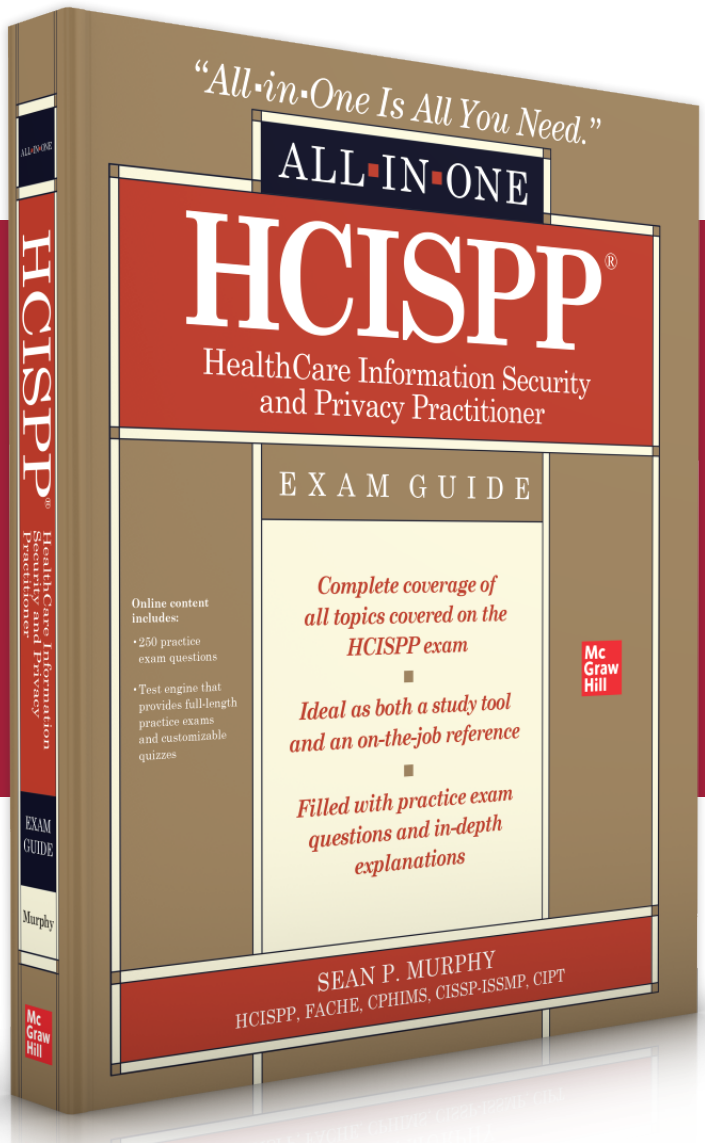
Mc Graw Hill

ALL·IN·ONE
HCISPP®
Healthcare Information Security and Privacy Practitioner
EXAM GUIDE



Sample Chapter

CHAPTER 5: Guiding Principles of Information Security: Confidentiality, Integrity, and Availability

LEARN MORE

BUY NOW

Because learning changes everything.®

mhprofessional.com

ALL IN ONE

HCISPP®
HealthCare Information Security and Privacy Practitioner

EXAM GUIDE

Sean P. Murphy

Mc Graw Hill

New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

Mc Graw Hill

ALL-IN-ONE
HCISPP®
Healthcare Information Security and Privacy Practitioner
EXAM GUIDE

ISBN: 978-1-26-046007-0
MHID: 1-26-046007-X

The material in this eBook also appears in the print version of this title: ISBN: 978-1-26-046006-3, MHID: 1-26-046006-1.

eBook conversion by codeMantra
Version 1.0

ALL-IN-ONE
HCISPP®
Healthcare Information Security and Privacy Practitioner
EXAM GUIDE

CHAPTER 5

Privacy and Security in Healthcare

This chapter covers Domain 5, "Privacy and Security in Healthcare," of the HCISPP certification. After you read and study this chapter, you should be able to:

- Identify key information security objectives and attributes
- Understand common information security definitions and concepts
- Know fundamental privacy terms and principles used in information protection
- Comprehend the interdependence of privacy and security in healthcare organizations
- Categorize sensitive health information according to US and international guidelines
- Define privacy and security terms as they apply to healthcare
- Distinguish methods for reducing or mitigating the sensitivity of healthcare information

