© SidorArt/Shutterstock.

Overview of U.S. Compliance Laws

CHAPTER 2

TO STAY COMPLIANT WITH REGULATIONS means you must interpret the regulation. Equally important, you must understand how regulators interpret the laws. Ultimately court cases and judges decide if a company is compliant, but rarely do regulatory compliance cases ever come to court for a ruling. The vast majority of the time, company representatives will demonstrate compliance through the appropriate regulator. Consequently, three core tenants to sustain compliance include understanding the norms of the industry for compliance, having a good working relationship with regulators, and being able to evidence compliance.

A researcher from Harvard Business School published a study in 2021 that indicated the market impact of the Internet on the U.S. gross domestic product was $2.45 trillion, an eightfold increase from $300 million in 2008. The study was commissioned by the Interactive Advertising Bureau (IAB). The study found that the Internet economy grew seven times faster than the total U.S. economy during the past four years at a rate of 22% per year.

The Internet economy is driven through the exchange of personal information as well as goods and services. No government can sit on the sidelines with so much at stake, such as personal privacy and the economic impact to name a few. state governments and the federal government establish laws (referred to as "regulations") that define how to control, handle, share, and process sensitive information that this Internet economy relies on. Much of that information is about you! "Regulators" are the individuals who help enforce these rules. Industries also try to "self-regulate," which means they create standards their members must follow. Failure to follow regulations or industry standards can result in fines or limits placed on the ability to operate. Gross violations of regulations can be seen as a violation of criminal law. These violations can result in the arrest of company officers and potential jail time.

In this chapter, we discuss major government laws and their compliance requirements. When we refer to regulations in this chapter, we mean those that relate to U.S. laws. We see how these requirements will influence security

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

policies. We examine major drivers for the regulations and the importance of protecting personal privacy. Many industry standards and government regulations affect information technology (IT) operations. Remember, each country has its own laws and regulations. Thus, the number of compliance laws and regulations expands greatly. Keep in mind that we are only scratching the surface. Other compliance regulations exist and are often specific to a particular industry.

Chapter 2 Topics

This chapter covers the following topics and concepts:

- What public and private sector regulatory requirements are
- What the Federal Information Security Management Act is
- What the Red Flags Rule is
- What the Cybersecurity Information Sharing Act is
- What the Sarbanes-Oxley Act is
- What the Gramm-Leach-Bliley Act is
- What the Health Insurance Portability and Accountability Act is
- What the Children's Internet Protection Act is
- What the Children's Online Privacy Protection Act is
- What the California Consumer Privacy Act is
- What the Family Educational Rights and Privacy Act is
- What the Payment Card Industry Data Security Standard is

Chapter 2 Goals

When you complete this chapter, you will be able to:

- Describe the goals and requirements for key acts of Congress
- Describe the goals and requirements of the Payment Card Industry Data Security Standard
- Describe various regulations concerning the protection of health, accounting, and other information

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Introduction to Regulatory Requirements

There are government concerns with consumer protection, promoting a stable economy, and maintaining a reliable source of tax revenue. All three of these drivers are linked. If people feel safe using the Internet to buy goods and services, a stable economy emerges. When you have a stable sector of the economy, the government has a reliable source of tax revenue. This is not to imply that any one of these drivers is the primary goal of government regulation. However, government regulations do exist, and the question is what to regulate and how much.

When you implement security policies, remember that there are pressures and trade-offs. For example, you may have to place restrictive controls on data to comply with a regulation that limits how your business operates. As you balance competing interests, you must be talking to the business. Security policies reflect how the business wishes to balance competing interests.

Nevertheless, it is first important to understand why these requirements exist. Equally important is to understand how the regulator within your industry interprets these regulations. It is the regulator interpretation that will set expectations on what controls the organization must deploy.

WARNING

There is an irony in regulatory compliance laws. Although the laws might appear complicated, they make high-level points that are simple to understand. A problem occurs when people interpret regulations in different ways.

technical TIP

Your internal policies should define what controls must be deployed to meet regulators' expectations. Policies should follow a framework that is easily understood and promotes compliance. Having a framework demonstrates a company's planned approach. Meanwhile, the policies demonstrate a company's drive and support to be compliant. Take the time to properly build your internal policies. This rids you of many headaches in the event you must undergo an audit. In other words, ensuring your policies follow a solid framework to comply with different regulations really pays off.

An example is the General Data Protection Regulation (GDPR), which was adopted by the European Union (EU) in May 2018. GDPR brings greater obligations on companies processing and handling personal data of individuals who live in Europe. Why is this important to U.S. companies? EU citizens buying products over the Internet or EU citizen traveling to the United States would be covered by the GDPR regulations. While this chapter only focuses on U.S. laws, a broader view of regulations would be needed.

