Cyber Security and Mobile Medical Devices: Protecting and Securing Patient Medical Information
CONTENTS

SUMMARY 3

1. Background 4
   1.1. The Healthcare and Public Health Sector and Cyber Threats Against the National Infrastructure 4
   1.2. Expansion of the Use of Mobile Devices in Healthcare 4
   1.3. Types of Mobile Devices in Use in Healthcare 5
   1.5. Patient Medical Information: Electronic Health Records, Electronic Medical Records 5

2. Who Poses Threats to Mobile Devices, What Are These Threats, and How Are They Carried Out? 7

3. What Challenges Are Related to the Use of Mobile Medical Devices in Healthcare? 8


5. What Techniques Are Used by Those Initiating Cyber Threats to Mobile Devices and Networks? 11

6. What Activities by Users Make Mobile Devices Vulnerable? 12

7. What Points of Contact in Healthcare Are Most Vulnerable to Loss of Electronic Patient Medical Information? 13

8. What Are the Most Common Ways That Electronic Patient Medical Information Is Lost or Stolen? 14

   9.2. Actions Users Can Take to Protect and Secure Mobile Devices 18
   9.3. Establishment of a “Security Culture” in Healthcare 19

CONCLUSION 21

REFERENCES 22
SUMMARY

This white paper addresses the protection and security of the US healthcare sector against disruption and compromise of critical technology and electronic data, especially as they relate to mobile medical devices and patient medical information (PMI).

The US “Healthcare and Public Health” (HPH) sector, a multitrillion dollar industry, encompasses various types of organizations, from hospitals and blood banks to pharmaceutical companies and federal agencies. In the ever-expanding environment of easily accessible electronic information, these private, corporate, and governmental entities and their combined 13.5 million employees are potential targets for cyber attack. Because the HPH sector is taking full advantage of rapidly advancing digital technology to manage and make information available electronically, all computing devices and networks used in the sector are also vulnerable to attack.

The use of mobile medical devices is expanding everywhere, including within the HPH sector. Technologic advances have resulted in higher storage capacities, faster computing speeds, easier use, and much improved portability and remote connectivity, all of which have greatly enhanced the utilization of mobile devices in direct patient care in real time. With easy and immediate access to information, however, come the vulnerabilities of computer systems and the responsibility to keep electronic PMI protected and secure.

Two major concerns of the HPH sector are securing mobile medical devices to protect them against cyber theft of PMI and to protect and secure networks against malicious intrusion. A perfect storm for loss of PMI exists today, resulting from the various ways in which mobile devices can be compromised, their numerous vulnerabilities, and the chronic attempts by cyber criminals to siphon off information. Compromise may result from, for example, inadequate incorporation of products onto networks, misconfigured networks, and poor security practices. Vulnerabilities are present because mobile devices have the potential to transmit and receive data over a network without encryption, allowing interception of that data. Cyber criminals exploit these opportunities using sophisticated electronic means, along with simple loss and theft, to illicitly obtain PMI.

Effective methods can be used to protect and secure mobile medical devices, networks, users, and ultimately, electronic PMI. One simple step is for organizations in the HPH sector to have in place and educate employees about security policies, procedures, and processes for devices, networks, and people. IT administrators can implement numerous controls such as using intrusion prevention software to monitor traffic from mobile devices and monitoring devices for messaging, data leakage, and inappropriate use. Actions by users that can help to protect and secure mobile medical devices include keeping them safe at all times when in public spaces and never using an unsecured public Wi-Fi network.

Today’s electronic environment poses enormous challenges to the HPH sector. Concerted and continuous efforts by everyone who works in the sector will be required to protect and secure electronic PMI.
1. Background

1.1. The Healthcare and Public Health Sector and Cyber Threats Against the National Infrastructure

The US “Healthcare and Public Health” (HPH) sector is vast, encompassing varied private, corporate, and governmental entities, among which are hospitals, patient care facilities, pharmacies, pharmaceutical and medical device companies, healthcare supply companies, blood and organ banks, and healthcare insurance companies and other payers. This multitrillion dollar industry also includes US federal agencies such as the Department of Health and Human Services (DHHS), the Department of Veterans Affairs, and the Centers for Disease Control and Prevention. The private HPH sector employs 13 million people and the federal government another 450,000 people. All of these entities and people are potential targets for cyber attack.1