The importance of understanding and applying proper privacy and security controls on healthcare information is foundational to your success as a healthcare information privacy and security professional. The healthcare industry is highly regulated in the United States as is the protection of personal data in most other countries. As we move from our discussion of the regulatory environments that impact our healthcare organizations, we will examine specific information security and privacy definitions and concepts that regulations and ultimately our policies and procedures are built upon. In this chapter, you will learn to understand security objectives and attributes, including the principles of confidentiality, integrity, and availability. You'll also learn about accountability, which is often a major part of the discussion of security as it relates to healthcare organizations. You will also learn general security definitions as they apply to healthcare.

As with most healthcare organizations, your organization likely faces a multitude of challenges, not the least of which is the need to apply a reasonable standard of due care and due diligence to safeguard the confidentiality, integrity, and availability of patient healthcare information. Whether the intent is to improve patient care, to protect the sensitive information we need to serve our customers, or to ensure compliance with regulatory requirements, the challenges are significant.

This chapter addresses security- and privacy-related topics together. This is in part because it also includes an overview of the relationship between information security and privacy. *Privacy* involves controlling access to personal information and the control a person can have over information discovery and sharing. *Security* is administrative, technical, and physical mechanism that protects information from unauthorized access, alteration, and loss. In short, privacy is about *what* we protect, and security is about *how* we protect it.[1]

EXAM TIP You will be tested on your basic understanding of security and privacy concepts and principles, the relationship between security and privacy, and the types of information requiring protection in the healthcare industry.

Privacy and security are important to everyone involved in healthcare, including health facility employees, patients, family members, and care givers. It also applies to anyone who works for organizations that play cursory roles in patient care—for example, workers at a clearinghouse for healthcare information who never work directly providing patient healthcare. These workers also have obligations to ensure that the privacy and security of patient data are maintained in accordance with their employers' policies and applicable regulations.

Guiding Principles of Information Security: Confidentiality, Integrity, and Availability

Data security has three guiding principles: confidentiality, integrity, and availability (CIA).[2] In general, it does not matter where you work, where you live, or what organizations you support; these principles remain the same. In addition to understanding CIA, you need to understand the importance of accountability, another central concept akin to CIA.

The CIA model is driven by the implementation of a combination of technical, administrative, and physical information protection controls. You should understand the relationship between CIA components in general and within your organization. Depending on a variety of concerns, including your role in the organization, the organization's mission and size, applicable regulatory authorities, and sensitivity of information, one component may be emphasized over the others. For example, as a system administrator, providing integrity and availability may be more appropriate to your job description than providing confidentiality.

The prevailing illustration used for the CIA triad is an equilateral triangle that indicates the "weight" of each component as being equal to the others. The reality of these relationships, however, depends on situational factors. This is an important concept, because the emphasis placed on these three factors represents the assessment and balance

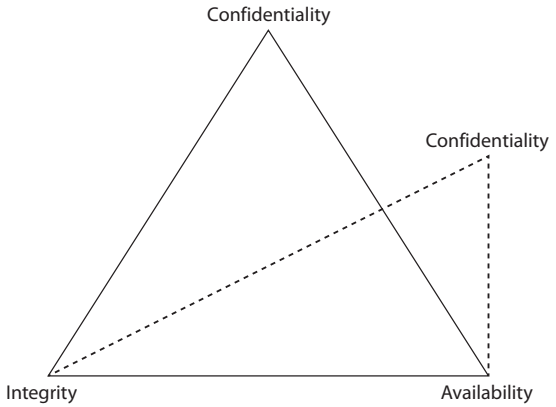


Figure 5-1 The CIA is often depicted as a triangle that implies the relationship of the three components.

of choices for security and privacy tools within your organization. So, for example, in your organization, confidentiality may be considered more of a priority than the other two factors, which means you'll have increased focus on access controls and encryption. Or if data availability takes precedence, you may invest more in technical solutions for disaster recovery.

Figure 5-1 shows a comparison of the CIA triad in two scenarios. In the solid line triangle, each component is weighted equally. The triangle comprising dotted lines depicts an emphasis on confidentiality in implementing security and privacy controls.

