and procedures cannot be quantified, but the financial impact of the incident certainly can.

Privacy

An individual's right to general privacy is protected by the Fourth Amendment to the US Constitution. More specifically, individuals' right to privacy of their health information is protected by HIPAA and the modifications to HIPAA made via the HITECH Act, along with later amendments. These laws are the most significant and comprehensive legal protections that exist for health information generally, and electronic health information specifically. The laws have multiple accompanying rules; two notable for this discussion are the Privacy Rule and the Security Rule. Detailed summaries and current information about these rules are available at www.hhs.gov.

The HIPAA Privacy Rule, enforceable for all entities since 2004, is binding on any healthcare provider, health plan, or covered entity that transmits health information electronically. The Privacy Rule ensures protection of individual health records through national standards and governs disclosure and use of the information. The Privacy Rule references personal health information (PHI), sometimes described as "protected health information," which is defined as "individually identifiable health information held or transmitted . . . in any form or media, whether electronic, paper, or oral" (OCR 2003). Electronic PHI is referred to by some sources as ePHI. The OCR, which oversees HIPAA enforcement, holds healthcare organizations accountable for protecting PHI under penalty of financial fines and loss of access to federally funded insurance programs, such as Medicare and Medicaid (OCR 2003).

Despite the significant burden engendered by HIPAA rules, notably with regard to the Privacy Rule, few changes were made between 2013 and 2019. One example of burdensome administrative requirements is that organizations must obtain written confirmation from patients that they were given a copy of the organization's privacy practices. Only limited changes are under consideration in 2019, with a focus on regulations that hinder efforts to provide coordinated care across multiple organizations (*HIPAA Journal* 2019a; *HIPAA Journal* 2019b), such as requirements for patient authorization to release PHI to a transfer entity.

The Security Rule supports the Privacy Rule by defining technical and nontechnical standards for archiving or electronic transfer of PHI. The intent of these rules is to allow entities some flexibility in designing policies and procedures to create, store, receive, and transmit PHI electronically, but to safeguard against inadvertent disclosure or unauthorized access to PHI in storage or during transfer. Because a significant proportion of the data maintained by a healthcare enterprise is classed as PHI, compliance with these security regulations is not a trivial matter. The rule requires that organizations address security issues with administrative, physical, and technical

safeguards; with policies and procedures; and by management of contractual business relationships.

Current issues that might drive future changes to the Security Rule include efforts to increase national system interoperability and reduce information blocking by covered entities through rules proposed by CMS and ONC in 2019. Because laws and regulations are subject to change, the practice community regularly verifies current requirements at authoritative websites such as www.hhs.gov and www.cms.gov.

Physical Security

Simply speaking, security in this context means to protect information resources—personnel, hardware, communication devices, and so on—from harm, theft, destruction, or other compromise of the integrity of data or infrastructure. Protecting the physical security of the enterprise information system requires a portfolio of approaches that range from management policies (such as specifying an individual's system access rights) to hardwired security features (such as a fire wall) to physical measures such as requiring a code or passkey to enter an off-site server facility. Ensuring the physical security of data and information system components is essential for compliance with regulatory and legal requirements in addition to the need to safeguard access to the information that flows through the system.

Physical security of health information and technology resources arguably was easier before the connectivity era. Paper records could be stored in locked file cabinets in a locked room with access control. The computer room could be locked and accessible only to HIT personnel and authorized administrators. Early secondary storage media increased the security risk only slightly, as centralized storage areas could be protected with similar approaches. The strategic management approach at this time consisted of well-defined policies to guide operational practices, coupled with consistent monitoring and stringent enforcement of the policies.

In today's computing environment, the sheer volume of computing devices distributed across the enterprise, portable storage options, mobile device access, number of authorized users, and many other variables converge to make physical security a complex challenge at best. However, well-defined policies, consistent monitoring, and policy enforcement remain pivotal success tactics.

Many healthcare organizations have a high-level position titled chief information security officer (CISO) or something similar. This individual is responsible for developing and enforcing policies and practices to anticipate and mitigate risks to the security of the information system in its entirety—the physical components, the information in the system, strategic relationships, and so on—as well as ensuring compliance with security regulations germane to the enterprise. In addition to regulatory compliance and physical protection, the CISO must be prepared to safeguard against financial and reputational threats to the enterprise resulting from HIT or data security incidents.