To help manage the potential risk of a catastrophic breakdown in the US healthcare infrastructure, the DHSS and its partners in the private sector and federal government developed the Healthcare and Public Health Sector-Specific Plan, which consists of four goals in different areas1:

1. **Service Continuity.** Maintain the ability to provide essential health services during natural disasters (eg, hurricanes), man-made disasters (eg, terrorism), or disruptions in the availability of supplies or support services (eg, power outages)

2. **Workforce Protection.** Protect the workforce from the harmful consequences of hazards that may compromise health and safety and limit the ability to fulfill responsibilities

3. **Physical Asset Protection.** Mitigate risks posed by all hazards to the physical assets of the HPH sector

4. **Cyber security.** Mitigate risks to the cyber assets of the HPH sector that may result in disruption to or denial of health services

This white paper addresses the last goal of cyber security by discussing the protection of the HPH sector against disruption and compromise of critical information technology (IT) networks, systems, and data, especially as they relate to mobile medical devices and electronic patient medical information (PMI).

1.2. Expansion of the Use of Mobile Devices in Healthcare

Mobile devices are everywhere. Digital technology in the form of smart phones, tablets, handheld personal digital assistants (PDAs), and iPads has transformed our daily lives and the way we communicate. The use of mobile devices is quickly expanding in healthcare settings because of technologic advances such as higher storage capacities, faster computing speeds, easier use, and better portability and connectivity.2 The HPH sector is taking full advantage of digital technology to enhance operations and lower costs.2 Digital healthcare infrastructures are bringing together the remote management, monitoring, and treatment of patients, affording better care.2 Wireless, or mobile, medical computing devices are connected to medical IT networks. Vice versa, IT networks
are remotely accessible through mobile medical devices. Consequently, because all PMI in these systems can be accessed remotely all of the time, all of these data are vulnerable.2

1.3. Types of Mobile Devices in Use in Healthcare

Three types of mobile computing devices are used in the healthcare industry2:

1. **Implantable Medical Devices.** Some medical devices are designed to be implanted in the body to collect, store, and analyze large amounts of data, and, ultimately, physicians act on that data. The capability of connecting to communications networks (connectivity) has been incorporated into implantable medical devices to increase their usefulness.

2. **External Medical Devices.** External medical devices, which are older versions of nonimplanted medical devices still in use, were designed as embedded systems with proprietary operating systems and little to no connectivity.

3. **Portable Devices.** Portable medical devices are being used by healthcare professionals in various direct patient care settings to discuss healthcare information (eg, test results) with patients in real time. These portable medical devices include smart phones, PDAs, and iPads. Another example of a portable medical device is wireless electrocardiography during which the patient monitor communicates with and continuously sends data gathered by the electrocardiogram machine to the hospital’s network, where the physician can monitor these data from anywhere at any time using a handheld device.

1.4. Federal Laws Related to Patient Privacy and Security in Healthcare

Protecting the privacy and security of PMI has been a major goal of healthcare facilities and providers since 1996 as they strive to comply with federal legislation (Health Insurance Portability and Accountability Act of 1996 [HIPAA]).7,8 Federal regulations (Patient Protection and Affordable Care Act [PPACA]) and state laws are in place to help secure patient electronic health records (EHRs) and electronic medical records (EMRs) (see Section 1.5) and to guide the adoption of health information technology (HIT).9 Health information technology (HIT) is defined as “the application of information processing, involving both computer hardware and software, that deals with the storage, retrieval, sharing, and use of healthcare information, data, and knowledge for communication and decision making.”10

1.5. Patient Medical Information: Electronic Health Records, Electronic Medical Records

EHRs and EMRs help to manage PMI more easily and seamlessly compared with paper records.3,4 An **EMR** is a digital version of a paper-based medical record for a patient that originates in a single facility, such as a physician’s office or clinic.11 A few different types of digitized health records, including EHRs, exist that contain most of the same types of information.11

