Overview

The Health Insurance Portability and Accountability Act was passed in 1996. The intent of the legislation was to reduce the administrative costs of health care. Although now most commonly associated with the Privacy and Security rules, the HIPAA legislation encompassed several areas of law including the availability, portability and renewability of health insurance, as well as other requirements such as changes to fraud and abuse laws, tax laws, the administrative costs in health care data transmissions and payment transmissions, and the application and enforcement provisions of group health plan regulations.

Congress recognized approximately 24 cents of every dollar spent on health care was being spent on administrative costs and not on what was most important: the provision of health care to individuals. One reason for the high administrative costs was the use of proprietary transactions between those who provided health care and those who paid for health care. Congress identified more than 400 proprietary methods for transmitting information between providers and payers. The solution was to mandate standard formats for transactions and code sets used in health care.

The standardization of electronic health information brought with it an increased concern that health information could be more readily used or
acquired for inappropriate purposes. As a result, Congress added the provisions to the statute that paved the way for what are now commonly referred to as the HIPAA privacy and security regulations.

The Administrative Simplification Section of Title II is the section of HIPAA that required the development of standardized transaction standards for content and transmission of the data, requirements for a single National Provider Identification number for all health care providers, as well as the Privacy and Security rules to protect the health information.

As Congress did not come to agreement on a Privacy or a Security standard, the Department of Health and Human Services issued the final Privacy Rule with an effective date of April 15, 2003. The final Security Rule was published later and became effective April 20, 2005.

The Privacy Rule has two essential approaches to protecting the privacy of health information. First, the rule assigns rights to individual patients to provide them with some control over their own health information. Secondly, it provides standards for the ways that health care providers, health plans and health clearing houses are permitted to access, use and disclose health information.

It should also be noted that HIPAA also includes certain administrative requirements such as the requirement for a Privacy Officer, implementation of safeguards to protect the confidentiality, integrity and availability of information, training and education requirements. However, this chapter will focus on the individual’s rights to their information, and the rules for providers and health plans to use and disclose health information.

**Preemption**

HIPAA is a national regulation and generally, if a federal statute states that it preempts or overrides state laws on a particular issue, then the federal law is the law that must be followed. The HIPAA statute has a modified pre-emption clause and is often termed a “floor,” in that it provides a national standard for the protection of health information that can be pre-empted by State laws in certain limited respects.

As a general rule, HIPAA will apply. In some states there may be specific aspects
of state law that can be more protective of the information or can provide patients with greater access or other rights to control their information, and thus would supersede the federal Privacy Rule. For example, California requires that a patient be given access to their medical record within 5 days and a copy within 15 days, which provides the patient with a greater right to their information than the 30-day time frame under HIPAA. It is necessary to understand state laws and how state law may preempt the federal HIPAA regulation in your individual state to ensure that a privacy violation does not occur. Checking with the privacy office is a good way to learn when state law might supersede HIPAA.

HITECH Act and the Omnibus Rule

Since the HIPAA rules’ effective dates, additional laws have been published that modify some aspects of the Privacy and Security rules. The Health Information Technology for Economic and Clinical Health (HITECH) Act was passed in February 2009 as part of the American Recovery and Re-investment Act (ARRA). HITECH was designed to promote the widespread adoption and standardization of electronic health records. The Act modified the Privacy and Security rules and was the first significant change to the HIPAA Privacy and Security rules since their original effective dates. HITECH includes notification requirements for breaches of unsecured information, increases the potential civil monetary penalties for violations of HIPAA, and strengthens certain privacy rights.

On January 25, 2013, the Department of Health and Human Services published the final rule to implement the statutory amendments under HITECH and to implement Section 105 of Title I of the Genetic Information Nondiscrimination Act (GINA). This rule became known as the “Omnibus Rule” and went into effect March 26, 2013, but covered entities were given until September 23, 2013 to comply with all requirements.