Confidentiality

Confidentiality relates to protecting sensitive proprietary information or personally identifiable information (PII) from unauthorized disclosure. The objective is to control access to a limited amount of data so that only those with proper authorization are allowed to access it. Security controls are implemented to protect confidentiality and avoid unauthorized disclosure. In healthcare, a breach in confidentiality could include an employee calling a media outlet to "anonymously" inform them that a public figure has been admitted to a rehabilitation facility. A similar example of a confidentiality breach, though beyond the scope of healthcare, also occurs when a fan magazine publishes photos of famous people enjoying personal time at a beach or other locale.

Although confidentiality is an important aspect in protecting information in any organization, healthcare information, in particular, warrants a higher level of protection and enforcement—consider, for example, an unauthorized disclosure that an individual has HIV, a psychiatric disorder, or another health concern.

Healthcare data confidentiality requirements are recognized internationally. For example, in the United States, the National Institute of Standards and Technology (NIST) has

issued directives regarding CIA for healthcare information, and within the scope of confidentiality it states the following in a 2008 publication:

> The confidentiality impact level is the effect of unauthorized disclosure of health care delivery services on the ability of responsible agencies to provide and support the delivery of health care to its beneficiaries will have only a limited adverse effect on agency operations, assets, or individuals. Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA [Health Insurance Portability and Accountability Act]. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations. In such cases, the confidentiality impact level may be moderate.[3]

In Canada, the Canadian Privacy Act, Section 63, states the following:

> Subject to this Act, the Privacy Commissioner and every person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their duties and functions under this Act.[4]

In healthcare, confidentiality is not only important to protect individuals from medical and financial identity theft, but research shows that a breach of confidentiality can impact patient care. In some cases, where breaches are all too common, some patients are worried their private information will fall into the wrong hands.[5] As mentioned in Chapter 4, providers understand that patients who fear their information might be disclosed in an unauthorized manner may delay seeking care or withhold information.

Specific circumstances require additional confidentiality considerations. For example, patient care information related to HIV, behavioral health, substance abuse, and children's health often have even more restrictive confidentiality requirements than other types of information.

Whether in the United States under HIPAA or in the European Union under the General Data Protection Regulation (GDPR), confidentiality requirements often continue even after an employee's role has changed or after an employee leaves a position or an organization. Most healthcare regulatory requirements clearly state that even when an individual no longer has access to the information, he or she is still required to keep the information confidential. For example, in the European Union, the Data Protection Directive, Article 28, Section 7, states the following:

> Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.[6]

By law, data collectors are responsible, in the United States and in most other nations, for maintaining the confidentiality of the information forever, even if the patient discloses the information. Of course, the patient can give consent for specific disclosures, but generally, regulations do not permit the healthcare organization to disclose the information outside of legal allowances. Further, the organization must protect the information from disclosure until it can legally and properly destroy it.

Integrity

Integrity is a security pursuit that is intended to protect information from unauthorized editing, alteration, or amendment. Imagine a scenario in which malicious code (such as a software virus) is introduced via a malware software application into a medical device. If, for example, that medical device is responsible for dosing medications to a patient, and the virus causes all decimal points to move to the right one space, the resulting dosage change can be significant, and potentially life-threatening, to the patient (for example, a dose of 0.5 ml may have a disastrous effect if only 0.05 ml is indicated). The integrity of healthcare data is important for patient safety and for many other reasons.

Data integrity is achieved by protecting the accuracy, quality, and completeness of the information. Integrity of information is maintained by assuring that any changes made to data are authorized and correct or not made at all. Security controls for integrity follow the data flow through the lifecycle of the information. When you examine the process of data collection and use in a healthcare setting, the data often changes format, and various data elements are combined, parsed out, or even aggregated. Throughout this process, however, the integrity of the data must remain intact. A patient name or date of birth, for instance, must remain the same even if it is collected as Jane Doe, December 14, 1970, at admissions and then changed to Doe, Jane, 12/14/70, after it gets transcribed into the billing system. Although this is an exceedingly simplified example, maintaining data integrity across data flow is one reason for the existence of standards such as the US Centers for Disease Control and Prevention (CDC) guideline ICD-10 for coding patient encounters, and Health Level (HL7), a set of international standards for transmitting health information across organizations and systems. Using standard data sets and transaction codes helps to assure data integrity.