Regulatory compliance is nothing new. However, government oversight and strong compliance regulations greatly increased due to the expansion of the Internet. Consider how quickly the Internet has become part of our daily lives. It's not just the browser we

WARNING

If you do business in other countries, you need to consider the requirements and compliance laws of those foreign countries. In addition, many U.S.-based companies rely on foreign, third-party service providers. This could result in noncompliance with U.S. or foreign regulations.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

use to surf the Internet that impacts our lives daily. Our doorbell may have an Internet camera, we may be using an Internet phone (smartphone), or those unwanted robot calls are usually generated through data obtained through the Internet.

Regulatory Acts of Congress

Congress enacts major legislation known as *statutes*. The president of the United States signs these **acts of Congress** into law. Examples of such acts include the Cybersecurity Information Sharing Act (CISA) of 2015, E-Government Act of 2002, the Sarbanes-Oxley (SOX) Act, and the Health Insurance Portability and Accountability Act (HIPAA).

After such acts become law, various government agencies create and enforce the federal regulations authorized by those acts. Some examples of these government agencies are the Food and Drug Administration (FDA), Environmental Protection Agency (EPA), U.S. Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), and Federal Communications Commission (FCC), to name a few.

Congress first typically passes a statute to address a problem, such as a social or economic issue. These are considered enabling legislation that allow **regulatory agencies** to create the necessary regulations to implement the law. (A regulatory agency is a public or government agency that has authority over some area of activity in a regulatory or supervisory capacity.) For example, the FCC creates regulations under CIPA. The SEC creates regulations under SOX.

Federal Information Security Management Act

The **Federal Information Security Management Act of 2002 (FISMA)** is contained within the **E-Government Act of 2002**, Public Law 107-347, as Title III. This act grants the importance of sound information security practices. It also controls the interest of national security and the economic well-being of the United States. This act was amended in 2014 by the Federal Information Security Modernization Act of 2014, which provides several key changes.

The purpose of FISMA is to do the following:

- Provide a framework for effective information security resources that support federal operations, data, and infrastructure
- Accept the interconnectedness of IT. Ensure effective risk management is in place
- Ensure coordination of information security efforts between civilian, national security, and law enforcement communities
- Facilitate the development and ongoing monitoring of required minimum controls to protect federal information systems and data
- Provide for increased oversight of federal agency information security programs
- Recognize that information technology solutions may be acquired from commercial organizations but leave the acquisition decisions to the individual agencies

FISMA tasked the National Institute of Standards and Technology (NIST) to develop and set standards and guidelines. These apply to federal information systems. Standards help

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

categorize information and the systems. They are developed using a risk-based approach. They include the minimum information security controls. For example, standards include the management, operational, and technical controls to apply to information systems.

NIST publications outline a complete set of security standards and processes. To be compliant, your policies must include key security control requirements. Regardless of the publication, often these requirements include the following:

- **Inventory**—The standards require an inventory of hardware, software, and information. The inventory identifies the type of information handled, interfaces to the systems, and special attention to national security systems.
- **Categorize risk level**—The publication outlines an approach to classify risk. It outlines how to map risk levels to computer systems and information. The risk drives what security to be applied.
- **Security controls**—The publication outlines what controls should be applied and when. It outlines how these controls are documented and approved. It is a risked-based approach giving some flexibility to the agency to tailor controls to meet their operational needs.
- **Risk assessment**—The standard defines and outlines the process to conduct risk assessments. Risk assessments are an essential part of a risk-based security approach. The risk assessment results drive the type of security controls to be applied.
- **System security plan**—The standards require a formal security plan for major systems and for the agency as a whole. The security plan serves as a roadmap. It is updated to keep current with threats and is an important part of the certification and accreditation process.
- **Certification and accreditation (C&A)**—This process occurs after the system is documented, controls tested, and risk assessment completed. It is required before going live with a major system. Once a system is certified and accredited, responsibility shifts to the agency to operate the system. This process is also referred to as the "security certification" process.
- **Continuous monitoring**—All certified and accredited systems must be continuously monitored. Monitoring includes looking at new threats, changes to the system, and how well the controls are working. Sometimes a system has so many changes that it must be recertified.

In support of FISMA, NIST developed the following publications:

- Federal Information Processing Standard (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems"
- NIST Special Publication 800-18, "Guide for Developing Security Plans for Federal Information Systems"
- NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems"

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST Special Publication 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View"
- NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"
- NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems"
- NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System"
- NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"

To comply with FISMA, the appointed inspector general of the agency performs a separate, annual evaluation. The evaluation first tests the value of the IT security policies, procedures, and practices. A subset of the information systems within the particular agency is tested. If no inspector general exists, an independent external auditor performs it. The external auditor submits the results to the Office of Management and Budget (OMB). The OMB is a cabinet-level office within the Executive Office of the President of the United States with oversight responsibilities. The OMB compiles the data from each agency. The OMB then prepares an annual report to Congress on compliance with the act.

