This chapter addresses the relevant information for medical practices from the Health Insurance Portability and Accountability Act (HIPAA) of 1996. It also includes subsequent legislation that expanded upon principles of HIPAA.

Overview of HIPAA Legislation

The main objective of HIPAA was to improve the portability and continuity of health insurance coverage. Secondarily, HIPAA enacted provisions to promote administrative simplification. Those provisions have produced numerous regulations and subsequent legislation and remain a work in progress to this day.

By including administrative simplification in HIPAA, Congress sought to improve efficiency and effectiveness of the health care system through the development of standards and requirements for the electronic transmission of health information and security and privacy protection of that information. The creation of simplified, electronic methods of doing business may seem obvious today, but in the mid-1990s, most of the administrative functions in health care were completed using the manual processes of mail, fax, and phone calls. In addition, each health plan had its own requirements and formats for completing the various transactions, thereby requiring physicians to complete the same transaction in varied ways based on the payer.

The HIPAA administrative simplification provisions sought to establish:

- unique identifiers,
- standard code sets,
- standard transactions,
- privacy rules, and
- security rules.

While all of these provisions fall under the heading of administrative simplification in HIPAA, the industry now considers administrative simplification to be limited to the unique identifiers, standard code sets, and standard transactions. Privacy and security have developed into separate areas, due to the significance of protecting the exchange of electronic health information. Each of the HIPAA provisions will be further explored in this chapter.

The requirements established in HIPAA apply to “covered entities,” which the law identifies as:

- **Health care providers**: Physicians and other providers of medical or other health care services who transmit any health information electronically.
- **Health plans**: An individual or group that provides or pays the cost of medical care. Health plans for workers’ compensation, auto, and property and casualty insurance were specifically excluded.
- **Health care clearinghouses**: Organizations that process nonstandard health information into standard formats.
HIPAA requires that any entity conducting an electronic transaction covered under the law must do so using the mandated standard transaction. An important distinction to make is that HIPAA does not require that physician practices conduct the transactions named in the law electronically. Instead, it requires the practice to use the adopted standard if the transaction is done electronically. Health plans and clearinghouses are required to accept any transactions that are sent to them using the electronic standards. Covered entities are subject to potentially significant penalties, including fines and imprisonment, for failing to adhere to HIPAA requirements.

**Administrative Simplification**

**Unique Identifiers**

HIPAA called for the adoption of unique health identifiers for use in the health care system for:

- individuals,
- employers,
- health care providers, and
- health plans.

Unique identifiers were designed to increase efficiency in transaction processing throughout the industry by creating a consistent method of identifying an entity across all of the standard transactions; however, the development and utilization of these identifiers has varied dramatically.

**INDIVIDUAL IDENTIFIER**

Despite the benefits of correctly identifying and matching patient records, concerns about privacy were immediately raised regarding the creation of a unique patient identifier. As a result, Congress prohibited the US Department of Health and Human Services (HHS) from spending money on the development of a unique patient identifier. At this time, no identifier has been implemented.

In recent years, problems have grown in correctly matching patient data across various disparate systems, as data have become more interoperable. Patient-matching strategies aim to decrease errors, and the idea of a unique patient identifier may be revisited in the coming years.

**EMPLOYER IDENTIFIER**

The employer identification number (EIN), issued by the Internal Revenue Service, was named in regulation in May 2002 as the employer identifier. As of July 2004, only the EIN can be used to identify employers in standard health care transactions.

**PROVIDER IDENTIFIER**

In January 2004, the National Provider Identifier (NPI) was established in regulation. Physicians and other health care providers were required to obtain their NPIs and begin using them in standard transactions by May 2008.

The Centers for Medicare & Medicaid Services (CMS) established the national plan and provider enumeration system (NPPES) for the assignment of NPIs. All eligible providers new to health care must obtain an NPI through the NPPES. Physicians are also required to update their information in the NPPES within 30 days of any change.
Although the NPI is only required in standard transactions, many health plans have required its use in paper and manual processes as well. Physicians and physician practices that do not conduct standard transactions are, therefore, likely to still need an NPI.

HEALTH PLAN IDENTIFIER
In September 2012, HHS published a final regulation to adopt the health plan identifier (HPID). In the industry’s review of the HPID and how it would be used, it became apparent that the issue addressed by the HPID, which was the routing of transactions, had been successfully addressed in the time between the publication of HIPAA and the subsequent HPID regulation. Concerns were raised that implementing the HPID, as now designed, would cause disruptions to the current processing of transactions. In October 2014, CMS announced a delay, until further notice, in the enforcement of the requirements of the final rule. CMS continues to solicit feedback from the industry on the need for a unique health plan identifier.

Standard Code Sets
The goal of adopting standard code sets was to eliminate the burden proprietary code sets added throughout the industry in conducting administrative transactions. Prior to standardizing the code sets, each health plan was able to establish its own code sets that had to be used by physician practices to relay different information. Practices had to track which codes to use with which health plan and submit the codes correctly to avoid having the transaction rejected.