The Administrative Safeguards provisions of the HIPAA Security Rule mandate specific security measures, generally implemented across the enterprise as policies and procedures. The categories of requirements include the following (Snell 2015):

- Security management processes—includes risk management and risk analysis
- Assigned responsibility for security—is typically a designated CISO
- Workforce security—ensures access for job performance; removes access from terminated employees
- Management of information access—ensures access on a need-to-know basis
- Security awareness and training—ensures compliance with policies and procedures
- Security incident procedures—reports structure; manages response
- Contingency plans—prepares for disaster; develops backup and recovery procedures
- Evaluation—monitors to adjust to environmental or operational changes that affect security
- Business associate contacts and other arrangements—is similar to business associate agreements related to Privacy Rule, but specific to ePHI

Managing information security requires a team of skilled personnel who work together to manage all facets of the security conundrum, and who are committed to monitoring changes in regulations and industry best practices. These individuals collectively need knowledge and experience in the technical aspect of HIT security, current privacy and security regulations and compliance requirements, interpersonal and communication skills, and data management skills.

Cybersecurity

Cybersecurity, or protection of internet-connected information systems, poses complex and pervasive challenges to protecting the information resources of an enterprise, not the least of which is the dynamic nature of the threats. Much like biological viruses, computer viruses and other forms of cyberattacks mutate and evolve to avoid destruction from approaches deployed by organizations to protect the security and integrity of an information system. All connected elements of the system, from an employee smartwatch that autodownloads email from an external vendor to a cloud network that hosts a large data warehouse (and everything in between), are vulnerable to cyberattack. Thus, all elements of the system, and all nonenterprise devices that connect, must be considered in designing security protocols to protect the enterprise information resources.

End-point devices, including employees' personal devices such as laptops, tablets, and smartphones or smartwatches, can put an enterprise information system at risk without any deliberate intent on the part of the user.

Cyberthreats and cybersecurity incidents receive immediate media attention and often are reported in the news in an inflammatory style. Sometimes, a very important aspect of the CISO's job is managing the public perception that information privacy and the security of that information is a top priority of the healthcare enterprise. In the aftermath of a security incident, it is important for the CISO, the enterprise CEO, and other top administrators to be coached by communications and legal experts in managing public statements and responses to public inquiries. The focus must remain on mitigating patient harm first, then organizational harm second.

Monitoring cyberthreat activity is important. Most CISOs and their staffs participate in professional networks and have trusted information websites or other sources to stay abreast of recent and emerging threats and how other organizations are responding to those threats. Accessing this type of information is a critical tool, along with managing system and network updates, monitoring network activity for aberrant access, and employing security approaches such as antimalware and antivirus software.

Cyberhygiene, adherence to good security practices for internet-connected components, can help protect devices from outside attack. Regular device and system monitoring and maintenance activities should be procedural, and oversight should be specifically assigned to accountable personnel. Minimal hygiene factors include the following:

- Maintain documentation of current system components and connections
- Ensure backup of critical data to secure but accessible storage, ideally off-line
- Designate storage options by data type (e.g., sensitive, clinical, research, business) to ensure coverage by appropriate security protocols
- Maintain current versions of antivirus and antimalware software
- Maintain current updates of software to ensure currency of security elements
- Enforce policy for regular strong password changes
- Limit access and user rights to system components on need-to-know basis

Many organizations have migrated to two-factor authentication (2FA), which requires entering a strong password and a second code provided by SMS text or a security token to access a system. While many users consider this inconvenient and inefficient, it is a strong deterrent to unauthorized access. In a survey of more than 1,300 senior healthcare executives, more

than 25 percent of respondents said they had been victims of a cyberattack, with losses exceeding $1 million for 70 percent of the organizations. About half of the executives responded to the incident by implementing 2FA to control remote access (Donovan 2018b).

Internet of Things

In 2017, the Information Security Forum, a nonprofit organization that produces research data on information security and risk management, released a report on the threat horizon through 2019. The report suggests that "cybercriminals will increasingly focus their ransomware efforts on smart devices connected to the Internet of Things (IoT)" (Olavsrud 2017)—and they rank this problem among their top nine. Ransomware, a malicious software, encrypts a computer or computing system to deny access or control by the owner until a ransom is paid. The virus often attacks the system through a phishing email, a bogus message that seeks to gain user information to access desired systems such as financial or healthcare data repositories, or infected websites.

