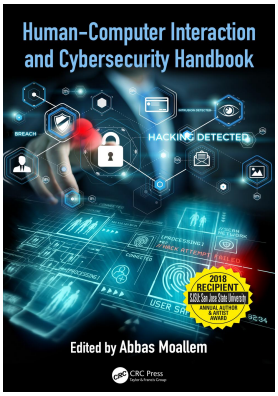

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Healthcare information security and assurance

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-13
Ulku Yaylacicegi Clark, Jeffrey G. Baltezegar
Published online on: 24 Oct 2018

chapter thirteen

Healthcare information security and assurance

Ulku Yaylacicegi Clark and Jeffrey G. Baltezegar

Contents

13.1 Introduction

Healthcare represents a significant segment of the US economy. In 2016, total health expenditures reached $3.3 trillion and are projected to grow to 5.6% per year until 2025 (CMS, 2016). Per Centers for Medicare and Medicaid Services statistics, the 2016 figures translate into $10,348 per person or 17.9% of the gross domestic product of the nation. The use of in healthcare organizations is believed to alleviate the expenditure while increasing the overall quality of patient care. HIT services involve the use of technology to provide healthcare as well as to enable the comprehensive exchange the digital health information (Office of National Coordinator for Health Information Technology, 2015). This chapter introduces and discusses some issues related to the digitization of health sector. Section 13.1 summarizes regulations Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) that started the digitization. Section 13.2 discusses the three-step evolution of digital records: adoption of electronic health records (EHRs), EHR-to-EHR information exchange, and EHR–personal health record (PHR) information exchange. The challenges and opportunities introduced by mobile devices (smartphones, tables, etc.) are presented in Sections 13.3 [mobile health (mHealth) applications] and 13.4 [mobile device management (MDM) and bring your own device (BYOD)]. Section 13.5 reviews the ransomware attacks and disaster recovery plans (DRPs) as a countermeasure. The user perspective of digitized health industry is reviewed in Section 13.6.

13.1.1 HIPAA

The HIPAA of 1996 (HIPAA, Public Law 104-191) is intended to provide continuous health insurance coverage for workers who lose or change their job and to reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission of administrative and financial transactions. The US Department of Health and Human Services (HHS) set guidelines by the HITECH Act in 2009 and expanded it with the HIPAA omnibus rule in 2013. Out of five titles of HIPAA, title II detailing administrative simplification addresses how electronic healthcare transactions are transmitted and stored. The HIPAA security rule mandated by title II establishes a standard for the security of electronic protected health information (aka ePHI) (Table 13.1).

The HIPAA security rule intends to safeguard the confidentiality, integrity, and availability of all ePHI by securing any individually identifiable health information during electronic or digital storage, processing, or transmission. The rule applies to covered entities (CEs) and business associates. CEs include healthcare providers, health plans, healthcare clearinghouses, and certain business associates. A business associate is any organization or person working in association with or providing services to a CE who handles or discloses personal health information (PHI) or PHRs. CEs choose the appropriate technology and controls for their own unique environment taking into consideration their size and capabilities, their technical infrastructure, the cost of the security measures, and the probability of risk. HHS Office of Civil Rights (OCR) authority is responsible for investigating violations and enforcing the security rule, and the fines for noncompliance are up to $1,500,000 per violation per year. The HIPAA security rule details administrative, physical, and technical safeguards.

The HIPAA privacy rule establishes national standards to protect individuals' medical records and other PHI and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically. The rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information,

Table 13.1 Five sections of HIPAA

Title I: HIPAA Health Insurance Reform	Title I protects health insurance coverage for individuals who change or lose jobs and prohibits group health plans and issuers from denying coverage to individuals with specific diseases and preexisting conditions.
Title II: HIPAA Administrative Simplification	Title II entails the HHS to establish national standards for processing electronic healthcare transactions. It also directs healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS.
Title III: HIPAA Tax-Related Health Provisions	Title III includes tax-related provisions for healthcare.
Title IV: Application and Enforcement of Group Health Plan Requirements	Title IV provides further details on provisions for individuals with preexisting conditions and those seeking continued coverage.
Title V: Revenue Offsets	Title V includes provisions on company-owned life insurance and the treatment of those who lose their US citizenship for income tax purposes.

Source: (https://www.hhs.gov/hipaa/for-professionals/index.html)

including rights to examine and obtain a copy of their health records and to request corrections.

The HIPAA enforcement rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA administrative simplification rules, and procedures for hearings.