To accomplish integrity, several methods are used, including error checking and validation procedures. The following list includes some generic data integrity approaches that apply, some sample technical methods, and the security improvements that are addressed. The list is adapted from data integrity guidance from the NIST SP 1800-11 (Draft), *Data Integrity: Recovering from Ransomware and Other Destructive Events*:[7]

- **Corruption testing** This procedure includes the use of extract-transform-load (ETL) data testing applications, reliable backups, and TCP/IP checksum testing to examine unauthorized changes. The process includes logging and auditing for a retrospective review of data. The testing uses file hashing and encryption algorithms to identify cybersecurity events and data alteration.

- **Secure storage** This process includes encrypted backups and immutable (unchangeable) storage solutions with write-once, read-many (WORM) properties. Technical processes, such as redundant storage—namely RAID—are storage configuration solutions that satisfy secure storage and data integrity protection.
- **Logging** A significant component of data integrity is to collect and enable the review of access to data and user activity. In this case, logging is used in alerting and analysis to discover any unusual or unauthorized activity and in legal discovery and e-forensics. It can be generated from individual systems. Several analysis tools can be used, such as security incident and event monitoring (SIEM) applications and network data capture systems.
- **Backup capability** Data integrity is preserved through procedures that enable data to be replicated and recovered periodically. Related to secure storage, backup tools support full, incremental, and differential schedules for backup. Another approach to backups is mirroring, which is similar to a full backup except that an exact copy of the data is stored separately, matching the source. Other backup procedures store files in one encrypted storage repository.

In healthcare, information integrity has a strong association with patient care and patient safety. While unauthorized disclosure (confidentiality) may lead to an unauthorized individual having access to healthcare data, and while the unavailability of data may hinder care, the fact remains that if the data we have on a patient is not accurate, it can in fact lead to death. For example, an unconscious patient who has an allergy to a specific medication undergoing treatment cannot advise staff about his allergy. In such a case, the availability of accurate data can save his life.

NOTE Security controls for integrity also apply to technology and processes that assure nonrepudiation. This means that the controls in place assure the authentication of a data user or sender without the possibility of another actor impersonating the user.

Availability

Information is valuable only if it is accessible and timely. The data can be accurate and kept private, but if it is not available when it is needed, this third part of the CIA triad has failed. Availability of data is generally described as proper access at the time the information is needed. In healthcare, we can certainly understand the failure of protecting PII and ensuring that patient records are accurate. But experiencing network downtime with no contingency operations plan in place would mean the information is not available at the point of care. If the provider does not have the ability to access the information he or she needs, patient care is affected and patient safety risks increase.

Paper-based health records and procedure manual processes can exacerbate the availability issue, because they may not be as easily accessed or enacted as digitally stored information. Not having availability of information can result in improper diagnosis,

inefficient or redundant tests, and in some cases adverse drug-to-drug interactions. A major assurance of availability from an information security and privacy perspective is reached through implementation of business continuity and disaster recovery procedures. These focus areas require the use of administrative, technical, and physical controls to oversee high-availability system architectures, reliable backups, secondary operating locations, and practiced recovery procedures.

Availability also relates to having only the necessary information available. Having too much information available or having unorganized raw data can pose a security issue. Privacy and security frameworks such as the DPD, GDPR, and HIPAA, for instance, address the issue of having relevant information versus having more information than is needed. Consider an example: A provider who requires a relevant prior MRI image when treating an orthopedic injury must certainly have the most recent MRI on the affected body part to compare against the latest image. However, that provider would be overwhelmed by having to search through all the images on record for unrelated care of that patient. If nothing else, the search would be time consuming and wasteful.

In addition, by limiting availability, we can prevent unauthorized disclosures or data breaches simply by not sharing unused or extra data in the transaction. For illustration, consider an example from the past. There was a time in the United States when credit card numbers were printed in their entirety on receipts. This was useful for identification purposes and convenient for the payer when proving a purchase or seeking a refund. But eventually the practice ceased, because proof of purchase could be determined in more discrete ways, such as using only the last four to six digits on the card with the other digits masked. The practice of including the entire credit card number introduced too much risk of data loss and identity theft. This is a good example of the security impact of unnecessarily disclosing too much information.