In August 2000, HHS published the final regulation for what is commonly known as the HIPAA Transactions and Code Sets (TCS). It established two categories of code sets:

- Medical code sets
- Nonmedical code sets

Valid codes used in a standard transaction cannot be rejected. Senders and receivers of standard transactions need to be aware of the ongoing, periodic updates of code sets and have their systems ready to accept code set changes.

MEDICAL CODE SETS
Medical code sets are the code sets for clinical information and identify clinical aspects of the patient’s care, including diagnoses, procedures, and drug information. The specific medical code sets adopted under HIPAA are:

- The combination of Health Care Financing Administration Common Procedure Coding System (HCPCS), as maintained and distributed by HHS, and Current Procedural Terminology, Fourth Edition (CPT-4), as maintained and distributed by the American Medical Association (AMA), for physician services and other health care services, including physician services, physical and occupational therapy services, radiologic procedures, clinical laboratory tests, other medical diagnostic procedures, hearing and vision services, and transportation services.
- International Classification of Diseases, 10th Edition, Procedure Coding System (ICD-10-PCS), as maintained and distributed by HHS, for procedures on hospital inpatients for prevention,

- **Health Care Financing Administration Common Procedure Coding System (HCPCS),** as maintained and distributed by HHS, for all other substances, equipment, supplies, or other items used in health care services, including medical supplies, orthotic and prosthetic devices, and durable medical equipment.
- **National Drug Codes (NDC),** as maintained and distributed by HHS, in collaboration with drug manufacturers, for drugs and biologics.
- **Code on Dental Procedures and Nomenclature,** as maintained and distributed by the American Dental Association, for dental services.

**NONMEDICAL CODE SETS**

Nonmedical code sets are used for nonclinical and general administrative information. Commonly known nonmedical code sets are state abbreviations and ZIP codes. Health care specific nonmedical code sets include the Health Care Provider Taxonomy, Place of Service Codes, Claim Adjustment Reason Codes, Remittance Advice Remark Codes, Claim Status Category Codes, and Claim Status Codes. Each of these code sets provides a specific set of information to be used uniformly across various senders and receivers of the transactions.

**Standard Transactions**

The goal of the administrative simplification provisions of HIPAA was to lower costs and increase efficiencies of the administrative side of health care by standardizing electronic health care transactions. Prior to HIPAA, completing administrative functions, including submitting and processing claims, verifying eligibility, sending and receiving remittance advices for services rendered, and checking the status of a claim, were manual, often idiosyncratic to health plans, and burdensome for all stakeholders. HIPAA was designed to streamline this process through the creation of standard electronic transactions.

The original HIPAA legislation named the following transactions to be conducted using an electronic standard transaction:

- Health claims or equivalent encounter information
- Health care payment and remittance advice
- Eligibility for a health plan
- Health claim status
- Referral certification and authorization
- Enrollment and disenrollment in a health plan
- Health care premium payments
- Health care attachments
- First report of injury

HIPAA requires that these transactions be developed and maintained by a standards-development organization. These organizations operate as volunteer organizations with members from the various segments of the industry. The three standards-development organizations for health care transactions are X12, Inc. (X12), Health Level 7 International (HL7), and the National Council for Prescription Drug Programs (NCPDP). These organizations are all accredited by the American National Standards Institute (ANSI).

HIPAA requires standards-development organizations to consult with four specific organizations—National Uniform Billing Committee (NUBC), National Uniform Claim Committee (NUCC), Workgroup for Electronic Data Interchange (WEDI), and American Dental Association (ADA)—
during the development and maintenance of the standards. The Secretary of HHS is not to consider a proposal to adopt or revise standards unless these four organizations have been consulted. Through these requirements, the law laid a foundation for multi-stakeholder, cross-industry participation in the development of the standards and, as such, established a framework to maximize implementation.

**SPECIFIC TRANSACTIONS**

The TCS regulation in August 2000 established the standards to be used for seven of the nine transactions named in HIPAA. Table 1 provides an overview of these standard transactions. The first version of the X12 transactions was named Version 4010. The compliance date for using the standard transactions was October 2002.

