appropriately safeguard PHI. This must be done through a signed BAC and requires due diligence on the part of the covered entity. For example, if the covered entity knows of a business associate's security breach, the covered entity must act.
- **Contingency plan:** A plan for responding to an organizational emergency. The plan should include: performing backups and testing recovery of backups; defining potentially affected business functions; addressing staffing needs; including appropriate emergency contacts; recovering from the loss of facilities; recovering from the loss of technical infrastructure; preparing critical facilities; and defining critical business functions that can be used to facilitate continuity of operations during an emergency (emergency-mode operations and recovering from a disaster). Should be regularly tested and updated. Requires staff training.

### HIPAA security solution: 12 steps

1. Assign security responsibility.
2. Perform risk analysis (at least annually).
3. Perform risk management.
4. Create security policies, procedures, and practices (administrative, physical, and technical and organizational) and provide workforce training.
5. Perform contingency planning, documentation, and testing.
6. Implement an appropriate IT security infrastructure.
7. Secure data exchange points and related processes.
8. Train and deploy an incident response team that is prepared for rapid deployment, mitigation of damages, notification of customers, patients, or health plan members when a security breach occurs, and implementation of measures to prevent similar damage in the future.
9. Create and enforce Business Associate Contracts.
10. Perform training (general HIPAA security training and, where appropriate, more detailed or specialized security training), and device security reminder.
11. Perform evaluations/audits (at least annually).
12. Enforce and apply sanctions.

## PREPARE FOR COMPLIANCE

### Additional HIPAA-related organizations

Additional HIPAA information is available at the following Web sites:

- Office of Civil Rights (OCR): [www.hhs.gov/ocr](http://www.hhs.gov/ocr)
- American Medical Association: [www.ama-assn.org/ama/pub/category/4234.html](http://www.ama-assn.org/ama/pub/category/4234.html)
- Health Information Management Systems Society (HIMSS): [www.himss.org](http://www.himss.org)
- National Institute on Standards and Technology (NIST): [www.nist.gov](http://www.nist.gov)
- International Association of Privacy Professionals (IAPP): [www.iapp.org](http://www.iapp.org)
- Information Systems Security Association (ISSA): [www.issa.org](http://www.issa.org)

### Prepare an organization for HIPAA compliance

1. Obtain executive management commitment to an organization-wide HIPAA compliance program.
2. Establish a strategic and financial plan for HIPAA compliance, and allocate the appropriate resources.
3. Establish a management position that will be responsible for the HIPAA compliance program.
4. Initiate and continue discussions with your IT partners, trading partners, and related government entities to continue to evaluate your organization's current performance relative to established HIPAA requirements.
5. Conduct training for all members of the workforce, and conduct specialized training for key executives, information management professionals, and IT professionals.
6. Follow the compliance requirements outlined in the HIPAA Administrative Simplification Rules.
7. Continue risk management, enforcement, policy review, and EDI trading-partner testing so that HIPAA compliance is not a one-time event.

### Brief executives on the scope of HIPAA

1. HIPAA privacy requirements are mandated, and more stringent state and other federal laws need to be addressed.
2. The security of patient/health-plan records must be addressed pursuant to the HIPAA Security Rule. There is a cost and it is best associated with a concept such as liability insurance versus return on investment.
3. Attention to appropriate and accurate transaction exchange (including proper use of code sets and national identifiers) is critical to the financial viability of the organization.
4. HIPAA compliance is an ongoing process and must be funded as such.

### Prepare information management systems for HIPAA

1. Prepare to send and receive (directly or indirectly) HIPAA-defined transactions.
2. Accommodate defined national employer and provider identifiers.
3. Address administrative, physical, and technical security requirements.
4. Include management of HIPAA security, privacy, TCS, and identifier issues in your emergency-mode operations and disaster-recovery planning.
5. Regularly conduct a risk analysis and weigh various means of strengthening the organization's existing privacy and security program. This step needs to involve more than IT management.
6. Maintain contact with vendors who supply your application systems, hardware, and software to determine and continue evaluating existing technical security, security gaps, and availability of security fixes or upgrades (including the software and hardware needed to generate appropriate audit logs).

## PREPARE FOR STANDARDS

### Prepare for the transaction standards

Continue to review and determine the accuracy of transactions sent and received by your organization, and monitor for changes in transaction and code set standards you will need to implement. The electronic health care transactions that health plans must accommodate include:

- Eligibility Benefit Request and Response (270/271)
- Claim Status Request and Response (276/277)
- Referral Certification (278)
- Plan Premium Payments (820)
- Benefit Enrollment and Maintenance (834)
- Payment and Remittance Advice (835)
- Dental/Professional/Institutional Health Care Claim (837D, 837P, and 837I)
- Coordination of Benefits (all 837 transactions)

### Prepare for the national identifier standards

1. Ensure that the appropriate employer identifier is being used in all HIPAA-covered transactions.
2. Covered providers should have obtained, inventoried, and validated all NPIs (individual and subpart) no later than May 23, 2007.
3. Develop and maintain *crosswalks* (spreadsheets that list old codes and the matching new codes) that include NPI and related data, such as tax ID, DEA number, license number, legacy number, address, and contact information, until mid-2009.
4. Test for compliance all applications that store, process, or transmit NPI.
5. Communicate NPIs (individual and subpart) to trading partners.
6. Covered providers must prioritize health plans, beginning with the health plan providing the largest amount of revenue.
7. Test with trading partners. Covered providers must begin testing with the largest revenue sources first.
8. Make sure the NPI contingency plan is documented, funded, and implemented to address trading partners not ready to convert to NPI.
9. Be prepared to demonstrate that a contingency plan has been implemented, and document progress toward compliance (required to qualify for the CMS NPI 12-month contingency period).
10. Regularly communicate with trading partners regarding preparedness, testing, and date of cutover to just NPI as the provider identifier. This is a **major key to success**.
11. Covered health plans must communicate with the provider community regarding the date of cutover to just NPI.
12. If you submit claims on paper (CMS 1500 and UB-04), remember that Medicare and many state Medicaid agencies require all health care providers to obtain and include an NPI on paper claims.
13. If you submit claims on paper, you should have cut over to the new CMS 1500 by June 1, 2007. Transition from UB-92 to UB-04 should have occurred no later than May 23, 2007.
14. Assign appropriate taxonomy codes to providers as required by Medicare and many state Medicaid agencies. This may require reporting taxonomy codes for multiple providers if claims 837I, 837P, and 837D are submitted electronically.
15. Implement procedures and requirements that prompt providers to update their national NPI record within 30 days of any change in required information.
16. Establish policies, procedures, and practices to communicate changes in providers and associated NPI information to trading partners.
17. Establish an audit process to determine if transactions with NPI are being processed correctly.