Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry. At the same time, new technologies were evolving, and the health care industry began to move away from paper processes and rely more heavily on the use of electronic information systems to pay claims, answer eligibility questions, provide health information and conduct a host of other administrative and clinically based functions. The Privacy Rule applies to all forms of individuals' protected health information, whether electronic, written, or oral. The Security Rule is a Federal law that requires security for health information in electronic form.

**Covered entities** must follow HIPAA law. Covered entities include:

- **Health Plans**—including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.

- **Most Health Care Providers**—those that conduct certain business electronically, such as electronically billing an individual’s health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.

- **Health Care Clearinghouses**—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

In addition, **business associates** of covered entities must follow parts of the HIPAA regulations. Often, contractors, subcontractors, and other outside persons and companies that are not employees of a covered entity will need to have access to an individual's health information when providing services to the covered entity. We call these entities “business associates.” Examples include:

- Companies that help an individual’s doctors get paid for providing health care, including billing companies and companies that process an individual’s health care claims
- Companies that help administer health plans
- People like external lawyers, accountants, and IT specialists
- Companies that store or destroy medical records

Covered entities must have contracts called **business associate agreements** in place with their business associates, ensuring that they use and disclose an individual’s health information properly and safeguard it appropriately. Business associates must also have similar contracts with subcontractors. Business associates (including subcontractors) must follow the use and disclosure provisions of their contracts and the Privacy Rule, and the safeguard requirements of the Security Rule.
**Protected Health Information (PHI)**

- Information created by a doctor, nurse, or other health care provider in an individual’s medical record
- Conversations an individual’s doctor has about their care or treatment with nurses and others
- Information about an individual in their health insurer’s computer system
- Billing information about an individual at a clinic
- Most other health information about an individual held by those who must follow these laws

Many organizations that have health information about an individual **do not** have to follow these laws. **Examples** include:

- Life insurers
- Employers
- Workers compensation carriers
- Most schools and school districts
- Many state agencies like child protective service agencies
- Most law enforcement agencies
- Many municipal offices
HIPAA Privacy Rule

The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care. Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties.

Protected Health Information (PHI) The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

“Individually identifiable health information” is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual

How This Information Is Protected

- Covered entities must put in place safeguards to protect an individual’s health information and ensure they do not use or disclose an individual’s health information improperly.
- Covered entities must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose.
- Covered entities must have procedures in place to limit who can view and access an individual’s health information as well as implement training programs for employees about how to protect an individual’s health information.
- Business associates also must put in place safeguards to protect an individual’s health information and ensure they do not use or disclose an individual’s health information improperly.

Required Disclosures. A covered entity must disclose protected health information in only two situations:

(a) To individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and

(b) To HHS when it is undertaking a compliance investigation or review or enforcement action.

Note: The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g.
Permitted Uses and Disclosures

In some circumstances, use and disclosure is permitted to family and friends...for example:

- An emergency room doctor may discuss an individual’s treatment in front of a friend when the patient asks their friend to come into the treatment room.
- A hospital may discuss a patient’s bill with the patient’s daughter if the patient does not object.
- A doctor may discuss the drugs his/her patient needs to take with a health aide who has come with the patient to an appointment.
- An individual’s nurse may not discuss the patient’s condition with an individual's brother if an individual tells her not to.
- HIPAA also allows health care providers to give prescription drugs, medical supplies, x-rays, and other health care items to a family member, friend, or other person the patient sends to pick them up.
- A health care provider or health plan may also share relevant information if the patient is not present or cannot give permission when a health care provider or plan representative believes, based on professional judgment, that sharing the information is in the patient’s best interest.
- A patient had emergency surgery and is still unconscious. A surgeon may tell an individual’s spouse about the patient’s condition, either in person or by phone.

Permitted: Treatment, Payment, Health Care Operations

Treatment A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

However, most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.

Payment to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.22
More Permitted Uses

Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility.

Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated, as long as the covered entity has adopted reasonable safeguards, and the information being shared was limited to the “minimum necessary”.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as required by law (including by statute, regulation, or court orders).

- **Public Health Activities.** Covered entities may disclose protected health information to individuals who may have contracted or been exposed to a communicable disease for example.
- **Victims of Abuse, Neglect or Domestic Violence.** In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
- **Judicial and Administrative Proceedings.** Through an order from a court or in response to a subpoena

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official’s request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person’s death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.
Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

Research. *This is a special topic that requires more study.*

Serious Threat to Health or Safety. Information must be shared as needed in the event of a serious threat and to prevent harm. Professional judgment must be applied.