In 2013, HHS announced the omnibus rule, which included modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the HITECH Act, the Genetic Information Nondiscrimination Act, and other modifications to HIPAA rules.

13.2 EHR, health information exchanges, nationwide health information network, meaningful use, fast healthcare interoperability resources standard, and PHR

Currently, one of the HIT services is the EHR system, which is an electronic record of patient health information generated by one or more encounters in any care delivery setting (PCORI, 2017). The mandated digitization of health records by the American Recovery and Reinvestment Act of 2009 resulted in 93% adoption of EHR systems by the end of 2014. Majority of the health organizations adopting EHR systems demonstrated meaningful use of EHR, which refers to the use of EHR to improve quality and safety, improve care coordination, and maintain security and privacy of ePHI. The complete picture of the patient's health history presented by the EHR provide essential information to physicians to make the most informed decision while cutting the costs of redundant tests and examinations. EHR implementations have been shown to increase the quality of healthcare delivery and reduce the associated costs (Bourgeois and Yaylacicegi, 2010).

One of the primary goals behind the initiative of the government for encouraging the adoption of EHRs is to increase health information exchanges (HIEs) and eventually maintain a nationwide health information network (NHIN). The NHIN aims to provide a secure and interoperable health information infrastructure that allows stakeholders, such as physicians, hospitals, payors, state and regional HIEs, federal agencies, and other networks, to exchange health information electronically (Cline, 2012). The NHIN will significantly help reduce healthcare spending in the United States while improving the patient care quality.

As EHR adoption and meaningful use increased, health professionals quickly realized a multitude of interoperability problems between the EHRs of different vendors. HL7, an organization that develops standards for the exchange, integration, sharing, and retrieval of EHR, drafted the first healthcare interoperability resources guide (FHIR) in 2004 in an attempt to address integration issues with EHRs, portals, HIEs, mobile phone applications, cloud communications, and other health information technology (IT) systems (Mandel et al., 2016). FHIR is expected to have full standard status by 2017.

The logical next step is the EHR-to-patient information exchange. Many providers permit patients to access their PHRs via patient portals (Schleyer et al., 2016). In addition, patients are collecting/recording data regarding their health using various mobile applications such as MyFitnessPal. In the 10-year vision of the Office of the National Coordinator for Health Information Technology, the empowerment of users/patients to manage their own PHR and consequently get timely individualized diagnosis and treatment with the help of real-time data shared by the providers are emphasized (ONC, 2015).

13.3 mHealth applications

mHealth is used to denote how mobile and wireless technologies can be used to improve health-related services. The field of mHealth has undergone rapid changes and continues to move up the healthcare agenda (Istepanian and Xhang, 2012; Sebelius, 2011; Varshney, 2011). Seventy-seven percent of the US population now have a smartphone (Pew Research Center, 2017), and these phones continue to develop new features and see improvements in computing power. Smartphones can now be used to track, manage, and improve health (Landau, 2012a, 2012b; Powell et al., 2014). Perhaps the most visible element of mHealth is the profusion of phone applications (apps), especially the ones related to fitness and wellness. A simple search in application stores shows the presence of a large number of such applications. There were more than 90,000 iOS mHealth applications available in 2015—with a more than 100% increase compared to 43,000 iOS mHealth applications available in 2013. In addition, global health application downloads increased from 1.7 billion in 2013 to 3.7 billion 2017 (Statista, 2018). In 2020, the global mHealth market value is estimated to be $58.8 billion.

mHealth "apps" are widely used by consumers and medical professionals (e.g., patients, doctors, pharmacists, and others). The main categories of mHealth apps that are in use are reference apps (such as WebMD), wellness applications (such as MyFitnessPal), social media apps (such as PatientsLikeMe), and apps designed to access EHRs (such as Care360) and PHI (such as Microsoft HealthVault) (mHIMMS, 2015). In another report, commissioned by Royal Philips Electronics, it is reported that a growing number of mobile users are turning to—and trusting—mHealth applications (RPE, 2012). One in 10 Americans surveyed in the study believe that if it were not for web-based health information, "they might already be dead or severely incapacitated." A quarter of those surveyed use symptom checker websites or home-based diagnosis technology as much as they visit the doctor, while another 27% use these interactive applications instead of going to the doctor. While only 66% of the patients would be willing to fill a prescription from their physician, 90% of the patients are willing to use an application prescribed by their doctor (mHIMMS, 2015).