At first, it appears only federal agencies need to worry about compliance, but this is not true. Federal agencies, for example, must care about their own systems as well as the systems of other contractors or organizations supporting the agencies. Any company or organization that expects to conduct business with the federal government needs to concern itself with FISMA.

The changes signed into law in 2014 authorize the Secretary of the Department of Homeland Security (DHS) to assist the OMB. In addition, the changes affect reporting and notification requirements. Agencies are required to provide timely notification of major security incidents to the OMB. Agencies also are required to provide much more specific information related to threats and compliance.

TIP

The annual reports submitted to Congress from the OMB concerning FISMA compliance are publicly available online. You can find them at FISMA FY2020 Annual Report to Congress (whitehouse.gov).

Red Flag Rules

The Red Flags Rule (RFR) was developed by the Federal Trade Commission with other agencies to establish a set of United States federal regulations that require financial firms and creditors to protect consumers from identity theft. The term red flag refers to having processes that look for suspicious indicator of identity theft and to "flag" those accounts for further review and verification of customer identity. These extra checks and supporting processes are referred to as the Red Flag Rules.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

An RFR program must include process to identify the red flags of identity theft that may occur in opening and accessing an account. For example, if a customer has to provide some form of identification that does not match their physical appearance or doesn't look genuine would be a "red flag." An RFR program:

- Should have policies and training to detect identify theft and red flags accounts.
- Should have clear process on how to respond to red flags.
- Must be updated regularly.

Cybersecurity Information Sharing Act

CISA was passed in October 2015. The law is considered significant as it provides legal boundaries for the sharing of sensitive **cybersecurity** information within and between the private and government sectors. The law solves a core problem that organizations are reluctant to share cybersecurity information that may expose them to civil or criminal liability, embarrassment, and loss of trust. This is especially true for companies that just suffered a cybersecurity data breach.

The objective of CISA is to improve cybersecurity in the United States through sharing of information about cybersecurity threats and breaches as well as for other purposes. The law authorizes private companies to share cybersecurity threat information for "cybersecurity purposes" with the federal government and with other private entities. A "cybersecurity purpose" is defined as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."

CISA contains four titles:

- Title I establishes a centralized mechanism for cybersecurity information sharing.
- Title II instructs DHS to take measures designed to strengthen cybersecurity in the federal government and at federal agencies as well as to facilitate the implementation of Title I.
- Title III calls for a cybersecurity-focused assessment of the federal workforce.
- Title IV provides for other measures intended to identify and address threats to critical information

Key components of the act are as follows:

- It limits the use of shared information by federal and state governments. The permissible purposes are to respond to, prevent, mitigate, investigate, or prosecute events that are considered a "threat of serious economic harm".
- It does not create a duty to share. CISA does not require private companies to share sensitive information. In fact, the act expressly prohibits the federal government from attempting to coerce sharing by withholding cybersecurity information or other benefits such as awarding government contracts.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

- It provides authorization to use defensive measures. CISA also authorizes private entities to use defensive measures to protect information systems and data. However, the CISA expressly prohibits private companies from attacking or "hacking back."
- Liability protections require sharing "in accordance" with CISA. To benefit from CISA's safe harbor from civil liability, antitrust, private entities' sharing activity must be "conducted in accordance" with CISA rules.
- Communications with regulatory authorities are permitted. Communication with regulators does not result in loss of CISA's liability protections.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002, also known as Sarbox or SOX, is a U.S. federal law. It is the result of the Public Company Account Reform and Investor Protection Act and Corporate Accountability and Responsibility Act. SOX dramatically changed how public companies do business.

The bill stems from the fraud and accounting debacles at companies such as Enron and WorldCom. Former President Bush characterized the act "as the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt." The act's primary purpose was to restore public confidence in the financial reporting of publicly traded companies. As a result, the act mandated many reforms to enhance corporate responsibility, enhance financial disclosures, and prevent fraud. SOX consists of the following 11 titles:

- **Title I, Public Company Accounting Oversight Board**—This title establishes the **Public Company Accounting Oversight Board (PCAOB)**. The PCAOB has several responsibilities, including overseeing public accounting firms, defining the process for compliance audits, and enforcing SOX compliance.
- **Title II, Auditor Independence**—This title establishes the conditions of services an auditor can perform while remaining independent. For example, a public accounting firm that performs external auditing services cannot provide financial information systems design or internal audit outsourcing services.
- **Title III, Corporate Responsibility**—This title requires the formation of audit committees. It also establishes the interactions between the committee and external auditors. Perhaps one of the more notable mandates of SOX is contained in Section 302, which requires the chief executive officer and the chief financial officer to take individual responsibility in certifying and approving the integrity of the company's financial reports.
- **Title IV, Enhanced Financial Disclosures**—This title addresses the accuracy and features of financial disclosures. For example, this title specifically addresses and prevents what Enron did, such as selling liabilities on its balance sheet as assets to special purpose entities. This title also contains the controversial Section 404, which requires companies to report the adequacy of their internal controls.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

- **Title V, Analyst Conflicts of Interest**—This title fosters public confidence in securities research and defines code of conducts between firms.
- **Title VI, Commission Resources and Authority**—This title provides greater authority to the SEC to fault or bar a securities professional from practice. This title also addresses the prevention of fraud schemes involving low-volume, low-price stocks.
- **Title VII, Studies and Reports**—This title requires the comptroller general and the SEC to conduct studies and report their findings. Examples include studying the effects of the consolidation of public accounting firms as well as studying previous corporate fraud and accounting scandals.
- **Title VIII, Corporate and Criminal Fraud Accountability**—This title provides the ramifications for corporate fraud and addresses the destruction of corporate audit records. This is a direct response to the auditing firm, Arthur Andersen, which shredded documents.
- **Title IX, White Collar Crime Penalty Enhancement**—This title reviews the rules and penalties regarding white-collar criminal offenses.
- **Title X, Corporate Tax Returns**—This title simply states that the CEO should sign the company tax return.
- **Title XI, Corporate Fraud Accountability**—Also known as the Corporate Fraud Accountability Act of 2002, this title provides additional guidelines regarding the consequences of corporate fraud. It also provides the SEC with the authority to freeze the funds of companies suspected of violating laws.

SOX is quite large and contains many reforms to rally public confidence. It also improves corporate accountability and helps to avoid corporate fraud and dishonesty. Two sections receive much of the attention, especially of IT. The first is Section 302, "Corporate Responsibility for Financial Reports." The second is Section 404, "Management Assessment of Internal Controls." These two sections place vast constraints on IT security. Although neither section mentions IT or IT security, financial accounting systems rely heavily on IT infrastructure. Thus, it has strongly driven the subject of IT security into the boardroom.

Section 302 requires the CEO and CFO to personally certify the truthfulness and accuracy of financial reports. They start and make internal controls. Then, they must assess and report upon the internal controls around financial reporting every quarter. Section 404 goes a step further. Section 404 requires the company to provide proof. Again, they must assess the effectiveness of their internal controls, which a public accounting firm must audit and attest. They then publish this information in the company's annual report.

SOX is lengthy and is specific in many areas—for example, criminal penalties for noncompliance. It still is very high level and leaves a lot of room for interpretation, especially concerning IT controls. SOX does not directly address IT control requirements. As a result, you need to become familiar with a couple of publications. These include the auditing standards created by the PCAOB and the SEC's release on management guidance—17

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

CFR Part 241. In this codification, the SEC issued further interpretation and guidance regarding Section 404. It provides "an approach by which management can conduct a top-down, risk-based evaluation of internal control over financial reporting." PCAOB also made a formal process to further define the criteria within Section 404. This process became Auditing Standard No. 2. This standard is now superseded by Auditing Standard No. 5, "An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements." Some notable changes to provide greater clarity and a more prescriptive approach include the following four areas:

- Aligning Auditing Standard No. 5 with the SEC's management guidance, mostly with regard to prescriptive requirements and definitions
- Adjusting the audit to account for the particular circumstances regarding the different sizes and complexities of companies
- Encouraging auditors to use professional judgment, particularly in using a risk-assessment methodology
- Following a principles-based approach to determining when and to what extent the auditor can use the work of others to obtain evidence about the design and effectiveness of the control

The standard also states that the auditor should use the "same suitable, recognized control framework" as the management of the company they are auditing. Furthermore, it even goes as far to suggest a suitable framework. That framework is the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

Gramm-Leach-Bliley Act

Also known as the Financial Modernization Act of 1999, the **Gramm-Leach-Bliley Act (GLBA)** repeals parts of the Glass-Steagall Act from 1933. The Glass-Steagall Act prohibited banks from offering investment, commercial banking, and insurance services all under a single umbrella. GLBA deregulates the split of commercial and investment banking. GLBA also provides provisions for compliance within Sections 501 and 521 to protect the financial information held by the industry. This protection is on behalf of the consumers. GLBA generally applies to financial institutions or any organization "significantly engaged" in financial activities. Examples include banks and securities firms. More examples are firms dealing with mortgages, insurance, tax preparation, debt collection, and much more. The FTC maintains and enforces GLBA.