<table>
<thead>
<tr>
<th>COMMON NAME OF TRANSACTION</th>
<th>TRANSACTION STANDARD</th>
<th>TRANSACTION FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health care claim</td>
<td>• X12 837 Health Care Claim: Professional (There are separate formats for institutional and dental claims.)</td>
<td>Submitting claims to the health plan</td>
</tr>
<tr>
<td>Remittance advice</td>
<td>• X12 835 Health Care Claim Payment/Remittance Advice</td>
<td>Receiving payment and/or remittance information from the payer</td>
</tr>
<tr>
<td>Claim status request and response</td>
<td>• X12 276 Health Care Claim Status Request • X12 277 Health Care Claim Status Response</td>
<td>Contacting the health plan for the status of a claim and receiving information about the status from the health plan</td>
</tr>
<tr>
<td>Patient eligibility request and response</td>
<td>• X12 270 Health Care Eligibility Benefit Inquiry • X12 271 Health Care Eligibility Benefit Response</td>
<td>Contacting the health insurer about the eligibility and benefits of a patient and receiving information from the health plan</td>
</tr>
<tr>
<td>Prior authorization request and response</td>
<td>• X12 278 Health Care Services Review—Request for Review • X12 278 Health Care Services Review—Response</td>
<td>Sending a request for referral authorization or prior authorization for services for a patient and receiving a response from the health plan</td>
</tr>
<tr>
<td>Enrollment and disenrollment in a health plan</td>
<td>• X12 834 Benefit Enrollment and Maintenance</td>
<td>Sending enrollment changes from the health plan—sponsoring organization to the health plan</td>
</tr>
<tr>
<td>Health plan—premium payment</td>
<td>• X12 820 Payroll Deducted and Other Group Premium Payment for Insurance Products</td>
<td>Sending payment for health insurance premiums to the health plan</td>
</tr>
</tbody>
</table>

The TCS regulation also named standards for submitting pharmacy claims and checking eligibility for pharmacy benefits. Standards for the health care attachments and first report of injury were specifically missing from the regulation, and standards for these transactions have yet to be adopted. Currently, full compliance with all of the other TCS transactions is required.

**STANDARD TRANSACTION UPDATES**

Because the business of health care is ever evolving, the standard transactions need to be modified to meet the needs of the industry. The standards development organizations continually work to update their transactions, periodically recommending that HHS adopt updated versions of the HIPAA standard transactions.

In 2009, a regulation was published to replace the original X12 Version 4010 transactions with Version 5010. As of January 1, 2012, all standard HIPAA transactions must be Version 5010. Any transactions using Version 4010 are noncompliant and will be rejected. X12 continues to work on updating its standard transactions, and the next upgrade to Version 7030 is expected to be adopted and implemented in the next several years.
Expanding the Work of HIPAA

The Patient Protection and Affordable Care Act (ACA) of 2010 expanded the administrative simplification provisions of HIPAA by enacting requirements for new transactions, operating rules, and a review committee process, as well as establishing a method to ensure health plan compliance. It also required the adoption of a standard transaction for health care attachments, which was named in HIPAA, but left out of the TCS regulation.

ELECTRONIC FUNDS TRANSFER

Although the HIPAA standard transactions covered many administrative interactions needed in the health care revenue cycle, the regulation did not establish a standard electronic form of payment. In the years following the passage of HIPAA, electronic funds transfers (EFT) became widely used throughout businesses in general, and specifically within the health care industry. EFT refers to any process through which money is exchanged electronically between two parties. Common examples of EFT are direct deposit of a paycheck into an employee’s bank account or electronic bill pay.

In order to streamline the numerous forms of EFT used in health care and create significant administrative and financial savings in the industry, the ACA required the development of a standard form of EFT. Subsequent regulation established the automated clearing house (ACH) CCD+ [cash concentration or disbursement type of transactions] addenda EFT (ACH EFT) as the standard form of EFT for health care. As with other HIPAA requirements, the ACH EFT regulation does not require a physician to accept EFT. If the physician requests to use EFT, then the health plan must use this method of payment. The deadline for complying with the EFT standard was January 1, 2014.

In recent years, many health plans have started paying physicians through payer-issued virtual credit cards (VCCs). When paying via VCCs, health plans send credit card payment information and instructions to physicians, who process the payments using standard credit card technology. The use of VCCs for payment comes at a significant cost to physicians. As with traditional credit card payments, VCC payments are subject to interchange and transaction fees. The interchange fees can run as high as 5% for certain transactions, while simultaneously health plans often receive rebates from credit card companies.

While the ACA permits VCCs or other forms of electronic payments, health plans are required to pay using the ACH EFT standard and to stop other electronic payment methods at a physician’s request.

ATTACHMENTS

To send additional information a health plan may require for adjudication of a claim or prior authorization request, providers often must send additional supporting documentation using attachments. Although named in the initial HIPAA legislation, the health care industry has yet to develop a standard electronic attachment transaction. Without a standard transaction, the process involves manual staff intervention to determine specific information needed and then faxing, mailing, or electronically submitting the documents via payer Web portals. This process often requires extensive time to complete, which can slow the timely adjudication of claims or prior authorization requests and can negatively affect patient access to timely care.

The ACA specifically required the development of a standard attachment transaction that would be implemented effective January 1, 2016; however, CMS has yet to mandate an attachment standard.

OPERATING RULES

To bring uniformity to the use of the standard transactions, the ACA required the creation of operating rules to supplement the transactions to improve industry functions and increase predictability. The HHS Secretary named the Council for Affordable Quality Healthcare (CAQH) Committee on Operating Rules for Information Exchange (CORE) as the authoring entity for these operating rules. CORE
The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a multi-stakeholder, voluntary effort to create operating rules with the goal of bringing additional efficiencies to the exchange of administrative transactions.

The CORE operating rules have been developed in phases and relate to specific transactions. While CORE has developed numerous operating rules, only those approved by CMS for enforcement under HIPAA are mandatory. Table 2 provides an overview of the operating rules and which ones have been adopted under HIPAA.

**TABLE 2 Operating Rules Adopted Under HIPAA**

<table>
<thead>
<tr>
<th>OPERATING RULE PHASE</th>
<th>TRANSACTION OPERATING RULE RELATED TO</th>
<th>OPERATING RULE FUNCTION</th>
<th>STATUS UNDER HIPAA</th>
</tr>
</thead>
</table>
| I                    | • X12 270 Health Care Eligibility Benefit Inquiry  
                       • X12 271 Health Care Eligibility Benefit Response | Establishes rules for:  
• Response times for batch and real-time transactions  
• System connectivity  
• System availability  
• Data content requirements for specific data elements | Adopted; compliance deadline was January 1, 2013 |
| II                   | • X12 270 Health Care Eligibility Benefit Inquiry  
                       • X12 271 Health Care Eligibility Benefit Response  
                       • X12 276 Health Care Claim Status Request  
                       • X12 277 Health Care Claim Status Response | Establishes rules for:  
• Response times for batch and real-time transactions for claims status response  
• System connectivity  
• System availability  
• Additional data content requirements for specific eligibility transaction data elements | Adopted; compliance deadline was January 1, 2013 |
| III                  | • X12 835 Health Care Claim Payment/Remittance Advice  
                       • ACH EFT standard | Establishes rules for:  
• System connectivity requirements  
• Data content requirements for specific data elements  
• EFT and ERA reassociation  
• Enrollment data for EFT and ERA | Adopted; compliance deadline was January 1, 2014 |
| IV                   | • X12 837 Health Care Claim  
                       • X12 278 Health Care Services Review—Request for Review  
                       • X12 278 Health Care Services Review—Response  
                       • X12 834 Benefit Enrollment and Maintenance  
                       • X12 820 Payroll Deducted and Other Group Premium Payment for Insurance Products | Establishes rules for:  
• Response times for batch and real-time transactions  
• System connectivity requirements  
• System availability | Not adopted; available for voluntary implementation |

Health plans are required to support the adopted operating rules and follow their requirements for standard transactions submitted by physicians. The operating rules that have not been adopted may be used voluntarily by health plans.

More information about CORE operating rules is available at [www.caqh.org/core/operating-rules](http://www.caqh.org/core/operating-rules).

**REVIEW COMMITTEE**

The ACA established the Review Committee, which has become a function of the National Committee on Vital and Health Statistics (NCVHS). The purpose of the Review Committee is to perform a review of the status of the current standard transactions and operating rules every two years. It is to compile its findings and make recommendations to HHS on improving and updating the standard transactions and operating rules.
ADOPTION EFFORTS STILL NEEDED

While the industry has had over 20 years with HIPAA and the goals of increasing efficiency and decreasing the burden of manual administrative process, there is still much work to be done. The CAQH Index tracks the industry’s use of electronic and manual transactions. In 2016, the CAQH Index published a report of its study on the use of HIPAA–adopted standard transactions and potential cost savings of moving the remaining manual process to the standards. Based on 2015 data, the study looked at the use of the transactions by physicians, other health care providers, and health plans. Table 3 shows the findings of the current adoption rate of the HIPAA transactions. These data clearly illustrate that there are still opportunities for increased adoption of electronic transactions in the industry and potential for significant additional savings in administrative costs. (The study estimates that US providers could save almost $8 billion if the transactions in Table 3 were all conducted using electronic standards.)

### TABLE 3 Adoption Rate of HIPAA Transactions

<table>
<thead>
<tr>
<th>HIPAA TRANSACTION</th>
<th>ADOPTION RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health care claim</td>
<td>95%</td>
</tr>
<tr>
<td>Patient eligibility request and response</td>
<td>76%</td>
</tr>
<tr>
<td>Claim payment with EFT</td>
<td>62%</td>
</tr>
<tr>
<td>Claim status request and response</td>
<td>63%</td>
</tr>
<tr>
<td>Remittance advice</td>
<td>55%</td>
</tr>
<tr>
<td>Prior authorization request and response</td>
<td>18%</td>
</tr>
<tr>
<td>Referral certification request and response</td>
<td>7%</td>
</tr>
</tbody>
</table>


Compliance with HIPAA

The goals of HIPAA to decrease costs and increase efficiencies of administrative transactions can only be achieved if the standards are implemented and followed by industry participants when completing transactions electronically. As a result, HIPAA requires covered entities to adhere to its provisions. In general, the following apply to HIPAA-covered entities:

- If a physician or other health care provider would like to conduct a transaction electronically in the standard form, the health plan may not refuse to accept the transaction.

- A health plan may not delay or reject a transaction on the basis that it is in the standard format.