**Essential Government Functions** such as Department of Homeland Security

**Workers’ Compensation.** Health care providers may need to provide health information to employers for workers’ compensation determinations.

**De-Identified Health Information.** There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

**Patient Rights Provided by the Privacy Rule**

- Ask to see and **get a copy** of one’s own health records
- Have **corrections** added to one’s own health information
- **Receive a Notice of Privacy Practices** that explains how health information may be used and shared
- Decide whether to **give permission** before the health information can be used or shared for certain purposes, such as for marketing
- **Get a report of when and why** an individual’s health information was shared for certain purposes
- **File a complaint** with the provider, health insurer, and/or HHS if it’s believed rights are being denied or health information isn’t being protected
EHRs are electronic versions of the paper charts in an individual’s doctor’s or other health care provider’s office. An EHR may include an individual’s medical history, notes, and other information about an individual’s health including an individual’s symptoms, diagnoses, medications, lab results, vital signs, immunizations, and reports from diagnostic tests such as x-rays. Patients have privacy rights whether their information is stored as a paper record or stored in an electronic form. The government created the HIPAA Security Rule to require specific protections to safeguard an individual’s electronic health information.

The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI).

General Rules
The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

The Security Rule defines confidentiality to mean that e-PHI is not available or disclosed to unauthorized persons. The Security Rule's confidentiality requirements support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.

The Security rule also promotes the two additional goals of maintaining the integrity and availability of e-PHI.

Under the Security Rule, integrity means that e-PHI is not altered or destroyed in an unauthorized manner.

Availability means that e-PHI is accessible and usable on demand by an authorized person.
When a covered entity is deciding which security measures to use, the Rule does not dictate measures taken, but requires the covered entity to consider:

- Its size, complexity, and capabilities,
- Its technical, hardware, and software infrastructure,
- The costs of security measures, and
- The likelihood and possible impact of potential risks to e-PHI.

**Risk Analysis**

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI.

The Administrative Safeguards provisions in the Security Rule require covered entities to perform risk analysis as part of their security management processes.

A risk analysis process includes, but is not limited to, the following activities:

- Evaluate the likelihood and impact of potential risks to e-PHI;
- Implement appropriate security measures to address the risks identified in the risk analysis;
- Document the chosen security measures and, where required, the rationale for adopting those measures; and
- Maintain continuous, reasonable, and appropriate security protections.

**Administrative Safeguards**

**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.** Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI 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 e-PHI. 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

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. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Technical Safeguards

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

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

Integrity Controls. A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security. A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.
The changes in the final rulemaking provide the public with increased protection and control of personal health information. Changes expand many of the requirements to business associates of covered entities that receive protected health information, such as contractors and subcontractors.

This rule requires doctors, hospitals, and other health care providers to notify an individual of a “breach.” The law also requires the health care provider to notify the Secretary of Health and Human Services. If a breach affects more than 500 residents of a state or jurisdiction, the health care provider must also notify prominent media outlets serving the state or jurisdiction. This requirement helps patients know if something has gone wrong with the protection of their information and helps keep providers accountable for EHR protection.

Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation.

<table>
<thead>
<tr>
<th>Each Violation</th>
<th>Total per category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100–$50,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000–50,000</td>
</tr>
<tr>
<td>Willful Neglect—Corrected</td>
<td>$10,000–50,000</td>
</tr>
<tr>
<td>Willful Neglect—Not Corrected</td>
<td>$50,000</td>
</tr>
</tbody>
</table>

Individual rights are expanded in important ways.
- Patients can ask for a copy of their electronic medical record in an electronic form.
- When individuals pay by in full out-of-pocket, they can instruct their provider not to share information about their treatment with their health plan.
- The final omnibus rule sets new limits on how information is used and disclosed for marketing and fundraising purposes and prohibits the sale of an individuals’ health information without their permission.

**Business Associates**

The Final Rule requires that business associates and their subcontractors comply with the HIPAA rules in the same manner as covered entities. **Any entity that “creates, receives or transmits” PHI on behalf of a covered entity may be held directly liable** for impermissible uses/disclosures. Business associates and subcontractors must conduct risk assessments under the HIPAA Security Rule. Although business associates are now directly regulated under HIPAA, covered entities are still responsible for their business associates’ actions. Therefore, CEs must ensure that they obtain satisfactory assurances of HIPAA compliance through their business associate contracts and business associates must do the same for their subcontractors.