To protect personally identifiable information, GLBA divides privacy requirements into three principal parts:

- **Financial Privacy Rule**—The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information.
- **Safeguards Rule**—The Safeguards Rule requires financial institutions to develop, maintain, and implement policies. These policies should tell how they will protect customer information.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Pretexting

Pretexting is a method of social engineering. It is more about human interaction than about technology. For pretexting to succeed, you must manipulate others to divulge sensitive information. The root of pretexting is pretext or a situation or reason that is deceptive or false. For example, investigators often use pretexting—at least in the movies! It typically involves some type of con or clever ruse.

Consider, for example, how to guess a password. You might use some programmatic mechanism to guess a password. Now consider how much easier it is to ask someone for the password, presumably under a pretext. This is one example of why companies so often reiterate that they will never ask you for your password. A famous recent example involved Hewlett-Packard (HP). At the time, contracted private investigators determined the source of an information leak. To do so, the investigators operated under a pretext. They impersonated HP board members or journalists from popular news outlets to obtain phone records.

There are countless examples of why pretexting occurs. The GLBA pretexting provision protects consumers from evildoers trying to obtain personal financial information under false pretenses. Identity theft is the greatest risk to consumers should their information be compromised.

- **Pretexting provisions**—The pretexting provisions protect consumers. This protection is from both individuals and organizations that obtain personal financial information under false pretenses.

The Financial Privacy Rule requires financial institutions to provide notices to their customers. The notices explain their privacy policies, specifically covering the information collection and sharing practices of the company. Consumers are also given control over 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 given events and changes in the firm's operations.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

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 its customers.
- Use forged, counterfeit, lost, or stolen documents to obtain customer information from the financial institution or 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 the 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 healthcare. 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:

- 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

Given the sensitive nature of one's personal health records, this regulation is usually taken very seriously and affects the following:

- Health care providers—Doctors, hospitals, clinics, and so on
- Heath plans—Those that pay the cost for the medical care such as insurance companies
- Health care clearinghouse—Those that process and facilitate billing

The last major update to the HIPAA rules was the HIPAA Omnibus Rule changes in 2013. While the fundamental requirements (referred to as *Safeguards*) in the act did not change, a number of details within each of the title's requirements under fine tuning:

- Performing a gap analysis to determine what policies and procedures must be revisited in light of the Omnibus Rules
- Revising privacy and security policies and procedures
- Revising breach notification policies, procedure
- Amending notices of privacy practices based on the new rules

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

- Enhancing training of the workforce and promoting more ongoing awareness
- Ensuring end-user training on proper handling of data is performed prior to granting access
- Updating risk analysis to reflect vulnerabilities such as mobile devices

Much of the focus around HIPAA is within the first two titles. Title I offers protection of health insurance coverage without regard to preexisting 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

⚠ WARNING

Several proposed changes in HIPAA are expected in 2022 and beyond. One of the changes would increase the right to access health information for individuals, known as the Right of Access. This would include information stored electronically. During the pandemic, many caregivers could not access medical information for older adults in their families. This was particularly challenging during medical emergencies.

As a result, the HHS has provided five rules regarding Title II of HIPAA. These rules 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 the 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

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

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.

Physical safeguards include the policies, procedures, and physical controls put in place. These controls and documentation protect the information systems and physical

TABLE 2-1 HIPAA administrative safeguards and implementation specifications.

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

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

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.

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.

TABLE 2-2 HIPAA physical safeguards and implementation specifications.

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

TABLE 2-3 HIPAA technical safeguards and implementation specifications.

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

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

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 U.S. First Amendment because 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 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," which means having technology in place that blocks or filters Internet access that is either obscene, harmful to minors, or represents child pornography. This requirement includes implementing a safety policy and controls that address the following:

- Access by minors to "inappropriate matter" on the Internet
- The safety and security of minors when using electronic communication such as email, chat rooms, and instant messaging
- Unauthorized access and unlawful activities by minors
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures restricting minors' access to harmful materials

Before implementing the policy and controls, however, the law also requires schools or libraries to first provide public notice and to hold a public hearing to address the proposed Internet safety policy.

You might have noticed that the term *inappropriate matter* could be considered vague and controversial. As a result, the act is clear in stating that the government may not establish the criteria for making such a determination. The act states that the determination is made at the local level by the school board, local educational agency, or library.

Finally, schools and libraries must comply with one more step before they can receive the E-Rate. They must certify they have an Internet safety policy in place meeting the preceding requirements. Noncompliance with the law occurs if there is a failure to submit for certification. In this case, the institution will not be eligible for services at a discounted rate. In addition, failure to ensure the use of the computers in accordance with a certification will be required to reimburse all funds and discounts for the certification period.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Children's Online Privacy Protection Act

Like CIPA, the **Children's Online Privacy Protection Act (COPPA)** is a U.S. federal law designed to protect children. COPPA is maintained and enforced by the FTC. COPPA requires websites and other online services aimed at children less than 13 years of age to comply with specific requirements of the law.