An **EHR** is an official health record for a patient that is shared among multiple facilities and agencies.12 An EHR usually includes contact information, information on health insurance, a family history, and a list of medications the patient is taking, along with information about immunizations,
allergies, diseases or conditions, visits to healthcare practitioners, hospitalizations, and surgeries and other procedures that have been performed. Among the potential benefits of EHRs are the ability to automatically share information and multimedia (eg, medical imaging results) among different offices and entities, more efficient storage and retrieval of information, easier standardization of services and patient care, less redundancy, the provision of decision support systems to healthcare professionals, and the ability to link records to sources of relevant and current research.12
2. Who Poses Threats to Mobile Devices, What Are These Threats, and How Are They Carried Out?

Cyber security threats to mobile devices can be unintentional or intentional. Unintentional threats may be due to inadvertent disruption of systems caused by software upgrades or defective equipment, failure of technology because of inconsistent firmware, system crashes, different versions of software being used concurrently, and environmental hazards (e.g., power surges, fires, water leaks, and natural disasters).

Intentional threats include targeted and untargeted cyber attacks. The level of threat varies based on the attacker’s capabilities, willingness to act, and motives. The following five types of attackers pose threats to mobile devices:

1. **Botnet operators** send malware to mobile devices and other computer systems to coordinate attacks on websites and to distribute phishing e-mail, spam, spyware, viruses, and Trojans. Botnet operators may seek to gain monetarily or to cripple a competitor. In the first 6 months of 2006, almost 5 million botnet computers were active. Today, botnets remain a major security issue and pose the greatest threat to the Internet.

2. **Cyber criminals** gain access to information stored on devices using phishing, spam, spyware, and malware and use that information for monetary gain or to commit electronic fraud, identity theft, or extortion. Cyber criminals may also attack mobile devices to conduct industrial espionage and large-scale monetary and intellectual property theft.

3. **Hackers** may attack mobile devices to show their skill or gain prestige in the hacker community. However, hacking no longer requires computer skills. Hackers can now download attack scripts and protocols from the Internet and use them to launch attacks against mobile devices.

4. **Foreign governments** may attack mobile devices as part of information-gathering and espionage activities, with political goals of disrupting mobile communications, supply chains, or economic and other infrastructures that support homeland security and national defense.

5. **Terrorists** may seek to exploit, incapacitate, or destroy critical infrastructures such as mobile networks to damage public morale and confidence, weaken the US economy, or threaten national security. Terrorists also may use phishing schemes or spyware and malware to generate funds or gather sensitive information from mobile devices.
3. What Challenges Are Related to the Use of Mobile Medical Devices in Healthcare?

The more that systems become integrated, and the more they become connected to the Internet, the greater is the risk for compromise of those systems and data stored on them.\(^2\) Increased wireless interconnectivity introduces configuration challenges between mobile medical devices, the main medical IT infrastructure, any remote facilities, and any partner IT infrastructures.\(^2\) The portability and remote connectivity of medical devices pose challenges to providing safe pathways to and from medical IT networks to which these devices are connected, putting the privacy and security of patients at risk. Securing medical devices to protect against malicious intrusion and cyber theft, especially regarding PMI, are major concerns in the HPH sector.\(^2\)

Mobile devices can be compromised in various ways, including inadequate incorporation of IT products, patient management products, and medical devices into medical IT networks; misconfigured networks; and poor security practices. According to the DHHS, four factors further complicate cyber security in healthcare:\(^2\):

1. When a system is deployed, security design features may not be implemented due to the complexity of the technology or to a lack of knowledge about the capabilities of the system. When the technology being deployed is new, an authoritative understanding of how to properly implement security features may be lacking, and thus devices may be open to cyber attack because of, for example, insecure deployment configurations or zero-day vulnerabilities (which take advantage of security vulnerabilities before updates for them are available).

2. New or more robust features (eg, custom applications) may rely on an increased amount of code developed by third parties, which can create vulnerabilities.

3. Budgetary restraints may require that healthcare facilities focus on conventional programs and operational considerations rather than on the security of medical devices and networks.