Beazley Breach Response Services, a specialist insurer, reported that healthcare is the field most targeted for ransomware attacks. In fact, ransomware accounted for 47 percent of their 2018 data breach claims (Beazley 2018). After ransomware, accidental disclosure was the second most common source of breaches at 20 percent. In addition to an increased number of data breach claims filed with Beazley relative to 2017 numbers, the ransom amount demands have increased, as high as $2.8 million. Ransomware attacks can be even more challenging because of issues in the malware itself or unskilled hackers. Either may result in fatal corruption of compromised data or an inability to decrypt data despite payment of the ransom. In many cases, backups have been compromised before the primary data were captured by the attackers; thus, the ransom demand has added power.

The *Internet of Things* is the entirety of devices and objects with unique identifiers that transmit data over the internet without an intermediary person or device. Based on machine-to-machine communication principles, the IoT is a network of smart devices, including medical devices, numbering in the billions. Some estimates suggest IoT growth will exceed 75 billion devices by 2025, powered by 5G mobile technology (Statista Research Department 2020). Device examples include sensors implanted in the body that transmit biomedical data such as glucose levels or heart rate, smart home applications such as automated temperature control, and geolocation chips in animals. IoT attacks are a major risk, as security is not robust on many devices, and exploiting one vulnerability engenders access to data produced by many other devices, including the types of personally identifiable data that cybercriminals seek. As "wearables" and other real-time data-capturing devices become more pervasive in healthcare, and more organizations adopt mHealth as a service delivery approach, security risks associated with the IoT will become higher priority.

Health Information Technology Legislation and Regulations

In addition to ongoing and pervasive amendments to HIPAA and related legislation, notably laws that apply to Medicare, several other laws are notable for their impact on HIT. Exhibit 5.3 provides a summary of legislative intent and key provisions of selected laws that mandate HIT practices. As discussed previously, compliance with evolving regulations and reporting requirements is a complex, challenging, and dynamic responsibility for all healthcare organizations. Monitoring legislative and regulatory updates should be the purview of a team of skilled staff.

EXHIBIT 5.3 Summary of Key Legislation

Law	Intent	Additional Information Source
Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191	Improve portability and continuity of health insurance coverage; combat waste, fraud, and abuse; regulate privacy and security	www.hhs.gov/hipaa/index.html
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009	Promote HIT, including EHRs and health information exchange	www.healthit.gov/hitac/committees/health-information-technology-advisory-committee-hitac
Food and Drug Administration Safety and Innovation Act (FDASIA) of 2012 (Section 618)	Set risk-based regulatory framework for HIT, including mobile applications	www.healthit.gov/sites/default/files/fdasiahealthitreport_final.pdf
Patient Protection and Affordable Care Act (ACA) of 2010, P.L. 111-148	Simplify administrative processes; establish operating rules for transactions; provide unique identifiers for health plans; set standards for electronic funds transfer and claims attachments	www.healthcare.gov/glossary/patient-protection-and-affordable-care-act/
Medicare Access and CHIP Reauthorization Act (MACRA) of 2015	Change physician payment models and provide funding for technical assistance	https://qpp.cms.gov/
21st Century Cures Act of 2018, P.L. 114-255	Amend HITECH Act; clarify HIPAA Privacy Rule; advance interoperability; promote medical product development	www.congress.gov/bill/114th-congress/house-bill/6

Summary

A robust HIT infrastructure, which comprises all components of an enterprise's IT resources—physical elements, software, policies, and contractual relationships—is complex, dynamic, and essential to a healthcare organization's survival. Technology supporting the clinical environment of the hospital has evolved such that the notion of the "state of the art" is a moving target as advancements and innovations accelerate. The business environment, with its changing payment models and shifting power relationships, requires organizations to be nimble and able to respond quickly to achieve financial incentives and avoid penalties. The need to exchange information with business partners, payers, patients, and other providers compel organizations to strive to achieve the full system interoperability goal set by the federal government.