- A health plan may not reject a standard transaction on the basis that it contains data not needed or used by the health plan.

- A health plan may not offer an incentive for a physician to conduct a standard transaction in a nonstandard format.

- A health plan that uses a clearinghouse to process a standard transaction may not charge fees or costs above what it would cost to process the same transaction directly with the health plan.
HIPAA regulation does not require physicians to use the standard transactions, therefore, physicians who opt to use manual methods are not in violation of HIPAA. However, physician contracts with health insurers, including Medicare, may require the use of certain electronic transactions. In these situations, physicians may be contractually obligated to process transactions using the standards.

**Enforcement of TCS Regulation**

Failure to comply with the mandatory provisions of HIPAA could result in significant penalties, including potential fines and prison. HHS assigned CMS with the oversight and enforcement of compliance with the unique identifiers, standard code sets, standard transactions, and HIPAA-adopted operating rules.

If a health plan (or an organization completing a transaction on its behalf) fails to follow the HIPAA requirements, the following steps can be taken to address the situation:

- **Contact the health plan:** Often, the quickest way of resolving a compliance issue is to contact the organization directly. This enables the physician practice to explain their concerns and receive an explanation. Physician practices are encouraged to contact the staff responsible for processing payments to attempt to resolve the issue. In addition, physician practices may also ask to speak with the health plan's compliance officer, as adequately meeting the HIPAA standards is an issue of regulatory adherence.

- **File a complaint with CMS:** The HIPAA regulation establishes a complaint process for the resolution of HIPAA standard transactions—compliance issues. CMS, the agency responsible for the enforcement of the standards, developed the administrative simplification enforcement and testing tool (ASETT) to enable physicians to test compliance and enforce their rights under the HIPAA standards. If unable to address transaction issues directly with the noncompliant health plan, physician practices are encouraged to utilize the ASETT resource to file a formal complaint with CMS. Physicians are encouraged to file complaints, especially if the issue has been raised with the health plan and the health plan has not corrected it.

In addition to the complaint process, the ACA contains a provision that requires health plans to certify compliance with the HIPAA adopted standard transactions and operating rules. On January 2, 2014, HHS issued a proposed rule addressing the requirements of health plans to certify to HHS that they are in adherence with the HIPAA transactions and operating rules. The proposed rule requires health plans to test their transaction processes and to attest their compliance with the HIPAA standards. Health plans that fail to submit such an attestation would be subject to governmental fines. A final certification rule has not yet been released, so these attestation requirements have yet to be mandated.

**HIPAA Privacy Rule**

The Privacy Rule restricts covered entities’ and business associates’ use and disclosure of an individual’s protected health information (PHI). “Business associates” include those persons and companies that physicians hire to carry out activities on their behalf, and who have access to their patients’ PHI, such as billing services, attorneys, accountants, and consultants. “Protected health information” means individually identifiable information that is held or transmitted by a covered entity or business associate in any form or media—whether electronic, paper, or oral, that relates to the past, present, or future physical or mental health of an individual, health care services, or payment for health care. The Privacy Rule also provides for individual rights, such as a patient’s right to access his or her PHI, restrict disclosures, request amendments or an accounting of certain disclosures, and a patient’s right to complain about a covered entity’s privacy and security practices without retaliation.
Notice of Privacy Practices

Covered entities must provide to all patients with whom they have a direct treatment relationship a formal notice of the uses and disclosures of PHI that may be made by the physician or his or her employees and of the patient’s rights and physician’s legal obligations with respect to PHI. This is called a Notice of Privacy Practices (NPP). The NPP also provides information on how patients may file complaints within the practice or facility and to the Office for Civil Rights (OCR). Patients must acknowledge receipt of the NPP. Note that any time the practice or facility’s privacy policies and procedures change, the NPP must be reissued.

A carefully crafted NPP can be a valuable practice asset. By clearly laying out the practice’s policies with respect to the use and disclosure of PHI and its commitment to protecting patients’ rights, the practice has:

- Set the stage for an appropriate, practice-specific training program.
- Created a powerful marketing tool demonstrating the value a practice places on patient confidentiality and welfare.
- Developed an important piece of the practice’s HIPAA compliance documentation, which not only meets a technical requirement, but also provides patients an understanding of how their PHI is used and disclosed, and thus, an opportunity to request restrictions.

The NPP must be written in plain language and contain the following elements:

- **Header**
  The NPP must contain the following statement prominently displayed: “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”

- **How the Covered Entity Will Use and Disclose PHI**
  The NPP must include a series of specific statements relevant to the practice’s use and disclosure of PHI, including when the patient’s authorization will be required. Remember, if the physician practice is in a state that has laws that are more protective of patients’ rights than HIPAA, the NPP must be consistent with those more stringent requirements.