In 2013, the FTC implemented new provisions that provide additional protections to keep pace with the changes in technology. The FTC also introduced a six-step plan to understand if an organization is required to comply with COPPA, and if so, how to be compliant. The six steps are as follows:

1. Determine if your company is a website or online service that collects personal information from children under 13.
2. Post a privacy policy that complies with COPPA.
3. Notify parents directly before collecting personal information from their children.
4. Get parents' verifiable consent before collecting information from their children.
5. Honor parents' ongoing rights with respect to information collected from their children.
6. Implement exceptions to COPPA's verifiable parental consent requirement.

With Step 1, an organization will likely need to consult the law and to understand precisely how terms are defined. For example, what does it mean to *collect*, or what exactly is considered *personal information*? Online services are obliged to comply with COPPA if asking for information that would even imply a child is less than 13 years of age—for example, "Do you now attend elementary school?"

After it is determined that COPPA applies, the next step requires the creation of a privacy policy. COPPA requires that the privacy policy list all operators who are collecting information. In addition, it must list an operator who will respond to any and all queries from parents. Next, the privacy policy must contain a complete description of the personal information that is collected and for what purposes. Finally, the policy must state the rights afforded to parents. For example, this must include a notice that parents have the right to review the information collected on their child and even provide direction that the collected data be deleted.

Except under limited classes of information, COPPA requires that parents be notified before data is collected from their children. The rule provides for very specific requirements that must be met with regard to such notice. Once notification requirements are met in Step 3, Step 4 requires verifiable consent. While the means of providing such consent is left up to the requesting organization, the rule does provide several examples of acceptable methods. One simple example is a signed consent form via fax, mail, or electronic scan. Another is the entry of a credit or debit card number when coupled with a financial transaction.

The final two steps require continual obligations upon the entity complying with COPPA. With Step 5, parents may ask to review, revoke, or delete the child's

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

information at any time. Such requests must be honored by the complying organization. At the same time, the organization must take necessary precautions, such as taking reasonable measures to ensure that parents are in fact who they say they are. The final step provides rules around the need to protect the confidentiality and integrity of the information collected as well as ensure that adequate retention and disposal practices are maintained.

California Consumer Privacy Act

The number of state laws related to cybersecurity are too numerous to outline. The emerging laws tend to focus on privacy and contain many of the core principles found in the California Consumers Privacy Act (CCPA), which was implemented in January 2020.

The law allows consumers the right to find out who has access to their personal data. Consumers can stop data from being sold or transferred to third parties through an opt-out function that must be prominently posted or request that companies delete their data.

Table 2-4 outlines key concepts embedded in the CCPA and many states' privacy laws:

The CCPA was one of the first state laws to significantly expand the definition of personal information. The law recognized the increased importance and impact on an individual's personal identity over the Internet. The CCPA's list of data elements that constitute "personal information" includes the following:

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers
- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
- Biometric information such as fingerprints, facial recognition files
- Internet or other electronic network activity information, including, but not limited to browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
- Geolocation data
- Audio, voiceprints, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information, defined as information that is not publicly available as defined in the **Family Educational Rights and Privacy Act (FERPA)** (20 U.S.C. §1232g, 34 C.F.R. Part 99) which protects education records and the student's

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

TABLE 2-4 Key privacy concepts.

CONCEPT	OBJECTIVE
Full disclosure	The idea is that an individual should know what information about them is being collected. They should be told how that information is being used.
Limited use of personal data	The idea is that only the data needed for the transaction should be collected. Do not collect more information than you need to provide the product or service.
Opt-in/opt-out	The practice of asking permission on how personal information can be used beyond its original purpose, such as a real-estate company asking permission of someone who sold their home if their information can be shared with a moving company. The difference between opting in and opting out generally refers to clicking a box on a webpage. In an opt-in process, unless the consumer clicks the "Yes" box, no additional service is offered. In an opt-out process, consumers are automatically enrolled in a service unless they click the "No" box or deselect the "Yes" box.
Data privacy	Expectations on how your personal information should be protected and limits place on how the data should be shared.
Informed consent	The idea that you are of legal age, capable, have the needed facts, and absent undue pressure can make an informed judgment.
Public interest	The idea is that an organization has an obligation to the general public beyond its self-interest. Although a vague term, it's not unusual for regulators to look at the impact a company has on the industry or the economy in general.

identification including disclosure of ay part of the student's Social Security number.

