**CHAPTER 26**

**Healthcare**

Internationally, healthcare systems are relying increasingly on technology for improvement in efficiency, safety, patient outcomes, and enhanced communication between patient and practice. Many economies are rapidly adopting electronic health records (EHRs) as a means to streamline operations and keep better operational control over costs and processes. While EHRs can lead to substantial increases in patient satisfaction, health record portability, and cost savings, they can also lead to substantial exposure if not protected properly. Laws in different economies vary. We offer some general advice; however, you should always seek local advice on specifics.

**Overview of Information Assurance Approach**

As introduced in [Chapter 3](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch3.html#ch3), the MSR information assurance model involves five *essential* services: confidentiality, integrity, availability, authentication, and nonrepudiation. When applied to the healthcare industry, these overarching concerns become apparent immediately:

• **Confidentiality** Patients have an expectation not only confidentiality but privacy of their medical records. While privacy is a special case of confidentiality, the requirement of protecting the information from unauthorized disclosure remains. Healthcare organizations and their partners must remember that patients own their information and are legally protected in many nations from disclosing it without permission.

• **Integrity** Patients must have confidence that their medial record is accurate and timely. Incorrect information in a medical record can lead to prescription errors, dosing errors, surgical mistakes, and worse. The information system handling medical information must ensure records are altered only by authorized personnel or processes and that a function exists to ensure the integrity of the information.

• **Availability** Especially in urgent or emergency care, the availability of medical information means the difference between life or death. If a healthcare organization is reliant on an EHR as the official system of record for medical files, the records must be available when needed regardless of maintenance, weather, or power outages.

• **Authentication** To maintain confidentiality, integrity, and nonrepudiation, the EHR must incorporate strong authentication. The authentication must ensure actions can be traced to a unique user or process. Authentication must be logged.

• **Nonrepudiation** Nonrepudiation ensures actions and changes to the system and records can be traced to a process or individual without dispute. Strong authentication is vital in ensuring accountability. Strong logging and auditing ensures actions are recorded and can be later referenced to individual users. By ensuring EHR users are using the system only as intended in a defensible manner, patients gain confidence in EHR systems when healthcare organizations can prove who accessed their records, for what reason, and what changes were made.

Using the previous information, the next step is to use the MSR framework to analyze the risks present in using EHRs and offer controls to mitigate, transfer, avoid, or accept risk. The approach will involve using the chapters of this book to describe, at a high level, action and controls that healthcare organizations should consider in mitigating risk.

**Healthcare-Specific Terminology**

The healthcare industry has developed several terms and definitions that define patient health information in electronic forms. The following are commonly used terms as adapted from the National Alliance for Health Information Technology:

• **Electronic medical record (EMR)** This is the electronic record of health-related information on an individual created, gathered, managed, and consulted by licensed clinicians and staff from a single organization who are involved in the individual’s healthcare.

• **Electronic health record (EHR)** This is the aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one healthcare organization and is managed and consulted by licensed clinicians and staff involved in the individual’s healthcare.

• **ePHR** This is an electronic, cumulative record of health-related information on an individual, drawn from multiple sources, that is created, gathered, and managed by the individual. The integrity of the data in the ePHR and control of access to that data is the responsibility of the individual. Microsoft’s HealthVault is an example of an ePHR.

By these definitions, an EHR is an EMR with interoperability (that is, integration to other providers’ systems). An ePHR could have interoperability with either EHRs or EMRs. The important distinction between the system types is the interoperability and who controls the patient’s information and access to the information.

**Information Assurance Management**

Information assurance must be a strategic priority established by senior management at the top of the organization. While small organizations may lack the resources to dedicate a full-time information assurance team, senior management must assign responsibility for information assurance throughout the organization. If blended roles are used, senior management must commit to an AT&E program for individuals in information assurance practices and strategies.

**Personnel**

Healthcare organizations must designate an overarching authority for record security and privacy. This person may be an office manager, a chief information officer, a chief risk officer, or even the head of the practice. Whoever is assigned functional responsibility for security and privacy should possess fundamental information assurance practitioner skills as they are applied to healthcare. Organizations should consider training and credentialing personnel to ensure a minimum level of competence is met. For example, (ISC)**2** offers the Healthcare Certified Information Security and Privacy Practitioner (HCISPP) credential. This credential tests and validates experience over the following domains of knowledge:

• Healthcare industry

• Regulatory environment

• Privacy and security in healthcare

• Information governance and risk management

• Information risk assessment

• Third-party risk management

If senior management decides to outsource information technology, the organization still has a responsibility to ensure the information assurance requirements are met. Including credentialing requirements as part of a contract agreement is a wise move to ensure those who handle sensitive health information understand basic information assurance concepts.