- **Individual Rights**
  The NPP must contain a statement of the individuals’ rights with respect to PHI and a brief description of how the individual may exercise those rights. These rights include:
  - The right to inspect and copy PHI
  - The right to amend PHI
  - The right to request restrictions on certain uses and disclosures of PHI
  - The right to receive confidential communications that include PHI by alternative means or at alternative locations
  - The right to prohibit the sale of patients’ PHI for its use in marketing purposes or its use in research
  - The right to receive an accounting of disclosures of PHI (ie, a list of third parties that have been given access to the patient’s PHI)

- **Covered Entity’s Duties**
  The NPP must include the covered entity’s various duties under the HIPAA Privacy Rule, including the duty to abide by the practice’s current NPP.

- **Complaints**
  The NPP must state that patients may complain to the physician or to the Secretary of HHS if they believe their privacy rights have been violated. A brief description of how to file a complaint and that there will be no retaliation must also be included.
■ **Contact**
The NPP must contain the name or title and telephone number of the person (generally, the practice’s designated privacy officer) to contact for further information.

■ **Effective Date**
The NPP must contain the date on which the notice is first in effect.

■ **Optional Elements**
The practice may include, and will be bound by, any additional, voluntary limitations on its use or disclosure of PHI, provided it does not limit uses or disclosures required by law or the right, to the extent it is otherwise permitted by law and standards of ethical conduct, to disclose information the physician believes in good faith is necessary to prevent or lessen a serious and unwarranted threat to the health or safety of a person or the public.

Physicians must make copies of the NPP available to patients at their offices, to all new patients, and to anyone else on request. Physicians who maintain a website must also post the NPP on their websites.

**Business Associate Agreements**

The HIPAA Privacy Rule generally prohibits covered physicians from using or disclosing PHI except pursuant to a written authorization signed by the patient or for treatment, payment, or health care operations (eg, quality reporting). However, covered physicians can disclose PHI to their “business associates” and authorize them to create, maintain, or receive PHI on their behalf if they take specified steps to safeguard the information, including the execution of a written business associate agreement (BAA).

A “business associate” is a person or entity who provides certain functions, activities, or services for or to a physician involving the use and/or disclosure of PHI. A person who is a member of the physician practice, ie, an employee, volunteer, trainee, and other person whose conduct is under the direct control of the practice, is not a business associate. A physician or other provider who receives PHI for treatment purposes is also not a business associate.

Examples of *functions* performed by business associates include:

- Claims processing or administration
- Data analysis processing or administration
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Practice management

Examples of *services* performed by business associates include:

- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation (ie, the combining of PHI to permit data analyses relating to health care operations)
- Management
- Administrative
- Accreditation
- Financial
Some organizations with “persistent” access to PHI they maintain (such as a document-storage firm or a data center that provides hosting or electronic PHI [ePHI] backup) are also business associates. Thus, physicians must review their relationships and determine if they must enter into BAAs with these entities or others that create, receive, store, maintain, or transmit PHI on their behalf. One way to think of this is, if an organization or individual with whom the practice does business has access to the practice’s patients’ PHI, then there is a strong likelihood that the practice needs to have a BAA with them. Often, however, physicians need expert legal assistance to determine whether a particular business associate is an agent or an independent contractor.

As stated earlier, physicians may disclose PHI to business associates without patient authorization if a BAA is in place. A BAA must contain the elements listed in 45 CFR §164.504(e); among other things, the BAA must:

- Establish the permitted and required uses and disclosures of PHI by the business associate
- Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law
- Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to ePHI.
- Require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI.
- Require the business associate to disclose PHI as specified in its contract to satisfy a covered entity’s obligation with respect to individuals’ requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings.
- Require the business associate to comply with the requirements applicable to the obligation, to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule.
- Require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by the business associate on behalf of the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule.
- Require the business associate to return or destroy all PHI received from or created or received by the business associate on behalf of the covered entity, at termination of the contract, if feasible.
- Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information
- Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract

Breaches

A “breach” is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA that compromises the security or privacy of the PHI. A use or disclosure of PHI in an unpermitted way is presumed to be a breach, unless the covered physician or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made
• Whether the PHI was actually acquired or viewed
• The extent to which the risk to the PHI has been mitigated

There is no need to have an independent entity conduct the risk assessment and no risk assessment need be conducted at all if the breach notification is made (although, physicians will want to undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case). The breach notification requirement may be delegated to a business associate depending on the language in the BAA; physicians are encouraged to coordinate with their business associates so that patients receive only one notification of the breach.

Note that HIPAA only requires breach notification for unsecured PHI (eg, unencrypted PHI). As such, physicians are encouraged to use appropriate encryption and destruction techniques for PHI, which render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

**NOTIFICATION REQUIREMENTS**

Once a covered entity knows or by reasonable diligence should have known (referred to as the “date of discovery”) that a breach of PHI has occurred, the entity has an obligation to notify the relevant parties (individuals, HHS, and/or the media) “without unreasonable delay” or up to 60 calendar days following the date of discovery, even if upon discovery the entity was unsure as to whether PHI had been compromised.

If the breach involves the unsecured PHI of more than 500 individuals, a covered entity must notify a prominent media outlet serving the state or jurisdiction in which the breach occurred, in addition to notifying HHS. For breaches involving fewer than 500 individuals, covered entities are permitted to maintain a log of the relevant information and notify HHS within 60 days after the end of the calendar year via the HHS website.

**Enforcement and Penalties**

Failure to comply with HIPAA can result in significant civil and criminal penalties. The OCR enforces the privacy and security rules, while CMS enforces the transaction and code set standards. Note that while HIPAA protects the privacy and security of an individual’s PHI, it does not create a “private cause of action” for those aggrieved. This means that an individual cannot take legal action against a covered entity for a HIPAA violation. State law, however, may provide other theories of liability under which an individual may take legal action against a covered entity.

**CIVIL PENALTIES**

The Health Information Technology for Economic and Clinical Health (HITECH) Act established a tiered civil penalty structure for HIPAA violations (see Table 4). The HHS has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The penalty amount is tied to a covered entity’s knowledge of the violation, its intent to violate HIPAA, and its efforts to correct the violation by coming into compliance with HIPAA rules. Note that HHS may waive a civil monetary penalty in whole or in part in some situations.
TABLE 4 Civil Penalty Structure for HIPAA Violations

<table>
<thead>
<tr>
<th>HIPAA VIOLATION</th>
<th>PENALTY RANGE</th>
<th>ANNUAL MAXIMUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</td>
<td>$100–50,000 per violation</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>Individual “knew, or by exercising reasonable diligence would have known,” of the violation, but did not act with willful neglect.</td>
<td>$1,000–50,000 per violation</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>HIPAA violation due to willful neglect but violation is corrected within the required time period.</td>
<td>$10,000–50,000 per violation</td>
<td>$1.5 million</td>
</tr>
<tr>
<td>HIPAA violation is due to willful neglect and is not corrected.</td>
<td>$50,000 per violation</td>
<td>$1.5 million</td>
</tr>
</tbody>
</table>

The assessment of penalties must be based on five principal factors: (1) the nature and extent of the violation, including the number of individuals affected; (2) the nature and extent of the harm resulting from the violation, including financial and reputational harm; (3) the history and extent of prior compliance; (4) the financial condition of the covered entity or business associate; and (5) such other matters as justice may require.

CRIMINAL PENALTIES

Criminal penalties for a violation of HIPAA are directly applicable to covered entities. Individuals, such as directors, employees, or officers of the covered entity, may also be directly criminally liable under HIPAA in accordance with principles of corporate criminal liability. Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

If OCR receives a complaint that may violate HIPAA’s criminal provisions, OCR may refer the complaint to the US Department of Justice (DOJ) for investigation. The HIPAA criminal statute, 42 U.S.C.A. § 1320d-6, reads in pertinent part as follows:

A person who knowingly and in violation of this part [the HIPAA rules]—
(1) uses or causes to be used a unique health identifier;
(2) obtains individually identifiable health information relating to an individual; or
(3) discloses individual identifiable health information to another person,
shall be punished as provided in subsection (b) of this section [of this statute].

The statute provides that covered entities and specified individuals who “knowingly” obtain or disclose PHI in violation of the HIPAA requirements may face a fine of up to $50,000, as well as imprisonment of up to one year. Violations that occur under false pretenses may result in penalties of up to $100,000 and up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm may face fines of up to $250,000 and imprisonment for up to 10 years.

Audits

The OCR conducts periodic audits to ensure that covered entities and their business associates comply with HIPAA’s requirements. Every covered entity and business associate is eligible for an audit. In 2001, OCR established a pilot audit program in which it measured the efforts of covered entities through a set of instructions known as an audit program protocol. The protocol was updated in 2016 for the second phase of its HIPAA Audit Program. This phase of the audit program involved the review of policies and procedures by covered entities and their business associates to meet the requirements of HIPAA’s
Privacy, Security, and Breach Notification Rules. Each phase of audits has its own processes for selection and notification, as well as which specific aspects of HIPAA the audits will cover.

**Designated Record Set**

The HIPAA Privacy Rule defines the designated record set (DRS) as a group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions. Broader than the legal health record, the DRS addresses all PHI, and contains business information unrelated to patient care. Organizations must define the types of documentation that comprise the DRS and identify where the records physically exist.

**Ongoing Maintenance**

While individual states generally govern how long medical records are to be retained, documents containing PHI generally should be retained by a provider for at least six years after the later of either the date of creation or the date when last in effect (eg, six years from a minor’s eighteenth birthday). State laws may require longer holding periods. Medicare managed care–program providers are required to retain patient records for 10 years. The practice must establish retention schedules for the content of the legal health record that comply with federal and state regulations and the needs for patient care, research, and administrative purposes (eg, legal and compliance).

**Purging of ePHI**

HIPAA requires covered entities to implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of ePHI and/or the hardware of electronic media on which it is stored, as well as to implement procedures for the removal of ePHI from electronic media before the media are made available for reuse.

**HIPAA Security Rule**

The HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164) requires physicians and other covered entities to protect patients’ electronically stored PHI by using specific procedures and mechanisms. Essentially, the Security Rule operationalizes certain protections contained in the Privacy Rule. While the HIPAA Privacy Rule deals with PHI in general, the HIPAA Security Rule only addresses ePHI—it does not apply to PHI transmitted orally or in writing.

Under the Security Rule, covered entities must put in place administrative, physical, and technical safeguards to protect ePHI. However, the rule allows practices to consider their individual risks and circumstances when deciding what safeguards to implement. In other words, the regulations do not expect the same security precautions from small or rural providers as are demanded of large covered entities with significant resources. It also does not prescribe the use of specific technologies, so the health care community will not be bound by hardware and software that may become obsolete and/or may be inappropriate for certain settings.
To create a flexible approach, the Security Rule uses implementation specifications. Some specifications are required, while others are only “addressable.” Required implementation specifications must be implemented by all covered entities. Addressable implementation specifications require a covered entity to conduct an assessment whether the specification is a “reasonable and appropriate” safeguard in the entity’s environment. If the specification is reasonable and appropriate, the covered entity must implement the specification. If a covered entity determines that an addressable implementation specification is not reasonable or appropriate, it must document its assessment and basis for such a decision, and implement an alternative mechanism that achieves a similar purpose.

As an initial starting point, every entity must conduct a risk assessment to evaluate the threats to its ePHI and consider what safeguards are appropriate. In addition, every security compliance measure is required to be documented.

**Components of the Security Rule**

**RISK ASSESSMENT**

The first step in identifying and implementing safeguards that comply with and carry out the Security Rule requirements is to conduct a risk assessment. Regular security risk assessments are a fundamental component of HIPAA compliance and a focus of many audits. In addition, risk assessment is also part of performance under the merit-based incentive payment system (MIPS) and the Meaningful Use (MU) program. Consequently, failing to perform a risk assessment can lead to substantial financial penalties.

There is no single method or “best practice” for conducting a risk assessment; however, OCR has developed a downloadable security risk assessment tool (available at www.healthit.gov/providers-professionals/security-risk-assessment-tool) to assist physicians and other covered entities as they perform this requirement. This guidance helps organizations in identifying and implementing the most effective and appropriate safeguards to secure ePHI and walks users through each of the HIPAA requirements.

The scope of the Security Rule’s risk assessment includes the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. An organization must identify where the ePHI is stored, received, maintained, or transmitted and then identify and document reasonably anticipated threats to ePHI. Organizations should assess and document the security measures an entity uses to safeguard ePHI, whether security measures required by the Security Rule are already in place and if current security measures are configured and used properly. This should include consideration of different types of safeguards, such as administrative, physical, and technical.

Furthermore, the risk-analysis process should be ongoing. While the Security Rule does not specify how frequently to perform risk analysis, this process should be considered as new technologies and business operations are planned. Based on the outcome of the risk assessment, practices can then determine what specific safeguards are appropriate to protect its ePHI.

**ADMINISTRATIVE SAFEGUARDS**

Administrative safeguards include policies and procedures that set out what the covered entity does to protect its ePHI. These requirements include training for employees, regardless if they have direct access to PHI. For example, the Security Rule addresses:

- **Security Personnel:** A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

- **Information Access Management:** A covered entity must implement policies and procedures for authorizing access to ePHI only when such access is appropriate based on the user or recipient’s role (role-based access).
Workforce Training and Management: A covered entity must provide for appropriate authorization and supervision of workforce members who work with ePHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation: A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

PHYSICAL SAFEGUARDS
Physical safeguards address ways to protect physical structures and electronic equipment from unauthorized access. Some of these requirements can be accomplished by using electronic security systems, but physicians should not rely on the use of certified electronic records technology (CEHRT) to satisfy their Security Rule compliance obligations. Physical safeguards include:

Facility Access and Control: A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security: A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media, including the transfer, removal, disposal, and reuse of electronic media.

TECHNICAL SAFEGUARDS
Technical safeguards apply to actions that are related to software and technology. For example, technical safeguards include:

Audit Controls: A covered entity must implement hardware, software, and/or procedural mechanisms to examine access and other activity in information systems that contain or use ePHI.

Integrity Controls: A covered entity must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed.

Transmission Security: A covered entity must implement technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network.


The HIPAA Security Rule Documentation Mandate
The HIPAA Security Rule has a policy and procedure documentation mandate—in 45 CFR 164.316—that parallels the mandate in the HIPAA Privacy Rule. The requirements include the following:

Maintain the policies and procedures in written or electronic form.

Retain the documentation for six years from the date of its creation or from the date of revision or date when last was in effect, whichever is later.

Make documentation available to persons responsible for implementing the procedures and plans.

Review documentation periodically and update as needed (eg, in response to environmental or operational changes that affect the security of ePHI).