Accountability

While generally not considered part of the CIA principles, accountability is often included as a high-level security principle. Within the healthcare environment, compliance standards often treat accountability as a basic principle. Accountability in information security and privacy refers to the determination of who is responsible for proper and improper information access and use. For example, a clinician treating a patient who enters data, thereby editing the patient record, is accountable for the actions they take to enter the information. The clinician should be responsible for ensuring that the information is accurate when it is entered. Accountability intersects with the CIA principles. The individual with access should ensure the integrity of the data entered, while leveraging availability of the system, and ensuring confidentiality that the information is available only to those with proper authorization.

An organization must also demonstrate accountability for the information it collects and uses. Data use actions must be logged and audited to various degrees to prove that measures of accountability are in place. Accountability incorporates tracking actions and identification of responsible parties in retrospect after cybersecurity incidents and data breach recovery. Auditing information disclosure reports enables us to view and remediate any disclosures that may have been unauthorized, or at least to prove to government

regulators that disclosures are tracked as required. Nonrepudiation also applies to accountability. By providing protections such as digital signatures and encryption algorithms, an organization can ensure that the sender of an electronic message cannot deny sending it and that the receiver cannot deny receiving it. In this way, nonrepudiation assists organizations by providing ways to prove accountability.

Understanding Security Concepts

The concepts that shape information security can seem abstract and complex. To help you understand the approaches and practices of information security, this section describes some basic approaches and methods to security that you should be familiar with. These concepts are central to information security practices and compliance, and many progressive security processes are based on them.

You should be familiar with three basic aspects of security that will help you better understand the information that follows in this and other chapters: security controls, defense-in-depth, and security categorization. Understanding these important concepts may also improve your ability to do a good job in supporting and providing security and privacy in your organization.

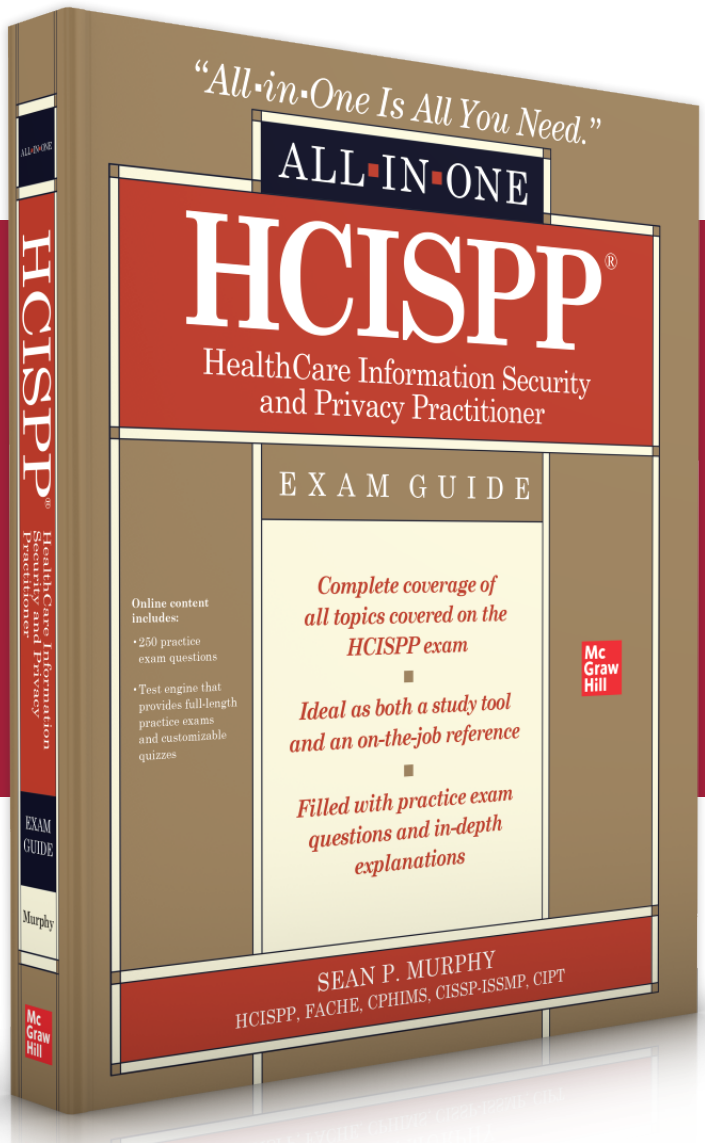
Security Controls Security controls include management controls (often administrative, such as policies or procedures), operational controls (the processes we follow to do things), and technical controls (hardware and software implementations to assist in securing computer-based resources). The organization's cost considerations and interrelationships between security controls have a great deal of influence on the ability of the organization to deliver on its mission.