4. System “owners” may be reluctant to allow access to manufacturers for upgrades or updates because once a medical device has been used, it contains private PMI.

The Food and Drug Administration (FDA) recently became aware of certain cybersecurity vulnerabilities and incidents that could have a direct negative impact on medical devices and hospital network operations. On June 13, 2013, the FDA issued a Safety Communication titled “Cybersecurity for Medical Devices and Hospital Networks” recommending that “…manufacturers and healthcare facilities take steps to ensure that appropriate safeguards are in place to reduce the risk of failure due to cyberattack, which could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings.”\(^16\) These cyber security vulnerabilities and incidents are as follows:\(^16\):

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smart phones, and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
• Uncontrolled distribution of passwords, disabled passwords, and hard-coded passwords for software intended for privileged device access (eg, for administrative, technical, and maintenance personnel);

• Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (called legacy devices);

• Security vulnerabilities in off-the-shelf software that is designed to prevent unauthorized access to devices or networks such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection (a technique used to attack data-driven applications).\^{16}
4. Why Are Mobile Devices Vulnerable?

Overall, mobile devices are subject to numerous security vulnerabilities. The following 11 vulnerabilities can be found on all mobile platforms:

1. **Passwords often are not enabled** to authenticate users and control access to data stored on devices.
2. **Two-factor authentication is not always used** when conducting sensitive transactions.
3. **Wireless transmission and receipt of data over a network are not always encrypted**, leaving data open to interception by eavesdroppers.
4. **Mobile devices may contain malware**, and it may be difficult for users to tell the difference between a legitimate application and one containing malware.
5. **Mobile devices often do not use security software** to protect against malware and spyware.
6. **Users do not always install security software**, possibly because it can slow operations of mobile devices and affect the life of the battery in some mobile devices.
7. **Operating systems may be out of date.** Security patches or fixes for operating systems of mobile devices are not always installed in a timely manner from manufacturers, or security patches may not be available for older devices.
8. **Software on mobile devices may be out of date.** Security patches for third-party applications are not always developed and released in a timely manner. Third-party mobile applications do not always notify consumers about updates. Unlike traditional web browsers, mobile browsers rarely receive updates.
9. **Mobile devices often do not have firewalls.** Without a firewall to limit ingoing and outgoing attempts to connect to the Internet, the mobile device may be open to intrusion.
10. **Mobile devices may have unauthorized modifications.** The modification of a mobile device to remove its limitations so that the user can add features (known as **jailbreaking** or **rooting**), or its modification so that the user is not tied to a particular wireless carrier, changes how security for the device is managed and could increase security risks.
11. **Communication channels may be poorly secured.** Having communication channels such as Bluetooth “open” or in “discovery” mode (allowing the device to be seen by other Bluetooth-enabled devices for connectivity) could allow cyber attackers to install malware or activate a microphone or camera to eavesdrop on the user. Using unsecured public wireless Internet networks or WiFi spots could also allow cyber attackers to connect to the device and view PMI.

In **two-factor authentication**, before being granted access users must “authenticate” with at least two different factors by answering questions about something the user knows (knowledge factor), possesses (possession factor), or is (inheritance factor).

A **firewall** is a set of related programs located at a network gateway server that protects the resources of a private network from users of other networks.
5. What Techniques Are Used by Those Initiating Cyber Threats to Mobile Devices and Networks?

Listed here are additional cyber techniques used to illicitly obtain information from or attack mobile devices and networks (see also Question 2)⁵:

- **Browser exploits** take advantage of vulnerabilities in software used to access websites. Visiting specific web pages or clicking on specific hyperlinks can install malware or perform other adverse actions on mobile devices.
- **Network exploits** take advantage of software flaws in systems that operate on local (e.g., Bluetooth and WiFi) or cellular networks and often can succeed without any user interaction, making them especially dangerous when used to automatically propagate malware. Cyber attackers can hijack users’ credentials and use them to impersonate a user online.
- **Keystroke logging** is a type of malware that records keystrokes on mobile devices to capture sensitive information, such as credit card numbers. Keystroke loggers may transmit the captured information to the website or e-mail of a cyber criminal.
- **Spoofing** hides the origin of an e-mail message by altering the sender’s address and other parts of the e-mail heading to appear as if it originates from a different source. Spoofed e-mails may contain malware.
- **Theft and loss** of mobile devices are common because they are small and portable, and gaining access to the information stored on these devices can be easy.
- **A denial of service (DoS) attack** is an incident in which a user or an organization is deprived of the services of a resource it would normally expect to have (e.g., a particular network service such as e-mail or the temporary loss of all network connectivity and services). In a distributed denial-of-service attack, large numbers of compromised systems (a botnet) attack a single target. DoS attacks usually do not result in information theft but can cost the targeted organization a great deal of time and money by interrupting service. DoS attacks also can destroy programming and files in computer systems. In the past, DoS attacks have forced websites accessed by millions of people to temporarily cease operations.¹⁸
6. What Activities by Users Make Mobile Devices Vulnerable?

Four basic activities by users make mobile devices vulnerable:\(^5\):

1. **Software downloads.** Unsuspecting users may download malware made to look like a game, device patch, or utility. Once the software is downloaded onto a mobile device, unauthorized persons can access the resources of the system and PMI.

2. **Malicious websites.** When users visit these websites, malware is downloaded either automatically or by an action taken by the user (eg, clicking on a hyperlink).

3. **Direct electronic attacks through the communications network.** Cyber attackers may try to intercept communications to obtain the use of mobile devices and access to PMI.

4. **Physical attacks.** Unauthorized persons may be able to access and use PMI stored on a lost or stolen device.

---

**Medical Identity Theft**

Almost 1.5 million Americans have been victims of medical identity theft, costing each an average of $20,500. In 64% of cases, the perpetrator was either a stranger conducting a cyber attack or an employee.\(^1\)
7. What Points of Contact in Healthcare Are Most Vulnerable to Loss of Electronic Patient Medical Information?

Three points of contact in healthcare are most vulnerable to cyber threat, especially related to PMI:\(^2\):

1. **Health insurance companies** handle the most sensitive data, including medical, personal, and financial information, which may be shared with physicians, pharmacies, third-party vendors, and others. The handling of sensitive information by so many entities has resulted in the theft of PMI. Medical identity theft may then lead to fraudulent claims by the criminal entity to the patient’s insurance company or may involve the selling of fraudulent prescriptions on the black market.\(^{19}\)

2. **EHRs and EMRs** are at risk when stored on laptops and mobile devices that are not encrypted. Internet connectivity is required to send EHRs and EMRs, which would be in response to a request by a patient or physician. A major threat to EHRs and EMRs is unauthorized access by insiders. Compromise of EHRs and EMRs can lead to loss of patient trust, a violation of HIPAA, and actual loss of the medical practice or business.\(^2\)

3. **Physician group practices** are where most people receive primary healthcare services and, because these group practices tend to be small groups, they may be the least able to properly configure and regularly maintain their networks.\(^2\)
8. What Are the Most Common Ways That Electronic Patient Medical Information Is Lost or Stolen?

Electronic PMI is lost or stolen in three main ways:

1. **Loss of personal devices:** Once a personal device (e.g., smart phone, iPad, PDA, or USB) is used to access PMI, all of that information is at risk if the device is not encrypted or is not password-protected and is subsequently lost or stolen. One USB drive can hold 25,000 patient records. If the loss of this many patient records would occur at a hospital, the resulting penalties would be more than $6 million because hospitals are held liable when employees compromise PMI because of theft or loss.

2. **Loss of equipment:** Loss or theft of equipment containing PMI occurs frequently and has severe consequences. Because PMI is increasingly being stored in electronic format (EHRs and EMRs), when a security breach occurs or when electronic media is stolen the number of individuals affected by each occurrence also increases. The Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009, requires that when a breach of PMI is discovered the covered entities and business associates must notify various parties—the affected patients, the Secretary of the DHHS, and in some cases the media—to ensure that appropriate steps are taken to mitigate the consequences of the breach, avoid similar incidents in the future, and promote public transparency.