Although, there is currently little evidence-based research that can directly support the health benefits of mHealth applications, there is good reason to believe that these applications have potential to significantly benefit overall health. Perhaps the most benefit potential lies in applications designed to access EHRs and PHIs; however, both patients and doctors need to know that the privacy, security, and safety of these applications are adequately addressed before mHealth can be successfully integrated into the healthcare system. mHealth apps allow patients to take control of their own health, especially in areas of healthy eating, managing chronic disease, and quitting smoking (Varshney, 2011). Additionally, PHRs, which include medical history, laboratory health results, and insurance information, help people manage their lives and actively participate in their own healthcare (Davis et al., 2017). For doctors, mHealth can help provide point-of-care resources and aid in managing their practices. For patients, mHealth can improve the convenience, cost, and quality of their healthcare. mHealth is an important tool in the healthcare arena and its significance and success or failure will be determined from how it integrates with health systems and allows for better care of patients.

Populations that currently use mHealth technologies have the most benefit from the use of this technology. Patients with chronic health conditions, as well as people who want to maintain good health, would benefit from the implementation of mHealth (Varshney, 2011). As more patients become aware of the health benefits of mHealth, they

are anticipated to increase subscriptions to mobile technologies and health applications. Even though there are applications that help manage a specific condition, applications that integrate and consolidate the data are still in the development phase.

For doctors, mHealth apps can help provide point of care resources and aid in managing their practices. Doctor's list privacy and security as concerns as the leading barriers to greater use of mHealth (Gagnon, 2016). Patients using mHealth applications need to have confidence that the products they are using are safe, secure, and accurate. Data security, access control, policy, and confidentiality are the main issues that must be addressed in order for mHealth to continue to flourish and deliver safe healthcare benefits.

13.4 MDM systems and BYOD

Many healthcare organizations utilize mobile devices in the workplace to allow providers to travel as needed. While these devices are a great asset for the providers, they have also presented many problems to the IT staff responsible for managing them. With the increased adoption of these devices for technology such as telemedicine, the need for secure management capabilities is increasing. There are several MDM systems (MDMSs) on the market that are designed to make it easier to manage smartphones, tablets, and laptops that are in use in the workplace. These systems typically offer a centralized interface for deploying and configuring agents on the mobile devices.

The challenge with managing these mobile devices is that a healthcare organization must protect patient data at rest, in transit, and in use on a device that may not be designed to be natively managed by an enterprise. To make matters worse, many users take their devices with them while travelling off site and outside of the protected corporate network of the organization. While travelling, new potential issues arise such as data interception, loss or theft of the device, and unauthorized access by third parties. To address these threats, a MDMS must be able to add a layer of encryption by utilizing a virtual private network. The MDMS enable users to remotely access and wipe the device on demand and ensure that only authorized users are able to access the data on the device. While some vendors have created management systems that are capable of providing these services, the IT department must also be able to effectively implement and enforce these controls on a daily basis.

In addition to configuring the device for MDM, users must be educated on how to use the MDM application, what the limitations of the MDM application are, and what their role is in supplementing the MDM application to ensure the security of their device. For instance, an IT department may choose not to enforce automatic updates to mobile devices, to help minimize downtime, or to prevent potential problems from new software revisions. The user is then responsible for updating their mobile device to ensure that it has the latest security patches in place. When considering mobile device vulnerabilities disclosed recently, patching mobile devices is critical to maintaining confidentiality of data in use on these devices. Users who are not aware of the importance of updating their mobile device will place their data at a much greater risk of exposure.

Some of the common capabilities found in MDM applications are device encryption, screen locks, encrypted backups, and remote wiping. Mobile device users must understand the purpose of these features and how they work to ensure the security of their device and the data stored on it. From a mobile device user's perspective, the MDM application may even be a hindrance rather than a tool that can greatly increase the security of their data. For instance, screen locks using a personal identification number (PIN) or password may be inconvenient, but they help prevent unauthorized parties from accessing the mobile

device. Some organizations may even enforce data destruction if the PIN or password is incorrectly entered more than five times. This protection measure greatly increases security while making the user more accountable for access to their device. Leaving a device in a bag or allowing a child to play with it could potentially cause the phone to be reset without the user's knowledge.

Alternative authentication measures such as fingerprint scanning or facial recognition are also possible. Using a fingerprint scan is already possible with several iPhone and Android devices, but is still not proven to be completely secure. According an article in the *New York Times*, researchers at the New York University and the Michigan State University "were able to develop a set of artificial 'MasterPrints' that could match real prints similar to those used by phones as much as 65 percent of the time" (Goel, 2017). Facial recognition is also available in some smartphones but, in some cases, has been defeated simply by placing a photo of the authorized user in front of the device's camera (Amadeo, 2017).