Defense-in-Depth Defense-in-depth consists of implementation of various defensive controls working together for your systems or applications to protect the overall security of organizational assets. In the IT world, examples of defense-in-depth include the integrated use of antivirus and antimalware software, firewalls, encryption, intrusion detection and prevention systems, and biometric authentication. An example of defense-in-depth in your home is an alarm system for the house that includes smoke and carbon monoxide detectors, which may or may not be separate from the smoke detectors; cameras that you can check remotely over the Internet; and smartphone apps that enables you to control lighting, entry doors, and so on. Figure 5-2 demonstrates the defense-in-depth principle, and although it may not depict a system used in larger organizations, it provides a basic understanding of how the layers of the system must rely on one another to be effective.

Security Categorization Security categorization enables you to determine the level of security required for a system based on the information (or data) type the system uses or maintains. This book specifically addresses working with healthcare information, which includes sensitive information such as protected health information (PHI) and electronic protected health information (ePHI), personal health records (PHRs), personally identifiable information (PII), and a number of other terms, depending on where you work (which can include the specific nation, continent, province, or state).

Mc Graw Hill

ALL-IN-ONE
HCISPP®
Healthcare Information Security and Privacy Practitioner
EXAM GUIDE



Sample Chapter

CHAPTER 5:
The Relationship Between Privacy and Security

LEARN MORE

BUY NOW

Because learning changes everything.®

mhprofessional.com

The Relationship Between Privacy and Security

Security is focused on protection of information from unauthorized disclosure as well as the capabilities needed to detect, respond, and recover from events that become incidents. The focus of privacy is restricting and managing the authorized access to sensitive information and making sure individuals provide personal information only after they are informed of and understand their rights. In performing your role as a healthcare information security and privacy professional in your organization, you must be familiar with certain general and specific areas, but it's also important for you to know how these areas relate to one another. For example, you must understand how consent relates to authorization, how openness relates to transparency, and how legitimate purpose relates to purpose specification. Knowing how HIPAA, DPD, PIPEDA, and other regulations differ is also important.

Privacy and security have evolved over time to become a combined general category of "information protection." The progression was natural, as we find more and more texts and seminars on healthcare privacy and security with the terms used synonymously. However, there is still a distinction between the two that you need to understand. Primarily, information security will never focus on privacy principles such as notice, consent, and accounting of disclosures, for example. Privacy, it can be argued, will focus on more than just digital assets; it will also fulfill obligations to the patient. For example, the organization's promise in the notice of privacy practice may indicate obligations it has that are not related to ensuring confidentiality, integrity, and availability of the data. Maybe its obligations are focused on ensuring the relevancy of the information it collects. This consideration may not have any impact on information security concerns for the same information.

Granted, the domains of privacy and security are closely related, and increasingly so. However, it is unlikely we will ever get to a point where they are indistinguishable and synonymous. We can be relatively certain that for privacy to be effectively provided, security controls must exist and operate effectively. With that in mind, there are a few concepts that demonstrate the interconnected nature of privacy and security, particularly in healthcare, where an unbreakable bond exists between the two: these concepts are dependency, integration, and ownership.

Dependency

The relationship between security and privacy has developed into one of dependency. To achieve security in the healthcare industry, there are certainly elements of privacy that must be addressed. Security controls are more effective and efficient when privacy principles such as data retention or purpose are followed, which reduce the need to protect data that is not required and can be potentially breached. At the same time, privacy is often provided through one or more information security controls.