The Omnibus Rule made several modifications to the privacy practices that covered entities must implement including:

- Expansion of the application of business associate agreements (“BAA”) to subcontractors of covered entities;
- Modification of the standard for a reportable privacy breach and specification of the assessment criteria;
• An exclusion from the definition of marketing any treatment communications about health-related products or services by a health care provider to an individual, provided that certain opt-out conditions are included;

• A prohibition on the sale of PHI without an individual authorization;

• Requirement that covered entities provide an “opt out” option for fundraising activities;

• Requirement that additional, specific language be included in the Notice of Privacy Practices;

• Supplementation of individual rights to access to PHI for electronic records;

• Permission of payments for PHI for research purposes provided that the payment is limited to “a reasonable cost-based fee to cover the cost to prepare and transmit” the PHI for the research;

• Exclusion from the HIPAA privacy and security protections the PHI of individuals who have been deceased for more than 50 years;

• Expansion of the exception for disclosures for public health to include disclosures of proof of immunization by covered entities to schools in States that have school entry or similar laws; and

• A restriction on information provided to health plans for health care for which the individual has paid in full out of pocket.

**HIPAA Provisions**

Most health care providers are impacted by the Administrative Simplification Section of HIPAA in virtually every aspect of their work. Any piece of legislation passed by Congress will result in new terms and acronyms. HIPAA is no exception. Key terms are included in the glossary. Review of these terms may be necessary to better understand concepts discussed in this chapter.

**What Does HIPAA Govern And Who Must Comply With These Regulations?**
HIPAA governs the use and disclosure of protected health information (PHI) by “covered entities” directly and their business associates indirectly. If the organization in question does not fit the definition of a covered entity, the regulations do not apply.

**Standard Transactions and Code Sets**

The technical make-up of a standard transaction is beyond the introductory intent of this chapter. However, an introduction to the standard transactions and code sets is appropriate. The standard transactions under HIPAA are:

- 837 – Claims/Encounter
- 834 – Enrollment/Disenrollment
- 270, 271 – Eligibility
- 835 – Payment and remittance advice
- 811, 820 – Premium Payments
- 276, 277 – Claims Status
- 278 – Referral Certification and authorization
- The standard code sets under HIPAA are: ICD-10-CM
- HCPCS Level I codes (CPT® codes)
- HCPCS Level II codes (medical and surgical supplies) CDT
- NDC

The goal in developing one standardized methodology is to reduce the administrative cost of health care. This would allow the health care industry to use dollars previously spent on administrative costs to pay for the provision of health care.

**HIPAA Privacy Regulations**
The HIPAA Privacy General Rule

The HIPAA Privacy Regulations state, “a covered entity may not use or disclose protected health information (PHI) except as permitted or required by this subpart or Subpart C of part 160 of this Subchapter.” This regulation is restrictive, meaning that uses or disclosures of PHI are not permitted unless an exception or requirement is satisfied. A covered entity is defined generally by the Privacy Regulations as health care providers that transmit any health information in electronic form, a health plan with more than 50 participants, and a health care clearinghouse that receives, processes, and transmits health information for payment purposes.

Protected Health Information

The Privacy Regulations define PHI as individually identifiable health information that is created, collected or stored by a covered entity and maintained in electronic or any other form (not including educational records). Individually identifiable health information is, generally, information that describes the past, present, or future health, condition, care, treatment, of an individual, or payment for such care or treatment. In addition, to be individually identifiable health information, the health information must either identify the individual or there must be a reasonable basis to believe that the information can be used to identify the individual. As such, the cumulative test to determine whether information is PHI includes these 3 elements:

1. Health information that describes the past, present, or future health, condition, care, treatment, of an individual, or payment for such care or treatment;

2. The information must reasonably identify the individual; AND

3. The information must be maintained in electronic or any other form.

All three of these elements are required for the information to be PHI and to be protected under HIPAA.

De-Identified Information

The HIPAA Privacy regulations exclude from the definition of PHI any health
information for which all of the identifying characteristics listed in the regulations (approximately 18 depending upon how they are categorized) have been removed. The presence of one of the 18 identifiers does not mean that the information is PHI. Rather, it is the absence of all 18 identifiers that means, by rule, the information does not reasonably identify the individual and is therefore not PHI. All 18 identifiers must be removed for health information to be considered de-identified.