What does all this mean for the end user? The safest built-in authentication method available for mobile devices is still the PIN or password. If the user is following password best practices, however, it is likely that they must keep up with as many as 20 different passwords for various accounts. The result is that many users will resort to using unsafe password management practices, such as reusing passwords for multiple accounts or using passwords that are easily guessed by an attacker. When considering the sensitive nature of data on mobile devices in the healthcare industry, strong authentication measures on mobile devices are a requirement. To supplement weak authentication measures, a two-factor authentication (2FA) mechanism such as a token (Yubikey, Duo, etc.) or time-based one time password (Google Authenticator, Duo, etc.) could be implemented. With growing support and integration into existing login portals, 2FA offers improved authentication security and may be easier to get users to "buy in" to secure processes. Simply entering an additional code into a login portal after typing in a password may be more easily adopted by a user than continually increasing the complexity of the password.

The work does not end when the device is delivered to the employee; regular auditing of its compliance status is critical but can easily be overlooked. In larger organizations, it is possible that some mobile devices are lost or stolen for extended periods before the IT staff has been notified. This scenario creates even more work for the IT staff, since they must then begin the process of reviewing log files for the time that the device was lost to identify whether a data breach occurred. Other poorly designed or implemented MDM platforms could allow a user to circumvent or altogether remove the MDM agent from the device. The device would then be unmanaged and therefore unprotected by the corporate controls that were put in place. Failure to properly configure just one mobile device could cause a major breach if the device becomes lost or stolen. According the HSS Breach Portal, there were approximately 824,324 records exposed due to a lost or stolen laptop or other portable electronic device from 2015 to 2017 (see Table 13.2). According to the data provided, 279,233 records were exposed due to lost or stolen laptops. Another 114,458 records were exposed due to lost or stolen devices identified as "other portable electronic devices." Of the breaches identified in this table, the two largest breaches—due to a lost or stolen laptop—account for over 74% of the records exposed during this time frame.

As the workplace evolves, many organizations are allowing their employees, contractors, and associates to bring their own personal devices into the workplace for use with corporate data systems. The immediate challenge is that the organization must come up with an effective method of management for these devices that meets organizational

Table 13.2 Reported number of records breached involving a mobile device from 2015 to 2017

Spokane VA Medical Center	3,275	Laptop
W. W. Grainger, Inc.	1,594	Laptop
Indiana Health Centers, Inc.	1,697	Desktop computer and laptop
South Bend Orthopedic Associates Inc	1,272	Laptop
Mercy Family Medicine	2,069	Other portable electronic device
Spectrum Health System	902	Other portable electronic device
California Pacific Orthopedics and Sports Medicine	2,263	Laptop and paper/films
Little River Healthcare	542	Laptop
Bay Area Pain and Wellness Center	548	Laptop
Southwest Community Health Center	6,000	Desktop computer and laptop
Durango Family Medicine, PC	18,790	Other portable electronic device
LKM Enterprises, Inc.	3,400	Desktop computer and laptop
Pacific Ocean Pediatrics	18,637	Other portable electronic device
LSU Healthcare Network	2,200	Other portable electronic device
Nova Southeastern University	1,086	Other portable electronic device
Michigan Facial Aesthetic Surgeons d/b/a University Physician Group	3,467	Laptop
Spine Specialist	600	Laptop
Lifespan Corporation	20,431	Laptop
Western Health Screening	15,326	Other portable electronic device
Specialty Dental Partners of Philadelphia, PLLC–DBA Rich Orthodontics	960	Desktop computer and laptop
Local 693 Plumbers & Pipefitters Health & Welfare Fund	1,291	Other portable electronic device
Denton Heart Group–Affiliate of HealthTexas Provider Network	21,665	Other portable electronic device
Sharp Memorial Hospital	754	Laptop and other portable electronic device
Wonderful Center For Health Innovation	3,358	Laptop
Children's Hospital of Los Angeles	3,594	Laptop
Managed Health Services	5,500	E-mail and laptop
Kinetorehab Physical Therapy, PLLC	665	Laptop
MGA Home Healthcare Colorado, Inc.	3,119	Laptop
Gibson Insurance Agency, Inc.	7,242	Laptop
Fred's Stores of Tennessee, Incorporated	9,624	Laptop
StarCare Speciality Health System	2,844	Laptop and paper/films
Kaiser Permanente Northern California	1,136	Other portable electronic device
California Correctional Health Care Services	400,000	Laptop
Quarles & Brady, LLP	1,032	Laptop
OptumRx, Inc.	6,229	Laptop
W. Christopher Bryant DDS PC	2,200	Other portable electronic device
Premier Healthcare, LLC	205,748	Laptop
Centers Plan for Healthy Living	6,893	Laptop
St. Luke's Cornwall Hospital	29,156	Other portable electronic device
Total	824,324	

Source: HHS, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, HHS, Washington, DC, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

policy but allows the user to retain some control over their own device—some users may be reluctant to hand over control of their personal devices to their employer. To further complicate matters, there is a wide range of smartphones and tablets that must be considered when considering a strategy to manage them.

While there are some MDMSs that integrate both Android and iOS managements, there is not one perfect solution that integrates natively across all platforms. The result is that the IT department must integrate third-party systems with their enterprise network, while protecting the connections between them. The increased risk created by implementing new software increases an organization's attack surface. Hence, new software configurations and remote access requirements can cause an increase in the number of headaches for the IT staff who implement it. While the recent push for cloud-based technologies has been a welcome shift for some organizations, other problems may arise as a result of transmitting and storing data with a cloud provider. For example, some MDM platforms may require access to the internal network to issue certificates to mobile devices for authentication to wireless networks, creating more exposure of internal services to the Internet. It is also possible that smaller organizations may be unable to implement an MDMS because of the cost and/or complexity of the system. This only increases the likelihood that they will experience a breach because of an unprotected mobile device being used to access or store patient data.

Even in an IT department with staff dedicated to managing mobile devices, there is still a possibility that an incorrect configuration could allow employees to access company data without restrictions. For example, an organization could adopt a very secure MDM application and deploy it to all company-owned mobile devices, but fail to prevent users from accessing their corporate e-mail account on a personal device that does not have the MDM application installed. With the availability and popularity of cloud-based e-mail systems such as Office 365, it is possible for a user to connect their own smart devices with their e-mail accounts with little or no trouble at all. According to Trend Micro (2015), 69% of employees say that they use their smartphones for work, while their IT staff believed that only 34% of them do.

Although MDMSs can provide organizations with great control over their devices, issues still arise with the implementation of these systems. For instance, the design of the Apple iOS does not allow for integration into a Microsoft Windows domain environment, preventing the devices from utilizing device certificates. The IT staff must then create user accounts to allow the iOS devices to utilize user certificates, which results in a new problem—orphaned user accounts that will exist within the active directory until the devices have been retired.

If mobile device manufacturers could work together to agree on an open standard for developing devices that could be managed in a corporate setting, it is very likely that the security of patient data could be greatly improved. Given the rapid adoption of mobile devices in the workplace, it is easy to see that this trend will continue and will increase the need for a unified management system for these mobile devices. Creating a common framework for the integration of devices into an lightweight directory access protocol environment could allow for these devices to be integrated into corporate networks that are relying on them more and more every day, allowing for native management of the configuration of the devices as well as ensuring the secure configuration of the devices is correctly implemented and enforced. User experience would also be greatly improved by using a common security baseline in devices from all vendors, eliminating vendor-specific training and the use of third party applications for management.

13.5 Ransomware attacks and the role of the DRP

Although careful planning and implementation of security systems is critical to the mitigation of risk, not all attacks and breaches can be prevented. Healthcare organizations must therefore carefully consider the actions to take when security incidents do occur so that they can create an effective action plan to be executed when needed. This type of plan is known as a business continuity plan, or BCP. A smaller component of the BCP is the DRP, which focuses on a specific department or service. For example, a BCP will identify processes and procedures to be carried out by an organization in the event of a disaster so that the overall business can return to normal operations as quickly as possible. A DRP created by the IT department in an organization would focus on identifying procedures that restore systems and services critical to IT department operations as quickly as possible.

While BCPs have always been a requirement of the HIPAA, the threats that organizations must prepare for have evolved. Twenty years ago, an organization may have considered a physical intrusion on company property to be more likely to occur than a remote attack by a hacker. Today, however, remote attacks occur at an alarming rate thanks to the evolution of both hardware and software, allowing attackers to gain access to remote systems more quickly and more easily than ever before. Twenty years ago, an organization might not have considered the possibility that an employee could walk off site with a copy of company data in their pocket. Today, flash drives and portable hard drives have increasingly large storage capabilities and can be transported in a coat pocket. Some organizations may even find that all their sensitive data could be stored in a single portable storage device.

In recent years, a new type of malware, called ransomware, has created a need for organizations to review their existing BCP and DRP documents to ensure that they are effective in stopping it. Ransomware typically infects a system through an e-mail attachment, by clicking a link in a phishing e-mail or by plugging in an infected universal serial bus drive. Once the ransomware has infected the system, it begins to encrypt all data that does not belong to the host operating system. After the encryption process is complete, the user is notified that their data are inaccessible, and a fee will need to be paid to regain access. The encryption used by ransomware is typically unbreakable, leveraging public key cryptography that is commonly used to protect confidential data while communicating with websites over the World Wide Web. To increase the pressure to pay the ransom as quickly as possible, the attackers may only give the victim a few days to pay the ransom, at which point the attacker destroys the decryption key and access to the stolen data are lost.

Until recently, the most effective approach to recovering from a ransomware attack was to create an out-of-band backup of the data of the organization so that it could be restored as quickly as possible when needed. Some recent ransomware attacks, however, have taken things a step further; the attackers threaten to release the encrypted data to the public if a ransom is not paid. Now, not only is the IT staff dealing with an infection that is impacting day-to-day operations, they must consider that possibility that their sensitive data will be exposed if they do not pay the ransom. While the backup provides them with a way to recover quickly, they must still pay the ransom to prevent their data from further exposure. The interruption of day-to-day operations and the cost of recovery from the infection can greatly affect an organization as well. Unfortunately, simply having an out-of-band backup is not sufficient anymore.

To be prepared for a ransomware infection, healthcare organizations must have a plan in place to quickly respond to an incident, isolate the infected machine, remove the infection, and restore the systems back into production state. Simply purchasing a standard

template or hiring a consultant to create the DRP is not enough, however. Every organization must regularly test its DRP for effectiveness so that when needed, the organization is able to follow the predetermined procedures with minimal delay. One effective method of testing the DRP is the "table top exercise," or "TTX," which facilitates the review of procedures in the DRP by having key personnel meet to respond to a mock disruptive event and discuss the response plan and how it would apply. Any potential problems could then be identified, and adjustments would be made to the DRP to ensure that it remains effective. Regular training should also be provided to all key personnel so that they are aware of the procedures to follow during a disruptive event, such as a ransomware infection.

A DRP should include a section that identifies all personnel who will be part of the computer incident response team, or CIRT. This team should include key members of the IT department, including system admins, network admins, technicians, as well as anyone in management. All members of the CIRT should be aware of their role as part of the team, as well as their responsibilities if called upon to respond to an incident. In the event of an emergency, an organization cannot afford to waste time deciding on which employees are responsible for each task in the recovery process. When considering the capability of recent ransomware variants such as WannaCry and Petya, it is apparent that a quick, efficient action is needed to isolate the infection before it spreads throughout a network, compromising other devices in the process. Without this critical step, a healthcare organization could potentially spend weeks recovering after a ransomware infection hits their network.

Communication is a critical component of the disaster recovery process. Once an incident occurs, it is imperative that an organization has clearly identified procedures for notifying key personnel so that they can execute the DRP. Having a documented path for the escalation of a potential incident could mean the difference between effectively stopping a ransomware infection from spreading and cleaning it up after it infects a network of devices. Once the disaster recovery procedures have begun, the communication between key personnel is critical to ensure that the plan is carried out effectively. Time spent waiting for a return phone call for authorization, for example, could cripple response efforts and allow valuable time to slip by. Recording contact information and alternate contact methods for key personnel in the DRP is a good step toward facilitating communication during this process. Notifying users of expected downtime is another critical step in communicating during a ransomware infection. Whether the effects are limited to a single server or the whole data center, the inability to access company resources during this time can have a significant impact on the employee's ability to perform their job. If they have not already been trained on how to continue operations during a disruptive event such as this, make sure they are provided specific instructions for continuing to function in their role within the organization until services can be fully restored. Finally, the communication between the organization and the patient is another critical step in the disaster recovery process. Notifying them of any potential breach and/or outage will ensure compliance with industry requirements and may help mitigate public relations problems down the road.

Given the serious nature of a ransomware attack in healthcare industry, it is imperative that organizations have a DRP in place to respond as quickly and efficiently as possible. As ransomware attacks evolve, health organizations must adapt to these threats proactively or face potentially catastrophic circumstances.

13.6 User experience

One important aspect of information security in any industry—especially healthcare—is the user's experience while interacting with the controls put into place. The oldest and

simplest authentication method, the password, is becoming more of a problem as technological advances in computing have made simple passwords extremely easy to defeat. Many security experts will agree that the recommended minimum length of a password should be 12 characters, but most organizations would find it difficult to enforce this requirement, if possible at all. To make matters worse, many users have multiple accounts online. In the healthcare industry, it is possible that healthcare staff members must remember passwords for the EHR system, e-mail account, computer login, mobile device login, voice-over-Internet protocol (VOIP) voicemail, and even time clock. From a password management standpoint, this could mean up to six different passwords remembered for various accounts. Many users will resort to using unsafe methods of remembering their passwords, such as writing down their password on notes attached to their monitor or keyboard, defeating the protection provided by requiring a strong password for authentication.

Another challenge that arises in the healthcare field is that devices are sometimes shared by multiple employees. For example, one laptop placed on a rolling cart could be used by several nurses while they make their rounds to check on patients and distribute medication. A user who forgets to logoff when they finish using the laptop might return to find that someone else has entered data under the wrong username. In some cases, passwords could be shared with users who forget theirs or who cannot access their account for some reason. As a result, the organization will not be able to get an accurate accounting record of what actions were taken by a user on the shared laptop. Another reason users may be required to share a laptop is that many healthcare facilities operate 24 hours a day. Staff who work rotating shifts will often share devices with other employees in their department while they are off the clock. To make this work, some devices—such as tablets—must be set up with a shared user account so that multiple users can access a single device. In this case, it is very likely that the password to the account is found written down somewhere close by.

To support their healthcare staff, IT departments must strive to make their systems as user friendly as possible while maintaining the security of patient data. In demanding work environments such as a healthcare facility, the stress of having to remember a unique password to login to an EHR system may create inefficiency in the workflow process. One way to improve upon using a unique password for every business system is to implement a single sign on, or SSO. The SSO is a login method whereby a user authenticates to one server, who then validates the user's identity to multiple other systems. Many software vendors already support some form of SSO based on the security assertion markup language (SAML), which is an open standard for authentication between systems. By utilizing SAML in all business systems, a healthcare organization could require their users to create one strong password that protects their user account, which is then used to authenticate them within the organization. For instance, a user could then login one time to their company web portal, which would verify the user's identify. That authentication server would then automatically provide SAML identity verification to any other system (e-mail, EHR, VOIP phones, etc.) the user attempted to login to, without the user having to enter any additional passwords. With only one strong password to remember, the user would have a much better experience when authenticating to a business system and security would be greatly improved.

One of the major hurdles that healthcare organizations and software vendors must overcome is that healthcare staff often go through training and certification just to enter the field and must then maintain licensure and accreditation through on-going training and recertification. The result is that healthcare employees must spend most of their time learning and honing their skills as healthcare professionals, which does not always include

technological training. Asking providers to take time away from their patients to improve their security awareness is not easily done and can negatively impact their ability to provide care to their patients. As is the case in many other industries, the organization must design a plan that can educate staff on information security fundamentals such as password strength and mobile device security in a way that can be understood and adopted by healthcare professionals.

Finally, healthcare organizations must also consider their patients when implementing EHR systems. The HITECH Act of 2009 requires that healthcare organizations provide patients with a way to access and download their electronic information. Providing external access to protected information presents a unique set of challenges to information security and must therefore be carefully considered before implementation. Many EHR systems provide a patient portal to meet the HITECH requirement and mitigate some of the risk faced by the healthcare organization. To access their data, patients typically go through a setup process where they access the portal to prove their identity and validate the personal information stored about them. Once this process is complete, the patient will be able to access their health records on demand. While this new technology is a great improvement, an extra burden is placed on the organization's staff to maintain the publicly accessible system through updates as well as continually monitor it for security events.

References

Amadeo, R. (2017, March 31). Galaxy S8 face recognition already defeated with a simple picture. *Ars Technica*, https://arstechnica.com/gadgets/2017/03/video-shows-galaxy-s8-face-recognition-can-be-defeated-with-a-picture/.

Bourgeois, S., and Yaylacicegi. U. (2010). Electronic health records: Improving patient safety and quality of care in Texas acute care hospitals. *International Journal of Healthcare Information Systems and Informatics*. 5(3), 1–13.

Cline, S. (2012). *About Health IT in North Carolina*. NDoHaH Services, North Carolina Department of Health and Human Services, Raleigh, NC.