**Management Approach**

Smaller organizations will most likely default to a bottom-up approach to information assurance management, but must be cautious because some regulatory environments mandate aspects of a top-down approach such as policies, procedures, standards, and guidance delivered from the head of the organization. Regardless of the approach, it should be documented in an information assurance strategy document ideally as part of the organization’s work plan or organizational strategy document.

Organizations of any size must determine how to adopt the basic Plan-Do-Check-Act (PDCA) cycle of information assurance management. As technology changes and culture shifts, organizations must have a way to determine the best approach to respond to changing organizational forces. The PDCA encourages a proactive approach to ensuring information assurance is integrated throughout the organization’s life cycle.

**Regulations and Legal Requirements**

Regulations and legal requirements will vary by location. You can find some of the more common regulations associated with privacy in Appendix F. In addition to privacy laws, some countries, states, and economies have additional laws related specifically to healthcare. For example, the Health Information Portability and Accountability Act of 1996 (HIPAA) in the United States requires healthcare entities and business associates to do the following:

• Report breaches of unsecured personal health information

• Implement the confidentiality provisions of the Patient Safety Rule

• Implement the requirements of the Privacy Rule

• Implement the requirements of the Security Rule

Another example of legal requirements is France. Through the Data Protection Law of January 6**th** 1978, France requires healthcare professionals to either apply as or work with an accredited medical data host when a third party (like a cloud provider) processes or stores medical information. Accreditation requirements can be quite strict, including appointing a doctor who will oversee the confidentiality and access of the medical data. The organization must understand the explicit requirements imposed by the legal jurisdiction they operate in. Organizations must also be aware of business partnerships, outsourcing arraignments, and cloud computing activities that may trigger certain aspects of legal requirements. We recommend advice from legal counsel in making major decisions in these areas.

**Information Assurance Risk Management**

image

If researched and an acceptable scope is established, the organization should have a good understanding of their operating environment. Senior leaders should be aware of any legal restrictions and should have assigned information assurance responsibilities throughout the organization. The next step is to understand information assurance risk. The MSR information assurance model addresses risk through the use of risk assessments. Risk assessments are based on assets, impacts, likelihood, vulnerabilities, and threats. You can find information regarding the development of risk management systems in [Chapter 11](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch11.html#ch11).

**Assets**

The medical records of patients are obviously valuable not only to the business but also to competitors, marketers, identify thieves, and anyone looking to possibly blackmail or smear the reputation of a patient. While medical records rank high on the list of assets, healthcare providers should not neglect other assets such as, but not limited to, the following:

• Prescription pads

• Banking information

• Contract information

• Employee information

• Proprietary procedures

• Research

Remember that not all assets are electronic; manual processes and paper constitute part of the information. These assets present the possibility of theft and therefore should be considered assets as part of an overarching information assurance risk assessment. Remember, assets may be digital or physical. A stack of prescription pads can be used the same way as a digital prescription. A printed medical record has the same information as a digital record. Categorize assets based on impact to the organization.

Some assets, such as medical records, may be “high” impact to the organization, while contract information is deemed “moderate” or even “low.” Organizations should consider different aspects of information assurance when categorizing information. For example, a medical record may have a “high” impact if confidentiality is breached but a “moderate” impact if availability is lost. You can find more information regarding threats in [Chapter 4](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch4.html#ch4).

**Threats**

Threats in the healthcare industry must be viewed through not only an information technology lens but also a physical lens. For printed medical records, the threat of physical theft is real; Appendix B describes commonly identified threats. The organization should consider each asset and determine which threats apply. Remember, human threats have motivation, means, and opportunity to be successful, while natural threats are based on location, patterns, and environmental conditions. You can find more information about threats in [Chapter 4](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch4.html#ch4).

**Vulnerabilities**

Like threats, vulnerabilities must be considered with the operational environment. Digital records are subject to vulnerabilities that hackers could exploit in addition to physical security concerns. Appendix C provides a detailed list of common vulnerabilities organizations should be aware of. Organizations should also incorporate continuous monitoring and vulnerability management programs into their identification of vulnerabilities. You can find more information about continuous monitoring in [Chapter 20](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch20.html#ch20).

**Risk Assessment**

As noted in [Chapter 11](https://learning.oreilly.com/library/view/information-assurance-handbook/9780071821650/ch11.html#ch11), risk management is the determination of risk by assessing the likelihood of an adverse event (a threat exploiting a vulnerability) and the resulting impact. Each asset must be aligned with relevant threats and vulnerabilities to determine the likelihood and impact to the organization. Remember, threats and vulnerabilities are not simply technical. They may manifest in personnel, procedures, policy, competition, environment, and information technology. The assessment should determine which areas, program systems, or assets of the organization contain the most risk. You can view an example risk analysis table in Appendix E.

**Risk Mitigation**

Once risks are identified, mitigation, acceptance, transfer, or acceptance must be identified. This section covers several of the controls mentioned throughout the book in the context of healthcare organizations. You can find more information regarding risk mitigation throughout the book.

**Policy, Procedures, Standards, and Guidance**

Healthcare organizations of any size must ensure they implement and use policies that memorialize management’s information assurance decisions. These policies should be updated and referenced in employee training materials. The policies should provide information about possible disciplinary actions as a result of violations of privacy and unauthorized sharing of personal health information. Policies should include legal or regulatory requirements to show management’s commitment for complying with applicable laws and setting the expectation for the rest of the organization.

Procedures and standards work hand-in-hand to provide specific structure around policy expectations. Some of the most common procedures for healthcare providers include, but are not limited to, the following:

• Release of healthcare information

• To the subject

• To other parties

• Protection of physical records

• Destruction of physical records

• Retention of physical records

• Protection of electronic records

• E-mail procedures to ensure information is not leaked

• Proper use of encryption tools when sending or storing health information

• System testing and upgrading procedures to ensure no leaks occur

• Proper standards for the secure destruction of ePHI

Standards identify specific technologies or criteria that are necessary to maintain the policy. The following represent some common standards present in healthcare organizations:

• Release of healthcare information

• Standard forms required

• Standard for identity proofing

• Protection of physical records

• Standards of sufficient destruction (tools and technologies)

• Standard periods for retention

• Protection of electronic records

• Standard approved encryption technologies approved for use

• Standards of reporting time for incidents

• Information system standards for secure configurations

Finally, guidance should be viewed as the glue that holds all three together. While not binding, guidance can be invaluable in providing context around the use of standards, policy, and procedures in specific scenarios.

**Human Resources**

Healthcare organizations have a duty to hire employees who are trustworthy and who will maintain the confidentiality of patient health information. In addition to background investigations and references as allowed by locality, healthcare organizations should consider whether credentials are necessary for a particular role in the organization. For example, a smaller organization’s owner may decide every new hire will obtain the (ISC)**2** HCISPP credential because they will all be expected to play a part in the decentralized approach to information technology employed at the organization.

Organizations must also be aware of restrictions on hiring. For example, in the United States, a provider that performs services for Medicare patients must ensure their staffs are not on the U.S. Department of Health and Human Services’ Office of Inspector General’s exclusion list. The individuals and organizations listed have been excluded from the Medicare program and are prohibited from rendering services to and billing for Medicare services.

**Certification, Accreditation, and Assurance**

Some economies and countries will require healthcare organizations to undergo a form of certification and accreditation. If the healthcare organization is in one of these environments, the requirement will necessarily drive many aspects of their information assurance approach. However, even organizations not subject to mandatory certification and accreditation standards should consider voluntarily adopting them. Not only can certification and accreditation help mature an organization’s information assurance processes, it can provide a safe harbor or a position of due care and due diligence. In the U.S., Texas healthcare providers can obtain certain safe harbor provisions for IT security breaches if their system is certified under the HITRUST model.

**Information Assurance in System Development and Acquisition**

The same information assurance requirements memorialized in the organization’s information assurance policy must be incorporated into system development activities and also system acquisition activities. In some countries, third parties such as cloud providers must meet stringent certification and accreditation requirements to process, store, or transmit healthcare information. Senior management must remember their commitment to protect health information extends not only to systems but to the data itself. The requirement for protection follows the data to whatever system or media it may travel.

**Physical and Environmental Security Controls**

Healthcare organizations must ensure their offices are physically secure. Most offices contain not only hard copy health information but also expensive medical equipment, prescription drugs, and computer equipment containing electronic health records; both electronic and hardcopy records must be planned for and protected. Healthcare organizations must ensure physical security requirements extend to any business partners or third-party processes, storing or transmitting information on their behalf. Physical security includes monitoring technologies such as cameras and voice recording. Healthcare providers must be careful not to have surveillance in areas where patients may have a legally protected expectation of privacy.

**Awareness, Training, and Education**

Healthcare organizations must ensure their workforce has continuous information assurance training and awareness. Organizations should require all new hires to complete baselines awareness and training to familiarize themselves with the organization’s information assurance policies, procedures, standards, and guidelines. System and sensitive information access should be restricted until the new employee has completed the training.

