limiting the sharing of their information or opting out. If the financial institution changes its policy, it must provide another notice to the consumer.

The Safeguards Rule requires financial institutions to develop an information security policy to consider the nature and sensitivity of the information they handle. The plan must include and the company must comply with the following:

- Designate at least one employee to coordinate an information security program.
- Assess the risks to customer information within each pertinent area of the company's operation. Evaluate the effectiveness of the current safeguards and risk controls.
- Implement a safeguard program. Regularly monitor and test it.
- Choose service providers that can maintain appropriate safeguards, and govern their handling of customer information.
- Evaluate and adjust the security program in view of events and changes in the firm's operations.

Likely, most organizations will protect against pretexting as part of their information security program. The best defense against pretexting is not technical, but rather awareness and training. Training is for both employees and customers. The Pretexting provision makes it illegal to do the following:

- Make a false, fictitious, or fraudulent statement or representation to obtain customer information from the financial institution or from its customers.
- Use forged, counterfeit, lost, or stolen documents to obtain customer information from the financial institution or from its customers.

Health Insurance Portability and Accountability Act

U.S. Congress enacted the **Health Insurance Portability and Accountability Act (HIPAA)** in 1996. The primary purpose of the statute is twofold. First, it helps citizens maintain their health insurance coverage. Second, it improves efficiency and effectiveness of the American health care system. It does so by combating waste, fraud, and abuse in both health insurance and the delivery of heath care. The U.S. Department of Health and Human Services (HHS) is responsible for publishing requirements and for enforcing HIPAA laws. However, the Office of Civil Rights, a subagency of HHS, administers and enforces the Privacy Rule and Security Rule of HIPAA. These laws are divided across five titles, which include the following:

> **WARNING**
>
> Hippo has the letter P in it twice—not HIPAA. Surprisingly, many vendors that sell HIPAA solutions and even the government are guilty of misspelling the acronym for the legislation in printed literature and on Web sites.

- Title I, Health Care Access, Portability, and Renewability
- Title II, Preventing Health Care Fraud and Abuse, Administrative Simplification; Medical Liability Reform
- Title III, Tax-Related Health Provisions
- Title IV, Application and Enforcement of Group Health Plan Requirements

- Title V, Revenue Offsets

Much of the focus around HIPAA is within the first two titles. Title I offers protection of health insurance coverage without regard to pre-existing conditions to those, for example, who lose or change their jobs. Title II provides requirements for the privacy and security of health information. This is often referred to as Administrative Simplification. The broader law calls for the following:

- Standardization of electronic data—patient, administrative, and financial—as well as the use of unique health identifiers
- Security standards and controls to protect the confidentiality and integrity of individually identifiable health information

As a result, the HHS has provided five rules regarding Title II of HIPAA. These include the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule. These five rules affect information technology operations within organizations. Specifically, the Privacy Rule and Security Rule affect information security. HIPAA is primarily concerned with **protected health information (PHI)**. PHI is individually identifiable health information. PHI relates to physical or mental health of an individual. It can also relate to the delivery of health care to an individual as well as payment for the delivery of health care.

The Privacy Rule went into effect in 2003. It regulates the use and disclosure of PHI by covered entities. Covered entities, for example, include health care providers, health plans, and health care clearinghouses. In many ways, the Privacy Rule drives the Security Rule. Under the law, covered entities are obligated to do the following:

- Provide information to patients about their privacy rights and how the information can be used.
- Adopt clear privacy procedures.
- Train employees on privacy procedures.
- Designate someone to be responsible for overseeing that privacy procedures are adopted and followed.

The Security Rule followed the Privacy Rule. Unlike the Privacy Rule, however, the Security Rule applies just to electronic PHI (ePHI). The Security Rule provides for the confidentiality, integrity, and availability of ePHI, and contains three broad safeguards:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

Each of the preceding safeguards consists of various standards. All are required or addressable. Required rules must be implemented, but addressable standards provide flexibility. This way, an organization can decide how to reasonably and appropriately meet the standard. Bear in mind, however, that addressable does not mean optional.