**Patient Privacy Rights**

Keeping patient information confidential is not a new concept to health care providers. It has always been part of the ethical obligations of the physician-patient relationship. However, an overriding theme to the privacy regulations is to place control over health information squarely in the hands of the individual who is the subject of the information. Thus, in addition to regulating the uses and disclosures of protected health information (PHI) held by a covered entity, the privacy regulations also provide individuals with certain rights regarding their PHI.

**Individual Rights under the Privacy Rule**

The federal privacy regulations under HIPAA granted individuals certain rights to be informed about and to control their PHI.

These rights include the:

1. Right to access and obtain a copy of their PHI, including receiving electronic copies of all records included in the designated record set
2. Right to amend their PHI
3. Right to obtain an accounting or listing of disclosures of their PHI
4. Right to receive a Notice of Privacy Practices
5. Right to have communications about their PHI conducted in a confidential manner
6. Right to restrict disclosure on certain uses and disclosures of their PHI
7. Right to file a complaint about a covered entity’s privacy practices to the covered entity as well as to the Office for Civil Rights (OCR)

While each of these rights appears on the surface to be straightforward, some additional discussion is warranted. It is important that covered entities fully understand the exact nature of each right that HIPAA grants individuals.

**Notice of Privacy Practices**

Health care providers and health plans are required to provide the patient with a copy of their notice of privacy practices that describes in easily understood terms how the covered entity uses and discloses the individual’s PHI, and provide examples of how their health information will be used or disclosed. For example, it should explain uses such as sending appointment reminders, sending communications such as patient classes at the medical center, how information is used in research, and other uses such as fundraising, including opt out provisions. The notice also explains what the covered entity’s legal obligations are under HIPAA, what the individuals’ rights are and who to contact with complaints and questions.

The notice should be carefully drafted. A covered entity is bound by the notice. Thus, if the notice does not fully describe how PHI is used and disclosed, it could be argued that the covered entity’s ability to use and disclose information is more restrictive than what the privacy regulations allow. In addition, if the notice is revised, it must be made available upon request. For health plans, any material change to the notice requires prominent posting of the change to the notice on its website, or other provision of the revised notice or information about the material changes to its covered individuals. The Omnibus Rule required several changes to the Notice of Privacy Practices, thus constituting a revision or material change requiring redistribution and/or notification.

The notice must be provided to the individual at the first episode of care. The covered entity is required to make a good faith effort to obtain an acknowledgement from the individual that the notice of privacy practices was received. If the first episode of care was via the telephone, the covered entity must mail its notice to the individual within 24 hours. Calling the physician’s office to schedule an appointment, or calling the hospital to schedule a
procedure, would not be considered an episode of care.

Access to Health Information

The privacy rules require that a covered entity provide individuals with access to their PHI or a copy of their PHI at their request. Individuals cannot necessarily have access to everything in the record. The covered entity can restrict the individual’s access to such things as psychotherapy notes; information the covered entity compiled to prepare for actual or anticipated litigation; or PHI that the covered entity is prohibited from sharing pursuant to the Clinical Laboratory Improvements Amendments of 1988. A covered entity that is a correctional institution may also restrict an inmate’s access to his PHI if the access would put the security of the individual, another inmate, or the institution at risk. Finally, the PHI can be restricted from an individual’s access if the PHI was obtained during a research study and the individual agreed to the restricted access in the authorization signed at the beginning of the study; if the PHI was obtained from someone other than a health care provider and the individual was promised confidentiality; or the PHI is subject to the federal Privacy Act.

A covered entity may also deny an individual access to PHI if a licensed health care professional has determined, based on her professional judgment, any of the following:

- Sharing the information would put the individual or another person in danger

- The information was obtained from someone other than another health care provider and sharing the information would be reasonably likely to put that person at risk for substantial harm

- The request for access is by a personal representative and sharing the information would be reasonably likely to put the subject of the information or another person at substantial risk of harm

If the individual is denied access for any of these three reasons, the covered entity is required to provide a method for the individual to appeal the denial. Another licensed health care professional must review the decision. The licensed health care professional reviewing the denial must not have been involved in the original decision to deny access. The covered entity is required
The HITECH Act as finalized by the Omnibus Rule added the requirement that the covered entity must provide the PHI in an electronic format if the information is maintained electronically. Although no specific format is required, the covered entity is expected to work with the individual to determine a reasonable, acceptable electronic format for the records. A covered entity is permitted to send records through unencrypted emails provided, however, that the covered entity has “advised the individual of the risk, and the individual still prefers the unencrypted email.”

**Right to an Amendment of Protected Health Information**

An individual may believe certain information in their health record is inaccurate or incomplete, and the individual has the right to request that the covered entity amend the information.

The covered entity may correct the record in a manner consistent with the entity’s policies and procedures if the information is incorrect. Note that as a general rule, original information documented in a medical record should not be altered in such a way as to completely eliminate the information.

A covered entity is not always required to make the requested amendment to the record. If the covered entity has determined that the record is accurate and complete, the individual’s request for the amendment may be denied. The covered entity may also deny requests for other reasons. One reason is that the information was not generated by the covered entity. Another reason is that the individual wishes to amend information that he or she is not entitled to access, or that the information is not part of the designated record set.

**Right to Request Restrictions**

An individual may request additional restrictions on the uses and disclosures of PHI when the use or disclosure is for treatment, payment or health care operations, or the disclosure is to a family member, friend or another individual involved in the patient’s care or payment for the care. These are the only uses and disclosures that the individual is allowed to further restrict.

The privacy rule is very explicit. While an individual has the right to request a restriction, the covered entity is under no obligation to agree to the restriction.
If a covered entity does agree to the additional restriction on the use or disclosure of PHI, then the covered entity is bound by its agreement. Generally, the administrative burden of monitoring such restrictions for a covered entity of any significant size makes agreeing to the restrictions overly burdensome.

The exception to the restriction rights was added with HITECH as finalized by the Omnibus Rule, which requires that a health care provider not disclose health information about a particular health service to a health plan provided three requirements are satisfied: (1) The individual requests that the information not be provided to the health plan; (2) The individual has paid out of pocket for the service in full; and (3) The health plan would normally obtain the information for payment or health care operations. This includes situations in which a family member is paying out of pocket for the service for the individual.

Right to Request for Confidential Communications

Unlike restrictions which further limit the manner in which PHI can be used or disclosed, a request for a confidential communication addresses the manner in which PHI is communicated. If an individual makes a reasonable request to have PHI communicated in a specific manner, a health care provider is required to accommodate the request. What does this mean? An individual may ask that the provider only call one number to communicate PHI. The individual may ask that no messages are left on an answering machine or that messages are left only on the voicemail of the individual’s cell phone. Unless the provider has a basis for arguing that the individual’s request is unreasonable, an accommodation must be made to meet the request.

The confidential communication rule varies slightly for health plans. If a health plan receives a reasonable request for a confidential communication, accommodation of the request can be contingent on the individual stating that disclosure of the information in another manner could endanger the individual.

Right to Request an Accounting of Disclosures

The HIPAA privacy regulations give an individual the right to know who has received his or her PHI. If an individual requests an accounting of disclosures, a covered entity must be prepared to provide the individual with a list of all the disclosures it has made of the individual’s PHI. An accounting is not required if
the disclosure was:

- For treatment, payment or healthcare operations
- An incidental disclosure
- Made in a limited data set
- Made with an authorization from the individual
- Made for national security purposes
- A disclosure prior to the enforcement date of the privacy regulations, April 14, 2003
- A disclosure to the subject of the information
- A disclosure that only required giving the individual an opportunity to object
- A disclosure to a correctional institution or other law enforcement official having custody of the individual for purposes of providing appropriate care to the individual.

The accounting must include: who received the information, the date the disclosure was made, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. An individual may request an accounting that covers up to a six-year period.

HITECH added a requirement that health care providers who have implemented electronic health records are required to provide patients with an accounting of uses and disclosures for treatment, payment and health care operations that are made from the electronic health record. The effective date is dependent on when the provider acquired their electronic record system. Final rulemaking has not been issued for this requirement and as such, there is currently no requirement to include disclosures for treatment, payment, and health care operations in the accounting of disclosures.

**Complaints**

The patient has a right to file a complaint regarding the covered entity’s
privacy practices with both the covered entity, usually to the Privacy Officer, as well as the Office for Civil Rights (OCR) of the Department of Health and Human Services. The patient has the right to be notified of this and contact information is generally included in the notice of privacy practices.

**Uses and Disclosures of Patient Information**

The privacy regulations were drafted with the intent of allowing the free flow of information for the provision of health care and for other purposes in the public interest. If a covered entity is not using or disclosing PHI for the direct provision of health care and related activities, then the method by which the information can be used, accessed, or disclosed will be limited.

The ways that PHI can be used or disclosed can be further divided into three subcategories:

1. Uses and disclosures the covered entity is required or permitted to make without an individual’s explicit permission

2. Permitted uses and disclosures if the covered entity has given the individual an opportunity to object to the disclosure

3. Uses and disclosures only with the individual’s explicit permission.

Put another way, a covered entity may only use or disclose PHI if the use or disclosure falls within one of the above-listed categories.

**Permitted Disclosures: TPO**

The primary uses of PHI are for one of three purposes: treatment, payment and health care operations, often referred to as “TPO.” If the use or disclosure of the PHI fits into one of these three definitions, the PHI can be used or disclosed without obtaining the explicit permission from the individual. This allowance ties directly to the intent of the privacy regulations to allow for the free flow of PHI for purposes directly related to the provision of health care. Requiring an individual’s permission to use or disclose PHI for these purposes, commonly referred to as TPO, was deemed too cumbersome to allow for efficient and effective delivery of health care.

Examples of TPO uses or disclosures:
• **Treatment**—A physician can call his or her colleague in another specialty to get the colleague’s input on the care being provided.

• **Payment**—A physician’s staff can submit a bill to the individual’s insurance company to obtain payment for the service provided.

• **Health Care Operations**—A physician’s compliance staff can access the individual’s PHI to conduct an assessment of the physician’s coding and documentation practices.

**Required Disclosures**

Required disclosures are the second method through which a covered entity may use or disclose PHI without requiring permission from the individual. There are only two instances under the privacy regulations when the covered entity is required to disclose PHI: when the information is requested by a Secretary of the Department of Health and Human Services to investigate an allegation of a privacy violation, and when the subject of the information requests it. Please see section above for a discussion on the requirement to provide an individual with access to or a copy of their health information.

**Uses And Disclosures for which an Authorization or Opportunity to Object Is Not Required**

The third method through which a covered entity may use or disclose PHI without requiring permission from the individual falls under the general category of uses and disclosures that are deemed to be in the public interest. Most of the uses and disclosures under these provisions carry restrictions on the circumstances under which the PHI can be used or disclosed and to whom it can be disclosed. It is important to understand that the privacy regulations permit, but do not require, the covered entity to use or disclose PHI for purposes in the public interest.

There are twelve categories under which a covered entity is permitted to disclose information in the public interest without first obtaining the individual’s explicit permission. The categories include:

• required by law (different from the required disclosures discussed above)
• public health activities
• reporting on victims of abuse, neglect or domestic violence
• reporting for health oversight activities
• judicial or administrative proceedings
• law enforcement purposes
• information to coroners, medical examiners, and funeral directors about decedents
• information for organ donation
• certain research purposes
• disclosures to avert a serious threat to health or safety
• specialized governmental functions
• workers’ compensation.

The details regarding circumstances when PHI can be used or disclosed for the listed public interest purposes are quite extensive. State law may also have a significant impact on uses and disclosures in the public interest. A discussion of these provisions with someone familiar with the particulars of the specific state or region where one practices is recommended.

**Access Requiring an Opportunity To Object**

The next category of uses and disclosures requires the covered entity to provide the individual with an opportunity to object prior to the use or disclosure occurring. There are three purposes to which the opportunity to object applies and any one of the three purposes will allow access to the PHI.

The first purpose is when a covered entity includes limited information about the individual in its facility directory. An individual’s name, location within the covered entity, general condition, and religious affiliation may be maintained in a directory. The information may be shared with members of the clergy. Other individuals inquiring about the individual by name can get the person’s name, location, and general condition. The subject of the PHI must be informed
of the information that will be included in the directory and given an opportunity to object to the inclusion of all or some of her PHI in the directory. The individual must also be allowed to restrict to whom the directory information is disclosed. For example, an individual might not object to information being included in the directory, but may not want it disclosed to a clergy member asking for information about individuals with a certain religious affiliation.