- Inferences are drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, or the like

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard that describes how to protect credit card information. If you accept Visa, MasterCard, or American Express, you are required to follow PCI DSS. These card companies formed the **Payment Card Industry Security Standards Council (PCI SSC)** to create the standard. The Payment Card Industry (PCI) Data Security Standard (DSS) was released in 2006. The standard applies to everyone who stores, processes, or exchanges cardholder information.

The standard requires an organization to have specific PCI DSS security policies and controls in place. The organization must also have these controls validated. If you are a small merchant, you can perform a self-assessment questionnaire. Large-volume merchants must obtain their validation through a **Qualified Security Assessor (QSA)**. Failing to validate, or failing the validation, can result in fines from the credit card companies. In extreme cases of noncompliance, you may be prevented from handling credit cards. Taking credit cards away could put you out of business.

The PCI DSS is an information security framework, so it has lots of technical requirements. Two, in particular, have been a challenge for organizations to implement: network segmentation and encryption. PCI strongly encourages isolating credit card systems at a network layer. For many open network designs and shared systems, this is a challenge. Without network segmentation, the standard talks about the need that all systems on that segment to be brought up to PCI DSS level standards. This could also be expensive. The second major challenge is encrypting data at rest. As discussed in previous chapters, encrypting data in transit is common over the Internet and public networks. Encrypting data at rest, however, can be technically challenging and at times not feasible.

There are six control objectives within the PCI DSS standard. To be compliant, you need to include these control objectives in your security policies and controls:

- Build and maintain a secure network—Refers to having specific firewall, system password, and other security network layer controls.
- Protect cardholder data—Specifies how cardholder data are stored and protected. Also sets rules on the encryption of the data.
- Maintain a vulnerability management program—Specifies how to maintain secure systems and applications, including the required use of antivirus software.
- Implement strong access control measures—Refers to restricting access to cardholder data on a need-to-know basis. It requires physical controls are in place and requires individuals to have unique IDs when accessing cardholder data.
- Regularly monitor and test networks—Requires access to cardholder data be monitored. Also requires periodic penetration testing of the network.
- Maintain an information security policy—Requires that security policies reflect the PCI DSS requirements. Requires these policies be kept current and an awareness program be implemented.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

FYI

Compliance with PCI DSS is required for merchants and credit card processors. Enforcement of the PCI DSS requirements is through contractual obligations. Noncompliance can result in a merchant not being allowed to accept credit cards. The PCI Security Standards Council also provides guidance for software developers of payment application systems to ensure products used to accept credit card payments are secure.

PCI DSS is unlike most regulatory laws in one way. It is very specific with regard to requirements and expectations. The requirements generally follow security best practices and use the 12 high-level requirements, aligned across six goals, as shown in **Table 2-5.** Each requirement listed in the table consists of various subrequirements. Also

TABLE 2-5 Goals and high-level requirements for PCI DSS.

GOALS	HIGH-LEVEL REQUIREMENTS
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data.	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a vulnerability management program.	5. Use and regularly update antivirus software or programs. 6. Develop and maintain secure systems and applications.
Implement strong access control measures.	7. Restrict access to cardholder data on a need-to-know basis. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly monitor and test networks.	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an information security policy.	12. Maintain a policy that addresses information security for employees and contractors.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

included are procedures for testing. These must be documented as either being in place or not in place.

Consider requirement 8, for example. It requires a unique ID to be assigned to each person with computer access. Within the security standard, this requirement consists of 21 subrequirements. Many of them are very specific:

- Incorporate two-factor authentication for remote access.
- Set first-time passwords to a unique value and change immediately after first use.
- Remove or disable inactive accounts at least every 90 days.
- Require a minimum password length of at least seven characters.

Since PCI DSS started, the Security Council periodically releases supplemental documents. These documents can be found on the Security Council website at https://www.pcisecuritystandards.org/minisite/en/pci-dss-v3-0.php.



CHAPTER SUMMARY

A common truth is that these laws recognize the power of information. The more personal the data, the more powerful the information. The power comes from the impact that personal information has on our lives. With the power of personal information comes the ability to influence everything from buying choices to political beliefs. It influences what type job we can have, car we drive, home we live, and it determines the quality of medical care we receive. The misuse and abuse of this information is equally powerful to make our lives miserable. Stealing a person's identity is a major problem. It can take years of effort to restore your credit. We've all hear stories of millions of credit cards stolen each year. While slow to react, the government does respond to these headlines and public pressure. Although compliance with regulations can touch many different groups within an organization, IT departments are increasingly discovering they need to stay abreast of the latest regulations as IT continues to be pervasive throughout organizations. It might seem overwhelming to keep up with the requirements of all the existing regulations, not to mention new ones. However, sound governance, risk-management, and compliance program within organizations using a well-defined framework can make the process much more efficient and effective.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