3. **Loss through insiders:** Replacement of portable devices, employee turnover, and the availability of data stored in cloud computing systems create opportunities for insiders seeking to steal data. Data can be transferred easily, quickly, and without detection using portable devices or by uploading to the "cloud." The most common method of data exfiltration by insiders involves the transfer of information from the network by e-mail, a remote access channel, or computer files.
9. What Steps Can Be Taken to Secure Mobile Medical Devices, Networks, Users, and Patient Medical Information?


One effective effort that organizations in the HPH sector can make to reduce the risk of compromised PMI is to have in place and educate employees about security policies, procedures, and processes.2,6

- Make employees aware of whether personal mobile devices are allowed or prohibited on the network.
- Provide training on policies for medical devices so that employees clearly understand what is and what is not acceptable.
- Educate employees on the password policy.
- Inform employees about the types of malware and phishing scams they may be targets of because of their knowledge of and access to PMI.

IT administrators in the HPH sector can reduce the risk to patients who rely on a medical device and can help to ensure that EHRs and EMRs are secure through established policies and procedures.2

- Put into place a solid overall strategy for securing medical devices used by medical professionals for patient care that encompasses all mobile devices used by the organization, not just those connected to the network.
- Provide access to EHRs and EMRs only to personnel who require access.3
- Regularly monitor the access by personnel to EHRs and EMRs using logs, to ensure that access privileges are not being misused.
- Use robust measures such as encryption and authentication to deter cyber attackers. An encryption policy for medical devices should be in place to protect devices and to add another layer of security in the event of loss or theft. Encryption methods should include information that is transmitted both to and from medical devices.
- Maintain a firewall for medical devices connected to networks. Many existing medical devices were designed with embedded operating systems, so most current cyber attacks cannot affect them. However, new devices are increasingly being configured with commercial operating systems, which can be susceptible to malware and viruses if left unprotected.

---

**Password Checklist**

- Policies should be in place for passwords, and all staff members should understand and agree to these policies.
- Passwords should be at least eight characters long.
- Each password should contain both upper and lower case letters, one number, and at least one special character (e.g., a punctuation mark).
- Passwords should be unique to individuals.
- Passwords should be changed quarterly.
- Passwords should not include words that can be found in a dictionary, even when altered (e.g., by replacing a letter with a number).
- Passwords should not include personal information (e.g., birth date; names of self, family members, or pets; social security number).
- Passwords should not include any information that is posted on social media sites.
- Passwords should not be reused.
- Passwords should not be revealed to or shared with others.
IT administrators can also implement controls for organizations to protect networks, computers, mobile devices, users, and thus, PMI:\footnote{5}:

- Adopt centralized security management to ensure that mobile devices are compliant with the security policies of the organization.
- Use mobile device integrity validation software tools to scan devices for key compromising events. These tools report the results of the scan, including the risk rating and recommended mitigation.
- Implement a virtual private network (VPN) to provide a secure communications channel for sensitive data transferred across multiple public networks during remote access. VPNs provide a way to secure wireless local networks, such as those at public WiFi spots and in homes.
- Use public key infrastructure support services. Public key infrastructure (PKI) is a system of hardware, software, policies, and individuals that can provide a suite of information security assurances (confidentiality, data integrity, authentication, and nonrepudiation) that are important in the protection of sensitive communications.
  - Require conformance with government specifications.
  - Install a firewall to isolate all unapproved traffic to and from mobile devices.
  - Monitor traffic entering the network from mobile devices using intrusion prevention software.
  - Monitor and control devices for messaging, data leakage, and inappropriate use, and to prevent illicit applications from being installed.
  - Enable, obtain, and analyze device log files to detect suspicious activity and ensure compliance.

\textbf{9.1.1. Healthcare Facilities}

On June 13, 2013, the FDA issued a Safety Communication titled “Cybersecurity for Medical Devices and Hospital Networks,” in which it recommended that steps be taken to evaluate network security and protect hospital systems. “In evaluating network security, hospitals and health care facilities should consider [see also Question 3]\footnote{16}:

- Restricting unauthorized access to the network and networked medical devices.
- Making certain antivirus software and firewalls are up-to-date.
- Monitoring network activity for unauthorized use.
Access Control Checklist
- Policies should be in place for control of access, and all staff members should agree to abide by these policies.
- Every user account should be positively tied to a currently authorized individual.
- Users should be authorized to access only information that they need to know to perform their duties.
- All files should be set to restrict access to unauthorized individuals.
- Computers that are running healthcare-related systems should not be available or used for other purposes.