A second disclosure can be made if the individual is given an opportunity to object. In this situation, a disclosure can be made to family, friends, or others involved in the individual’s care or payment for the care. The information disclosed must be directly related to the individual’s involvement in the subject’s care. When the subject of the PHI is present, the disclosure can be made if the individual agrees to the disclosure, if the individual does not object to the disclosure, or if under the circumstances, one can reasonably infer in the exercise of professional judgment that the individual does not object.

If the individual is not present or is incapacitated, a disclosure to family, friends, or others involved in the individual’s care may be made if, in the exercise of professional judgment, the disclosure is in the best interest of the individual, and the disclosure is limited to the PHI relevant to the party’s involvement in the individual’s care.

Finally, a covered entity can disclose PHI under this provision for purposes of assisting in disaster relief. The disclosure can be made to either a private or public entity authorized by law, or by its character, to assist with disaster relief. Such disclosures would generally be made so the location and condition of the individual could be accessible to family and friends.

**Authorizations**

The final category of uses and disclosures may only occur with the permission from the individual in the form of an authorization. The authorization form must meet specific requirements including:

- Description of the PHI to be used or disclosed in a specific and meaningful fashion

- Name or other specific identification of the person or class of person(s) authorized to make the use or disclosure of the PHI
• Name or other specific identification of the person or class of person(s) authorized to receive the PHI

• Description of the purpose of each requested use or disclosure

• An expiration date

• Signature of the individual and date

• Statement informing the individual of the right to revoke the authorization in writing

• Any restrictions on the individual’s right to revoke and instructions for how the authorization can be revoked

• A statement informing the individual that signing the authorization is a precondition of treatment, participation in research, eligibility for benefits, or enrollment in a health plan, if applicable.

• Statement informing the individual that the recipient of the PHI may re-disclose it in a manner that makes it no longer protected by the privacy regulations.

The individual is entitled to a copy of the authorization. If an authorization does not include all the required elements, it is not valid and a covered entity cannot rely on it to use or disclose PHI. Marketing and fundraising are just two examples of uses and disclosures that require an authorization. As with any rule, however, there are exceptions.

**Fundraising**

If a covered entity wants to engage in fundraising, the HIPAA privacy rule permits the use of the limited PHI without an authorization. The limited PHI includes demographic information such as name, address, or other contact information, insurance status and date of care. This information can be used for fundraising by the covered entity or it can be disclosed to the covered entity’s business associate or an institutionally related foundation. If the covered entity wants to use additional PHI, an authorization from the individual would be required.

The HITECH Act, finalized by the Omnibus Rule, added the requirement that all
fundraising communications provide the individual with a clear and conspicuous way for the individual to opt out of receiving further fundraising requests. The way to opt out has to be easy for the individual and not cost more than a nominal amount, such as a postage stamp. Once an individual has opted out, the covered entity is prohibited from sending further fundraising communications to the individual. The covered entity is also prohibited from conditioning treatment or payment on the individual’s choice to opt out.

**Marketing**

The Privacy Rule prohibited the use of PHI for “marketing” purposes unless the patient had specifically authorized the disclosure of the information and the patient was notified by the provider that the provider was receiving direct or indirect remuneration for the disclosure of the information.

If the marketing activity is done in a face-to-face encounter with the individual, or if an item of nominal value is given to the individual, an authorization is not required. It is helpful to note that the definition of marketing under HIPAA does not include information given to an individual about particular benefits or service that is part of the individual’s health plan; information related to the treatment of an individual or information about alternative treatments, therapies, health care providers or settings of care.

The HITECH Act, finalized by Omnibus Rule, further restricts the use of PHI for marketing activities and expands the requirement for an authorization for certain health related communications sent by a health care provider to an individual in exchange for financial remuneration received from the third party whose product or service is being described. For example, an authorization is required when a health care provider is sending out a notice about new state-of-the-art medical equipment if the equipment manufacturer paid the costs of sending the mailing to the patients. There is a limited exception for refill reminders.

For subsidized treatment communications, the health care provider is required to disclose within the authorization that remuneration was received and provide an opportunity for the patient to opt out of receiving such communications.