The healthcare environment is a complex configuration of opportunities to provide high-quality patient care with available technologies, coupled with extensive risks inherent in using those same technologies. The concept of opportunity versus risk can also be applied to IT. The convenience of digital and wireless technologies has increased the complexity of managing the physical security of information resources and the information itself. Arguably, the greatest challenge to ensuring security and privacy of health information is protecting against malicious, invasive attacks by individuals or groups for personal financial gain or notoriety.

Leaders, managers, and HIT professionals will be challenged to design, maintain, and protect the organization's information resources in a volatile environment—one that is constantly changing as a result of technology advancement, regulatory expansion, and constrained business models. Building and supporting a team with the needed skill mix, who are guided by a good strategic plan and governance framework, will be key success factors.

Web Resources

A number of organizations (through their websites) provide more information on the topics discussed in this chapter:

- The American Health Information Management Association (www.ahima.org) was established in 1928. AHIMA is the recognized leadership and advocacy group for health information professionals, promoting the "advancement and use of health data and information for the delivery of quality healthcare worldwide."

- The American National Standards Institute (www.ansi.org) serves as "the voice of the U.S. Standards and conformity assessment system." ANSI "oversees creating, promulgation, and use" of standards in many fields, including healthcare.
- Centers for Medicare & Medicaid Services (www.cms.gov) is an agency of the HHS that administers Medicare and other federally funded health programs. This federal government website available to the public provides extensive information about the agency, regulations, guidance, and research data, among other topics.
- The Cybersecurity and Infrastructure Security Agency (www.us-cert.gov) is an official website of the Department of Homeland Security. It was authorized by the Cybersecurity and Infrastructure Security Agency Act of 2018 to provide cybersecurity and infrastructure-security knowledge and practices to enable risk management and protect the nation's information resources. Specific priorities include federal network protection, cyberprotection, infrastructure resilience, and emergency communications.
- The HHS maintains a public-facing government website, www.hhs.gov, that provides information on laws and regulations in addition to HHS programs and services. An extensive index is available to aid searches.
- The National Information Standards Organization (www.niso.org) is a US-based, nonprofit standards organization accredited by ANSI that "identifies, develops, maintains, and publishes technical standards to manage information in today's continually changing digital environment."
- OASIS (www.oasis-open.org) functions as a nonprofit consortium whose goal is to drive "development, convergence and adoption of open standards for the global information society."
- The Office of the National Coordinator for Health Information Technology (www.healthit.gov) exists to support the adoption of HIT and nationwide health information exchange to improve healthcare.
- Health Level Seven (HL7) (www.hl7.org) is a leading healthcare standard-developing organization. HL7 is working as a coordinating agent for various active standard-setting groups.

Discussion Questions

1. Differentiate between primary and secondary data storage, providing examples.

2. Suggest how the use of a patient ID bracelet containing a bar code representation of the patient's ID and a bar code scanner can lead to improved quality of care in a hospital.
3. Distinguish between an interfaced system and an integrated system. Provide some examples in which one model would provide an advantage over the other.
4. Describe some important applications of electronic data interchange in the healthcare field.
5. How does mobile computing differ from wireless communication?
6. How do data standards organizations contribute to quality of healthcare?
7. Why is the Internet of Things considered an extreme security risk to personal health information?
8. Define cybersecurity and discuss system vulnerabilities that pose threats.
9. What is the purpose of a data governance plan?
10. Differentiate the requirements posed by the HIPAA Privacy Rule and HIPAA Security Rule.
11. Discuss barriers to achieving full interoperability in HIT data sharing.

References

Beazley. 2018. "Beazley Breach Insights October 2018." Published November 1. www.beazley.com/news/2018/beazley_breach_insights_october_2018.html.

Centers for Medicare & Medicaid Services (CMS). 2017. "Transactions Overview." Published July 26. www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html.

Donovan, F. 2018a. "Healthcare Continues to Bear the Brunt of Ransomware Attacks." *Health IT Security*. Published October 31. https://healthitsecurity.com/news/healthcare-continues-to-bear-the-brunt-of-ransomware-attacks.

———. 2018b. "Healthcare Data Presents Lucrative Target for Cyberattackers." *Health IT Security*. Published September 7. https://healthitsecurity.com/news/healthcare-data-presents-lucrative-target-for-cyberattackers.