Physical Control Checklist
- Policies should be in place for the physical safety and security of all devices, and all staff members should agree to abide by these policies.
- All devices containing EHRs and EMRs should be inventoried and accounted for.
- Computers should be protected from current and potential environmental hazards.
- Only authorized individuals should have physical access to secure areas where computer equipment is located.
- Computers running EHR systems should be shielded from the view of unauthorized persons.
- Equipment located in high-traffic or less secure areas should be secured physically.

- Protecting individual network components through routine and periodic evaluation, including updating security patches and disabling unnecessary ports and services.
- Contacting the device manufacturer for cyber security problems related to medical devices...
- Developing and evaluating strategies to maintain critical functionality during adverse conditions. 16

Healthcare facilities, and other organizations in the HPH sector, should put into place a layered security approach using the following suggested best practices2:
- Operate and maintain the following:
  - External-facing firewalls
  - Network monitoring techniques
  - Intrusion detection techniques
  - Internal network segmentation
- Establish and enforce strict policies for the following:
  - Passwords
  - Software upgrades
  - Routine maintenance, review, and audit of network configurations.
  - The connection of all devices, particularly those that are wireless (including laptops, tablets, USBs, smart phones, PDAs, and iPads) to the network so that no access is provided to unsecured or unrecognized devices.
- Use only networked medical devices that have well-documented, fine-tuned security features and that IT administrators can configure safely on their networks.
- Use vendor support for ongoing firmware, patches, and antivirus updates as a suitable risk-mitigation strategy.
- Implement safe, effective, legal patches for networks that support regulated medical devices.
- Use encryption and authentication to secure incoming and outgoing communications channels, especially wireless ones.
- Use the “principle of least privilege” to decide which accounts need access to specific medical device segments, rather than providing access to the entire network.
- Configure access control lists (ACLs) on network segments so that only authorized accounts can access network segments.
9.2. Actions Users Can Take to Protect and Secure Mobile Devices

Users can take some general key security practices to combat common cyber threats and vulnerabilities:

- Maintain physical control by keeping the device secured.
- Limit the following:
  - Use of public WiFi networks
  - Exposure of mobile phone numbers
  - Storage of sensitive information on mobile devices
  - Installation of unnecessary applications
- Do not do the following:
  - Follow links sent in suspicious e-mails or text messages
  - Click on suspicious advertisements in an application
  - Modify mobile devices; doing so can prevent the receipt of security updates or expose devices to security vulnerabilities
  - Turn off or set Bluetooth connection capabilities to “nondiscoverable,” so that Bluetooth-enabled devices are invisible to unauthenticated devices

The federal government is making efforts to increase awareness about mobile security in the public and private sectors. According to a brochure made available at HealthIT.gov titled “Using a Mobile Device. How to Protect and Secure Health Information,” there are different ways of securing mobile devices at different locations.

9.2.1. Public Spaces

Among key practices that should be used in public spaces to protect and secure mobile devices are the following:

- Maintain physical control by keeping the device secured.
- Use a privacy screen shield or keep your back to a wall to protect the screen from the view of others.
- Never use an unsecured public Wi-Fi network to access, transmit, or receive PMI; use a VPN or other secure connection to connect to the private network or system of an organization.
- Always keep your mobile device with you.

9.2.2. Remote Locations

Key practices to protect and secure mobile devices in remote locations include the following:

- Maintain physical control by keeping the device secured.
- Lock the screen of your mobile device.
Keep the device in a secure location when not in use.
Use a privacy screen shield or keep your back to a wall to protect the screen from the view of others.
Follow the instructions provided by the manufacturer to secure your home Wi-Fi network. Change the default administrator passwords and user names.
Make sure the firewall for your router is turned on. For additional protection, install and run personal firewall software on each mobile device connected to the router.
Use a VPN or other secure connection to connect to an organization’s PMI system or other private network.