CMS (Centers for Medicare & Medicaid Services) (2016). *NHE Fact Sheet*. CMS, Baltimore, MD. https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nhe-fact-sheet.html (last accessed: 1/15/2018).

Davis, S., Roudsari, A., Raworth, R., Courtney, K. L., and MacKay, L. (2017, July 1). Shared decision-making using personal health record technology: A scoping review at the crossroads. *Journal of the American Medical Informatics Association*. 24(4), 857–866, https://doi.org/10.1093/jamia/ocw172.

Gagnon, M.-P., Ngangue, P., Payne-Gagnon, J., and Desmartis, M (2016). m-Health adoption by healthcare professionals: A systematic review. *Journal of the American Medical Informatics Association*. 23(1), 212–220, https://doi.org/10.1093/jamia/ocv052.

Goel, V. (2017, April 10). That fingerprint sensor on your phone is not as safe as you think. *New York Times*. https://www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

HIPAA (US Department of Health and Human Services). HIPAA for Professionals. HHS, Washington, DC. https://www.hhs.gov/hipaa/for-professionals/index.html.

HHS (US Department of Health and Human Services). *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. HHS, Washington, DC. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Istepanian, R., and Xhang, Y.-T. (2012). Guest editorial introduction to the special section: 4G health—The long-term evolution of m-health. *IEEE Trans on IT in BioMedicine*. 16(1), 1–5.

Landau, E. (2012a). Smartphone apps become "surrogate therapists." *CNN*. http://www.cnn.com/2012/09/27/health/mental-health-apps.

Landau, E. (2012b). Tracking your body with technology. *CNN*. http://www.cnn.com/2012/09/21/health/quantifiedself-data/index.html.

Mandel, J., Kreda, D., Mandl, K., Kohane, I., and Ramoni, R. (2016). SMART on FHIR: A standards-based, interoperable apps platform for electronic health records. *Journal of the American Medical Informatics Association*. 23(5), 899–908.

mHIMMS (2015). *mHealth App Essentials: Patient Engagement, Considerations, and Implementation*. Healthcare Information and Management Systems Society, Chicago, IL. http://www.himss.org/mhealth-app-essentials-patient-engagement-considerations-and-implementation.

ONC (2015). *Update On The Adoption Of Health Information Technology And Related Efforts To Facilitate The Electronic Use And Exchange Of Health Information*, Washington, DC. https://www.healthit.gov/sites/default/files/Attachment_1_-_2-26-16_RTC_Health_IT_Progress.pdf (last accessed: 5/23/2018).

PCORI (Patient-Centered Outcomes Research Institute) (2017). *Users' Guide to Integrating Patient-Reported Outcomes in Electronic Health Records*. PCORI, Washington, DC. https://www.pcori.org/document/users-guide-integrating-patient-reported-outcomes-electronic-health-records (last accessed: 1/24/2018).

Pew Research Center (2017). *Record Shares of Americans Now Own Smartphones, Have Home Broadband*. Pew Research Center, Washington, DC. http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/, (last accessed: 1/24/2018).

Powell, A. C., Landman, A. B., and Bates, D. W (2014). In search of a few good apps. *JAMA*. 311(18), 1851–1852. https://doi:10.1001/jama.2014.2564.

RPE (Royal Philips Electronics) (2012). *Philips Survey Reveals One in 10 Americans Believe Online Health Information Saved Their Life*. RPE, Andover, MA. http://www.newscenter.philips.com/us_en/standard/news/press/2012/20121212_Philips_Survey_Health_Info_Tech.wpd#.UZVUN7Xrz7Q.

Schleyer, T., King, Z., and Miled, Z. B. (2016). A novel conceptual architecture for person-centered health records. *AMIA Annual Symposium Proceedings*, 1090–1099.

Sebelius, K. (2011). Keynote Address at mHealth Summit, Washington, DC. http://www.hhs.gov/secretary/about/speeches/sp20111205.html.

Statista (2018). *Number of mHealth App Downloads Worldwide from 2013 to 2017*. Statista, Hamburg. https://www.statista.com/statistics/625034/mobile-health-app-downloads/.

Trend Micro (2015). *Implementing BYOD: How Lost or Stolen Devices Endanger Companies*. Trend Micro, Shibuya. https://www.trendmicro.com/vinfo/ph/security/news/mobile-safety/how-lost-or-stolen-devices-endanger-companies.

Varshney, U. (2011). *Pervasive Healthcare Computing: EMR/EHR, Wireless and Health Monitoring*. Springer, New York.