Empel, S. 2014. "Way Forward: AHIMA Develops Information Governance Principles to Lead Healthcare Toward Better Data Management." *Journal of AHIMA* 85 (10): 30–32.

FTI Consulting. 2015. *The Information Governance Guide for Compliance Professionals*. Accessed February 3, 2020. http://static.ftitechnology.com/docs/toolkits/IG-for-Compliance-Teams-Toolkit.pdf.

HIPAA Journal. 2019a. "Expected HIPAA Updates and HIPAA Changes in 2019." Published January 31. www.hipaajournal.com/hipaa-updates-hipaa-changes.

———. 2019b. "New HIPAA Regulations in 2019." Published March 4. www.hipaajournal.com/new-hipaa-regulations.

———. 2018. "Largest Healthcare Data Breaches of 2018." Published December 27. www.hipaajournal.com/largest-healthcare-data-breaches-of-2018.

Houser, S. H., D. J. Slovensky, and L. Wang. 2017. "Information Governance for Analytics Support: Remember the Life Cycle Component." *Journal of the American Health Information Management Association* 88 (6): 38–40.

Journal of AHIMA. 2011. "Practice Brief: Managing Nontext Media in Healthcare Practices." *Journal of AHIMA* 82 (11): 54–58.

Kurzweil, R. 2001. "The Law of Accelerating Returns." Published March 7. Kurzweil Network. www.kurzweilai.net/the-law-of-accelerating-returns.

Office for Civil Rights (OCR). 2003. "Summary of the HIPAA Privacy Rule." US Department of Health & Human Services. Revised May. www.hhs.gov/sites/default/files/privacysummary.pdf.

Office of the National Coordinator for Health Information Technology. 2019. "Interoperability." Reviewed May 9. www.healthit.gov/topic/interoperability.

Olavsrud, T. 2017. "9 Biggest Information Security Threats Through 2019." *CIO*. Published March 28. www.cio.com/article/3185725/9-biggest-information-security-threats-through-2019.html.

Pew Research Center. 2019. "Mobile Fact Sheet." Published June 12. www.pewinternet.org/fact-sheet/mobile.

Ponemon Institute. 2018. "2018 Cost of a Data Breach Study: Global Overview." IBM Security. Published July. www.ibm.com/downloads/cas/861MNWN2.

Rosen, S. 1969. "Electronic Computers: A Historical Survey." *Computing Surveys* 1 (1): 7–36.

Snell, E. 2015. "A Review of Common HIPAA Administrative Safeguards." *Health IT Security*. Published July 17. https://healthitsecurity.com/news/a-review-of-common-hipaa-administrative-safeguards.

Statista Research Department. 2020. "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions)." Published February 19. www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.

Willig, J. H. 2015. "The Many Lives of Data." In *Handbook of Healthcare Management*, edited by M. D. Fottler, D. Malvey, and D. J. Slovensky. Cheltenham, UK: Edward Elgar Publishing.

CHAPTER

6

HEALTH INFORMATION TECHNOLOGY SERVICE MANAGEMENT

Learning Objectives

1. Articulate the impact that unplanned work has on the health information technology (HIT) department.
2. Identify a number of different process improvement frameworks that could be applied to the management of the HIT department and the advantages and disadvantages of each approach.
3. Describe ITIL management practices and their interrelationships.
4. Articulate why the configuration management database is critical to the service management practices.
5. Describe what service-level agreements are and why they are important to the HIT department.
6. Describe some of the reasons given for HIT service continuity plan failures.

Overview

A consistent area of focus throughout a healthcare manager's career, regardless of responsibility, is the constant effort to achieve efficient, cost-effective operations. While it is certainly true that all healthcare managers will continually be asked to think more strategically, a focus on the strategic aspects of the job at the expense of the operational aspects is a sure recipe for failure. Debra Walker, former chief information officer (CIO) of Goodyear Tire & Rubber Company, provides a framework for how to think about the effective management of a health information technology (HIT) department for both operational effectiveness and strategic impact. She suggests that the HIT department must master three levels of services. The base level provides a robust and reliable infrastructure for the organization, which is covered in chapter 5. The second level, which builds on the base level, provides excellent HIT services, which is the focus of this chapter. Walker characterizes the third level by noting that "if [the HIT department] achieves those two things, then