9.2.3. Healthcare Facilities, Hospitals, and Healthcare Offices
Among key practices that should be used at healthcare facilities, hospitals, and healthcare offices to protect and secure mobile devices are the following:
- Use a password or other user authentication to log on to the mobile device.
- Protect the mobile device screen from the view of others.
- Lock the screen of your mobile device when not in use.
- Keep the mobile device with you.
- Set your mobile device preferences to automatically either log off or lock the screen after a short period of inactivity.

9.3. Establishment of a “Security Culture” in Healthcare

Protecting PMI through good data security practices should be second nature in every organization in the HPH sector. A serious commitment to protect and secure network architecture at the top levels of the company is no longer an option. A culture that is security-minded must be instilled and supported by the organization, and every person in the organization should have a shared vision of the protection and security of PMI.

Security professionals are unanimous that the weakest link in any computer system is the user. One challenging aspect of instilling a security focus is overcoming the perception by users that only “other people” put PMI at risk. Regardless of the level of education or IT sophistication, people are alike in believing that they would never compromise PMI; nevertheless, it happens.

A basic first step in making security a priority is to include responsibility and accountability for the safety of PMI in the core values of the organization. Employees should be provided with frequent and ongoing education and training about the electronic computing devices that they are using and the associated processes and procedures. Finally, those who manage and direct the work of other employees must set a good example and resist the temptation to indulge in making “exceptions to the rule.”
In June 2013, Dimensional Research conducted a survey for Check Point Software titled “The Impact of Mobile Devices on Information Security,” with somewhat alarming results that deserve mention and provide a cautionary tale. When surveyed, IT professionals in various types of organizations reported the following:

- 93% have mobile devices connecting to their corporate networks
- 79% reported mobile security incidents in the last year
- 67% see securing electronic corporate information as the greatest “bring-your-own-device,” or “BYOD” challenge
- 66% view careless employees as a greater security risk than cyber criminals
- 63% do not manage the flow of corporate information on personal devices

In addition, the results of monitoring traffic for 120,000 hours in 900 companies revealed the following major security risks that organizations are exposed to daily:

- 75% of the organizations’ personnel visited malicious websites
- 63% of the organizations’ computers were infected with “bots”
- 54% of organizations had at least one potential data loss incident
- 36% of financial organizations sent credit card information outside of the organization
- **16% of healthcare and health insurance organizations sent HIPAA-protected PMI outside of the organization**
CONCLUSION

Waves of various types of improvements in digital technology have expanded the use of mobile medical devices in the HPH sector. The advantage of having all PMI available all of the time, however, has put PMI at increased risk because of the vulnerabilities inherent in computing systems. Federal and state laws protect the privacy and security of PMI; therefore, the entire HPH sector must be proactive and vigilant about maintaining patients’ privacy and security when it comes to both paper and electronic records.

On June 13, 1993, the FDA issued a Safety Communication on “Cybersecurity for Medical Devices and Hospital Networks” because of new awareness of cyber security vulnerabilities and incidents that could have a direct negative impact on these devices and networks. This action by the FDA again raised the alarm about privacy and security issues regarding PMI accessed by computing devices or stored on networks. The FDA made the following recommendations: restrict unauthorized access to these devices and networks, ensure antivirus software and firewalls are up-to-date, monitor network activity for unauthorized use, routinely evaluate individual network components, contact the device manufacturer about security problems related to a medical device, and develop and evaluate strategies to maintain critical functionality during adverse conditions.

In addition to these recommendations, this white paper provides specific steps that can be taken to secure wireless devices, networks, users, and PMI. Also included herein are checklists for passwords, firewalls, antivirus software, access control, physical control, and mobile device control for use by IT administrators and users.

Concerted and continuous efforts by all parties involved will be required to protect and secure electronic PMI. A serious commitment to protect and secure network architecture at the top levels of organizations in the HPH sector is required. A security-minded culture using best practices should be instilled and supported by organizations, and everyone working in those organizations should subscribe to a shared vision of protection of PMI.
REFERENCES