Administrative safeguards primarily consist of policies and procedures. They govern the security measures used to protect ePHI. Table 2-1 provides a summary of the administrative safeguards, including the required and addressable standards.

TABLE 2-1 HIPAA administrative safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Security management process	Risk analysis Risk management Sanction policy Information system activity review	Required Required Required Required
Assigned security responsibility	Not applicable	Required
Workforce security	Authorization and/or supervision Workforce clearance procedure Termination procedures	Addressable Addressable Addressable
Information access management	Isolating health care clearinghouse function Access authorization Access establishment and modification	Required Addressable Addressable
Security awareness and training	Security reminders Protection from malicious software Logon monitoring Password management	Addressable Addressable Addressable Addressable
Security incident procedures	Response and reporting	Required
Contingency plan	Data backup plan Disaster recovery plan Emergency mode operation plan Testing and revision procedures Applications and data criticality analysis	Required Required Required Addressable Addressable
Evaluation	Not applicable	Required
Business associate contracts and other arrangements	Written contract or other arrangement	Required

TABLE 2-2 HIPAA physical safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Facility access controls	Contingency operations Facility security plan Access control and validation procedures Maintenance records	Addressable Addressable Addressable Addressable
Workstation use	Not applicable	Required
Workstation security	Not applicable	Required
Device and media controls	Disposal Media reuse Accountability Data backup and storage	Required Required Addressable Addressable

Physical safeguards include the policies, procedures, and physical controls put in place. These controls and documentation protect the information systems and physical structures from unauthorized access. The same goes for natural disasters and other environmental hazards. The physical safeguards include the four standards shown in Table 2-2, along with the implementation specifications.

Technical safeguards consist of the policies, procedures, and controls put in place. These safeguards protect ePHI and prevent unauthorized access. Table 2-3 lists the five safeguards and corresponding implementation specifications.

TABLE 2-3 HIPAA technical safeguards and implementation specifications.

SAFEGUARD	IMPLEMENTATION SPECIFICATION	REQUIRED/ADDRESSABLE
Access control	Contingency operations Facility security plan Access control and validation procedures Maintenance records	Required Required Addressable Addressable
Audit controls	Not applicable	Required
Integrity	Mechanisms to authenticate ePHI	Addressable
Person or entity authentication	Not applicable	Required
Transmission security	Integrity controls Encryption	Addressable Addressable

Although covered entities must comply with the previously listed safeguards and implementation specifications, there isn't a safeguard listed that should surprise organizations. In fact, most of these safeguards are addressed through best practices for any sensitive information.

In 2006, the Final Rule for HIPAA was issued—the Enforcement Rule—and set the penalties to be levied as a result of HIPAA violations. The Enforcement Rule also established the procedures for investigations and hearings into noncompliance. The potential for increased enforcement of noncompliance to HIPAA was later introduced in 2009 when the **Health Information Technology for Economic and Clinical Health (HITECH) Act** was signed into law. HITECH was part of the American Recover and Reinvestment Act (ARPA). In addition to laying the groundwork for increased enforcement, HITECH also adds requirements for a breach notification. The notification is what an organization puts in action should PHI become disclosed in a readable—that is, nonencrypted—format.

Children's Internet Protection Act

The **Children's Internet Protection Act (CIPA)** is a federal law introduced as part of a spending bill that passed Congress in 2000. The FCC maintains and enforces CIPA. This act addresses concerns about children's access to explicit content (such as pornography) online at schools and libraries by requiring the use of Internet filters as a condition of receiving federal funds. CIPA is a result of previous failed attempts at restricting indecent content. The Communications Decency Act and the Child Online Protection Act faced Supreme Court challenges over the United States First Amendment. The reason was the act violated the right of free speech contained within the Constitution.

CIPA does not provide for any additional funds for the purchase of mechanisms to protect children from explicit content. Instead, conditions are attached to grants and to the use of E-Rate discounts. *E-Rate* is a program that makes Internet access more affordable for schools and libraries.

CIPA requires schools and libraries to certify compliance to implement an Internet safety policy and "technology protection measures." This means having technology in place that blocks or filters Internet access that is either obscene, harmful to minors, or represents child pornography. This includes implementing a safety policy and controls that address the following: