Mobile Device Security (Updated) - Retired

Save to myBoK

Editor's note: This brief supersedes the June 2003 and October 2000 practice briefs "Portable Computer Security."

Mobile devices have pervaded the everyday work environment in healthcare. An organization may use mobile devices to improve clinician workflow, bedside information gathering and reporting, or a host of other care delivery applications. In some cases, individuals may use their own mobile devices to meet their personal workflow requirements.

Whatever purpose the device serves, healthcare organizations must be prepared to understand all the issues related to mobile device use.

This practice brief reviews the legal and regulatory requirements that affect mobile device use in healthcare. It also provides best practices for ensuring appropriate safeguards are in place to protect all electronic protected health information (ePHI) used and processed within mobile devices.

Mobile Device Risks

Mobile devices come in a variety of forms, processing capabilities, and wireless accessibility. These devices include, but are not limited to, laptop computers, smart phones, USB thumb drives, external hard drives, tablet computers (e.g., iPad, Motorola Xoom), and even e-readers like the Kindle or the Nook.

Deploying mobile devices within a healthcare organization can pose several risks. Although mobile devices often contain sufficient storage space to easily accommodate massive amounts of ePHI, they are produced for consumer use and seldom incorporate technology to allow the device to be managed within a corporate "enterprise" IT environment. Consumer devices lack the inherent security and operational controls to enable management of the device from a centralized system. As a result, incidents can arise from not being able to adequately detect, manage, or provision and de-provision the device.

In addition, mobile devices are easily lost or stolen and thus pose increased risks to the confidentiality and security of patient health information. Loss or theft of a device could easily result in the need for patient breach notification and subsequent reporting to the Department of Health and Human Services and media as required under the American Recovery and Reinvestment Act.

Mobile Device Legal and Regulatory Requirements

When deploying and using mobile devices, organizations and providers must review the following legal and regulatory requirements in order to remain compliant.

HIPAA

HIPAA requires that protected health information (PHI) be safeguarded against threats to security, integrity, and unauthorized use.

Section 164.310 includes several references to workstations. It specifically requires that a covered entity "implement physical safeguards for all workstations that access ePHI to restrict access to authorized users" and "policies and procedures that govern the receipt and removal of hardware and electronic media containing ePHI into and out of a facility as well as the movement of these items within the facility."

HIPAA also mandates that covered entities implement policies and procedures addressing the "final disposition of ePHI and/or the hardware or electronic media on which it is stored" and the "removal of ePHI from electronic media before the media are made available for re-use."

In addition, it requires covered entities "maintain a record of the movements of hardware and electronic media and any person responsible therefore" and "create a retrievable, exact copy of ePHI, when needed, before movement of equipment."

Section 164.312 mandates that a covered entity "implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the 'administrative safeguards' section" (164.308). To do this, a covered entity must initiate four implementation specifications:

- Unique user identification (required): the entity must "assign a unique name and/or number for identifying and tracking user identity"
- Emergency access procedure (required): an entity must "establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency"
- Automatic log-off (addressable): the entity must "implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"
- Encryption and decryption (addressable): the entity must "implement a mechanism to encrypt and decrypt ePHI" as needed

ARRA and HITECH

The Department of Health and Human Services' interim final rule for breach notification of unsecured protected health information went into effect September 23, 2009. Section 13402(h) of the HITECH Act defines unsecured protected health information as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary."

As required by HITECH, the HHS secretary specified encryption and destruction as technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that breach notification would not be required.

Furthermore, HITECH refers to the National Institute of Standards and Testing (NIST) as a source for encryption standards, specifically the Federal Information Processing Standard 140-2. FIPS 140-2 identifies requirements for specific encryption algorithms and modules that are tested and approved to protect information ranging in various levels of sensitivity. Healthcare organizations should look for IT products that state conformance with FIPS 140-2.

Note: At press time, the interim final rule is still in effect. A final rule is expected later this year. Organizations are expected to meet the requirements of the current interim rule as well as the final rule, once the final rule is published and becomes effective.