Within the regulatory process for protecting privacy of personal information (for example, under HIPAA), encryption is seen as an adequate information security control for ensuring the confidentiality of the information transferred via e-mail. Integrated within this security control is the ability to make sure that the person to whom you want to send the e-mail is authorized to view it. The patient experiences the dependency of privacy on security in that the confidentiality they expect is usually regulated by access controls and detection of unauthorized use, as examples. In short, information security tools are used to protect unauthorized disclosure from a privacy perspective.

Privacy depends on good information security practices to preserve the right of individuals to choose who has access to their information. In fact, maintaining the right to refuse to share the information at all is an element of privacy that information security is designed and implemented to protect. In the use of EHRs, identification, authentication, and access management technologies serve to allow credentialed access to defined amounts of data. Without proper credentials, access is denied. Based on the patient's choice and consent, access is even more defined. For example, when patients choose to disallow any requests for their patient status, information found in the EHR cannot be shared with friends, family, or individuals calling the reception desk. Of course, there are usually additional instructions provided to allow specific family members or powers of attorney to receive patient status updates.

Integration

Privacy and security depend on each other, and that dependence results in an integration of the two. In other words, providing information security may involve privacy issues. Conversely, providing privacy can introduce unintended information security concerns that may have nothing to do with whatever privacy protection is being implemented. For example, a number of security safeguards (surveillance cameras and facility access logs, for example) require monitoring people or collecting personal information. These safeguards introduce privacy concerns, because not only do they keep data and people more secure, but they collect personal data in the process. So, while initially you may be concerned with unauthorized access to a patient portal, you may end up having an additional concern with privacy controls. As information privacy and security professionals, we must balance such information security measures against the privacy impacts of collecting personal information, constantly assessing risk. Almost daily, we see integration of privacy and security processes. The goal is to ensure that we understand the implications of privacy and security actions on one another as well as on the problem we intended to address.

This is not to say that integration necessarily produces a negative consequence. Most integration of privacy and security is positive in nature. Information security controls in a digital environment successfully provide privacy as they automate routine processes such as access management. They also reduce errors in enforcement that would exist in paper-based environments, where policy adherence or human action is the only line of defense. For instance, a network firewall or access control list programmed into a router is certainly less fallible than a records room clerk in charge of clearing individuals for facility entry. Moreover, privacy is the intended consequence of many information security practices. Where organizations enforce role-based access configuration of their EHR systems, the privacy of each individual's information is protected by allowing access only to those providers who have a requirement to use the data. In a paper-based records system, this level of data segmentation and constrained availability is nearly impossible. Eavesdropping and easy access to data in plain view is too likely. In the context of integration of information protection, it is relevant to reiterate that the introduction of HIT often improves privacy and security concerns, even as we examine the impacts to information protection HIT capabilities generate.

Another example, and a timely one, of how privacy concerns are integrated with information security involves bring-your-own-device (BYOD) initiatives. While healthcare organizations are increasingly allowing individuals to bring their own smartphones, laptops, tablets, and mobile devices to work, under these initiatives, they are also instituting information security policies and procedures to protect the PHI and PII on their networks—the same networks these devices are accessing. One such procedure is *data wiping*: In the event an employee quits or is terminated, and that person used his or her own device to access the organization's network resources, the BYOD policy likely gives the organization the right to remotely and completely erase everything on the device. This would include the work-related information along with any potential PHI or PII. It could also include pictures, personal information, and personal property.[22] Because of this, the healthcare organization's effort to protect privacy through information security may actually infringe on the privacy of the employee. When implementing the BYOD policy, the integration of privacy and security issues should be considered.

Ownership of Healthcare Information

When it comes to healthcare, traditional expertise grew independently around privacy (such as protecting identity) and information security (such as protecting resources). Over time, both disciplines evolved and developed into specific competencies found in the workforce.

Today that reality has changed. Privacy and security have been integrated into an almost singular competency that every person handling PHI or PII requires. The reasons for the integration have already been discussed—the digitization of health information, networking of medical systems and devices, and regulatory pressures to safeguard health information, to review a few. This is a global reality.

Let's examine the impact of privacy and security from the perspective of information use, beginning with a quick look at health information ownership according to international law and customs, with a focus on the key concern of ownership of the information

once it is collected by a healthcare organization. This concern is addressed differently in different countries, based on each country's views on data ownership and laws. Recognizing how authorities view this concern helps you understand how relevant guidelines, laws, and customs affect the overall privacy and security approaches the country expects healthcare organizations (or data collectors) to take.

United States (HIPAA)

True ownership of health information is hard to determine. If we try to make a comparison between how the United States regulates property rights against a notion of data ownership, the comparison is flawed. To clarify, the issue is what level of control a patient in the United States actually has with regard to the use of their private information. Property rights offer owners control as to how their property is used or not used. The rights enforced by US laws provide guidance about how the information is used, but patients don't have ownership rights in that some nonconsensual PHI uses are authorized, such as use for public health reasons or for use under purview of an institutional review board (IRB).

NOTE An IRB is an internal organization in an academic healthcare environment where research is conducted and is in place if clinical trials are performed with the use of human subjects. The IRB governs some baseline consent and authorization guidelines that would not necessarily include additional input from the patient.

Patients do have the right to know what information is collected about them, the right to access that information, the right to request amendment when the information is believed to be incorrect, and the right to know who else has seen the information. Once the data is collected, however, the healthcare organization owns the information in the recorded format, whether written or electronic, such as a file folder or a digital file. The legal responsibility to safeguard the information under HIPAA stems from a perspective of proper caretaking of the data, but the law favors healthcare organization ownership.

European Union (GDPR)

In the European Union, GDPR makes it very clear that the individuals who provide their personal information are the data owners. Data collectors have a responsibility to protect sensitive information continually, but the rights individuals have over their information do not change as the information changes hands. There are strict provisions for gathering personal data, which allow collection of data only for legitimate purposes. Once data is collected, the healthcare organization must respect the rights of the individuals as the data owners. Chief among the rights of data owners under GDPR is the right to complain and obtain redress if an individual believes his or her information is not being used in a way the data collector indicated. In fact, as mentioned earlier in the chapter, as the data owner, the individual has the right to be forgotten from that organization's databases.

United Kingdom

Because healthcare is funded and provided almost exclusively by the National Health Service (the United Kingdom's government healthcare system), health data and medical records in the United Kingdom are seen as government property. Controls must be in place to safeguard the information, of course. There are provisions for patients to view and address perceived discrepancies in their records, but the philosophy of ownership leans toward the government. The overall responsibility for the records lies in the authority of the Secretary of State for Health.

NOTE The UK implementation of GDPR includes a national data opt-out, which became effective in March 2020. Under this provision, individuals can choose not to allow their sensitive information to be used for research and healthcare planning.

Germany

Germany is presented here outside of the governance of the GDPR, because Germany passed its own law, known as an *implementing law* for GDPR. The Federal Data Protection Act (FDPD), effective as of May 25, 2018, was enacted the same day as the GDPR. Germany was the first EU member state to issue its own implementing law.

One of the most important focuses of the FDPD is extensive provisions on the processing of personal data of employees. The law serves to clarify and strengthen the obligation of the provider not only to safeguard the information, but to document all health information completely. For example, the provider must document information such as patient history, diagnoses, treatment, and prognoses. The law mandates that the provider properly maintain the records (whether paper or digital) and preserves ownership with the individual. For example, the law mandates that any and all information be made available for the patient upon his or her request. However, there is some ambiguity in the implementation law about secondary uses of health data. A debated issue is that data controllers in special cases may process the health data for a purpose that is different from the original one. FDPD references GDPR, which has an exception that permits the processing of data for scientific or historical research, or statistical purposes, without consent.

Understand Sensitive Data and Handling

The process of collecting, recording, storing, and exchanging data electronically introduces risks of disclosure, but understanding how healthcare data might be impacted by the method in which you handle it is an important aspect of your role in protecting that data. Most individuals obviously do not want their healthcare records disclosed to others without their permission. Confidentiality is essential to privacy, which is essential to patient care. Confidentiality practices are in place to protect the dignity of patients and to ensure that patients feel free to reveal complete and accurate information required for them to receive the correct medical treatment.