Annual or even more frequent training and awareness should be incorporated into the organization’s information assurance culture. Organizations of any size should consider credentialing information assurance “superusers” with credentials such as the (ISC)**2** HCISPP and appointing them as “go-to” people when questions surrounding information assurance arise. Successful awareness and training programs add an element of competition in training and awareness completion. Organizations should consider adding training and awareness as a performance element for their employees and contractors.

Of the preventive information assurance tools and techniques available, none carries the significance of proper change management and configuration management. Change management ensures all aspects of the healthcare organization’s systems are considered when changes occur. Change management should interact with policy updates, regulatory changes, and changes to information systems to ensure changes do not negatively impact the information assurance posture of the organization.

Configuration management should be implemented to provide a mature and consistent application of technical information assurance controls across the enterprise. When products are vulnerable or updates are required for operating systems, knowing the standard configuration is invaluable in mitigating the risk.

**Access Control**

Healthcare organizations should strive to adopt multifactor authentication whenever possible. Multifactor authentication requires two different factors for successful authentication. For example, a username provides identification, a password or PIN is something known, and a further element such as a token is something someone has. By requiring additional factors for authentication, healthcare organizations can greatly strengthen not only access control requirements but also nonrepudiation requirements. Access control must be carefully monitored and logged. Successful and unsuccessful authentication attempts should be logged, monitored, and reviewed.

**Continuous Monitoring, Incident Response, and Forensics**

Much as healthcare organizations care for patients by monitoring vital signs to determine deviation from norms and determining the output from diagnostics, information systems rely on the same rigor to keep a steady read on risk. Most continuous monitoring takes the form of vulnerability monitoring produced through automated vulnerability scanners. Even the smallest of organizations can afford basic vulnerability scanners that will help determine configuration weaknesses of information systems.

Vulnerability information must be relayed to the change management and configuration process for mitigation and patching. Remember, vulnerability is only part of the overall risk equation. If likelihood of a threat exploiting the vulnerability is low, the organization may not want to prioritize the patching or mitigation if it is resource intensive.

Healthcare organizations must engage in incident response. U.S. laws such as HIPAA require timely reporting of information breaches to authorities. Organizations that fail to report a breach face larger fines and sanctions when discovered. Many laws also require organizations to notify patients of the breach and ensure appropriate credit monitoring is in place at the expense of the healthcare organization. Forensics may help a healthcare organization prove due diligence if the forensics process determines sufficient technical controls such as encryption were in place to mitigate the breach.

**Business Continuity and Backups**

Healthcare organizations must carefully consider the availability requirements of their mission and data. Information needed frequently and without delay should be housed in a hot-site hosting arraignment or similar. Healthcare organizations need to clearly determine business continuity plans and disaster recovery plans to ensure service is available in times of disaster. Healthcare services are often the hardest hit during a disaster because they see increased demand for their services while often operating in a contingency mode themselves.

**Further Reading**

• American Recovery and Reinvestment Act of 2009 (ARRA). Title XIII, “Health Information Technology for Economic and Clinical Health Act (HITECH),” §13600, 2009. [www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf](http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf).

• Center for Democracy and Technology. Health Privacy (web page), 2013. <https://www.cdt.org/issue/health-privacy>.

• Data Protection Act 1998, Chapter 29. 1998. [www.legislation.gov.uk/ukpga/1998/29/data.pdf](http://www.legislation.gov.uk/ukpga/1998/29/data.pdf).

• Hernandez, Steven G. *The Official (ISC)***2** *Guide to the HCISPP CBK*. (ISC)**2** Press, 2014.

• HIPAA Case Examples and Resolution Agreements. [www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html).

• Organization for Economic Co-operation and Development. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980. [www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm](http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm).

• Ponemon Institute. Third Annual Survey on Medical Identity Theft. June 2012. [www.ponemon.org/local/upload/file/Third\_Annual\_Survey\_on\_Medical\_Identity\_Theft\_FINAL.pdf](http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf).

• The European Data Protection Directive, 2001. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF>.

• The Patient Protection and Affordable Care Act of 2010. Pub. L. No. 111-148, § 124 Stat. 119, 2010. [www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf](http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf).

**Critical Thinking Exercises**

1. A U.S.-based healthcare clinic consists of an owner who is the head doctor of the practice, a physician’s assistant, an office manager, a few nurses, and a couple assistants. Who is responsible for ensuring ePHI security and privacy?

2. Assuming a clinic uses ePHI within the scope of the UK’s data protection law, what technical controls should the clinic consider implementing to ensure the confidentiality and privacy of its records?