KEY CONCEPTS AND TERMS

Acts of Congress
Availability
Certification and accreditation (C&A)
Children's Internet Protection Act (CIPA)
Children's Online Privacy Protection Act (COPPA)
Confidentiality
Cybersecurity
E-Government Act of 2002
Family Educational Rights and Privacy Act (FERPA)
Federal Information Security Management Act of 2002 (FISMA)
Gramm-Leach-Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
Integrity
National Institute of Standards and Technology (NIST)
Payment Card Industry Data Security Standards (PCI DSS)
Pretexting
Protected health information (PHI)
Public Company Accounting Oversight Board (PCAOB)
Qualified Security Assessor (QSA)
Regulatory agencies

CHAPTER 2 ASSESSMENT

1. Which of the following acknowledges the importance of sound information security practices and controls in the interest of national security?

A. FISMA
B. GLBA
C. HIPAA
D. FACTA
E. FERPA

2. What organization was tasked to develop standards to apply to federal information systems using a risk-based approach?

A. Public Entity Risk Institute
B. International Organization for Standardization
C. National Institute of Standards and Technology
D. International Standards Organization
E. American National Standards Institute

3. Pretexting is a technical method of intercepting passwords embedded in text messages.

A. True
B. False

4. Which of the following organizations was tasked to develop and prescribe standards and guidelines that apply to federal information systems?

A. NIST
B. FISMA
C. Congress
D. PCI SSC
E. U.S. Department of the Navy

5. What section of SOX requires management and the external auditor to report on the accuracy of internal controls over financial reporting?

A. Section 301
B. Section 404
C. Section 802
D. Section 1107

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

6. SOX explicitly addresses the IT security controls required to ensure accurate financial reporting.

A. True
B. False

7. Which of the following was established to have oversight of public accounting firms and is responsible for defining the process of SOX compliance audits?

A. COSO
B. Enron
C. PCAOB
D. Sarbanes-Oxley
E. None of the above

8. Which of the following is *not* one of the titles within SOX?

A. Corporate Responsibility
B. Enhanced Financial Disclosures
C. Analyst Conflicts of Interest
D. Studies and Reports
E. Auditor Conflicts of Interest

9. Which one of the following is *not* considered a principal part of the GLBA?

A. Financial Privacy Rule
B. Pretexting provisions
C. Safeguards Rule
D. Information Security Rule

10. Which regulatory department is responsible for the enforcement of HIPAA laws?

A. HHS
B. FDA
C. U.S Department of Agriculture
D. U.S. EPA
E. FTC

11. Which one of the following is *not* one of the safeguards provided within the HIPAA Security Rule?

A. Administrative
B. Operational
C. Technical
D. Physical

12. In accordance with CIPA, who determines what is considered inappropriate material?

A. FCC
B. U.S. Department of Education
C. The local communities
D. U.S. Department of the Interior Library
E. State governments

13. The Family Educational Rights and Privacy Act prohibits the use of Social Security numbers as directory information, even the use of the just the last four digits of a SSN.

A. True
B. False

14. PCI DSS is a legislative act enacted by Congress to ensure that merchants meet baseline security requirements for how they store, process, and transmit payment card data.

A. True
B. False

15. To comply with the Red Flags Rule, financial institutions and creditors must do which of the following?

A. Identify red flags for covered accounts.
B. Detect red flags.
C. Respond to detected red flags.
D. Update the program periodically.
E. All of the above
F. Answers B and C only

16. Having a photograph or physical description on an identification that is not consistent with the applicant or consumer presenting the identification is an example of what type of red flag category?

A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.
B. The presentation of suspicious documents
C. The presentation of suspicious personal identifying information
D. The unusual use of or other suspicious activity related to a covered account

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

17. Regulatory compliance laws do *not* exist at what different level?

A. Local
B. State
C. Federal
D. International.

18. The Family Educational Rights and Privacy Act (FERPA) of 1974 is a U.S. federal law that protects the privacy of student education records and allows parents certain access rights to the student's educational records, even when a student turns 18 and attends college.

A. True
B. False

19. Which of the following does *not* deal with the HIPAA administrative safeguard of the security management process?

A. Risk analysis and management
B. Sanction policy
C. Facility security plan
D. Information system activity review

20. Which of the following does *not* deal with the addressable HIPAA administrative safeguard of workforce security?

A. Authorization and/or supervision
B. Workforce clearance procedure
C. Termination procedures
D. Contingency operations
E. This law attempts to limit children's exposure to sexual material.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.

© Jones & Bartlett Learning LLC, an Ascend Learning Company. NOT FOR SALE OR DISTRIBUTION.