Individual State Law

Individual states may have laws or regulations that require health information to be protected against threats to security, integrity, and unauthorized use. In some cases, state laws may be more stringent than federal law, in which case a preemption analysis must be applied.

For example, many states have laws with specific requirements and protections related to "high risk" records such as mental health, HIV, and substance abuse/treatment records. Legal counsel should be consulted for proper guidance in preemption decisions.

Medicare Conditions of Participation

The Medicare Conditions of Participation for healthcare facilities also address information security and include the following requirements:

- Hospitals "must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records."
- Home health agencies must ensure "clinical record information is safeguarded against loss or unauthorized use."

- Residents of state and long-term care have "the right to personal privacy and confidentiality of his or her personal and clinical records."
- Comprehensive outpatient rehabilitation facilities "must safeguard clinical record information against loss, destruction, or unauthorized use."
- A critical access hospital "maintains the confidentiality of record information and provides safeguards against loss, destruction, or unauthorized use."

Privacy Act of 1974

The Privacy Act of 1974 mandates that federal information systems protect the confidentiality of individually identifiable data. Section 5 U.S.C. 552a (e) (10) of the act states that federal systems must "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

Code of Federal Regulations Related to Alcohol and Drug Abuse

The Code of Federal Regulations relative to alcohol and drug abuse, 42 CFR, chapter I, part 2, section 2.1, states that records of the identity, diagnosis, prognosis, or treatment of any patient that are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall be confidential and disclosed only for the purposes and under the circumstances expressly authorized.

Accreditation Standards

The Joint Commission's standards for hospital and ambulatory care (IM.02.01.01 and IM 02.01.03) state the hospital "protects the privacy" and "maintains the security and integrity" of health information.

Mobile Device Best Practices and Recommendations

Mobile devices present numerous management challenges to the ePHI they carry and transmit. Some of the more critical challenges include increased privacy and security risks to the data and increased theft or loss of the device, which can lead to breaches and unintentional harm to the patient.

However, such risks can be minimized by establishing appropriate controls and implementing the necessary measures for optimal health information protections. It is also imperative that organizational policies and procedures are clearly communicated and enforced for all workforce members to establish expectations and convey accountability.

In terms of establishing appropriate controls and implementing necessary measures, healthcare organizations must, at a minimum, establish written policies and procedures covering the use of mobile devices that address the following issues:

Device ownership. If personal devices are permitted for business use, organizational policy must define the conditions that must be met and how compliance will be verified. For example, policies and procedures should consider the following in the event personal devices will be allowed:

- Annual agreement and signing of the organization's "rules of behavior" (see below)
- Requirements for password protection
- Lock-out features and specifications
- Appropriate use of texting
- Appropriate use of camera and video
- Appropriate use of sensitive information
- Alteration of factory defaults and operating systems (i.e., jail-breaking)
- Appropriate use of applications and conditions of downloading software
- Reservation of rights by the healthcare facility to examine the system for compliance and investigation of incidents
- Procedures during employee or contractor termination

A clear definition of data ownership. Organizational policies must clearly define data that belong to the organization and data that may belong to the individual user. Clinicians and organizations may sometimes differ in their respective viewpoints

regarding what patient data belong to the organization and which may belong to the clinician. Such issues must be resolved and appropriate controls established to safeguard ePHI appropriately.

Required written authorization by the HIM director or the privacy and security officers when mobile devices are to be used to collect or maintain patient health information; for example, the requirement for each user to sign a "rules of behavior" agreement.

Conditions under which it is appropriate to use a mobile device. Mobile device users should refrain from transporting sensitive patient information on a mobile device unless an approved workflow is in place for the specific use in question. For instance, it may be appropriate to configure some devices for direct access to a patient care system. This does not mean it is appropriate for all mobile devices to access the system.

Rules of behavior and expectations for acceptable use of mobile devices. Such rules may cover specific expectations such as not using mobile devices to photograph patients, visitors, staff, and facilities. The rules of behavior should also specifically communicate expectations regarding the use of mobile devices by physicians (including outside physicians), contractors, and other non-employees.

Organizations should be sure to cover policy expectations related to the use of social media and social networking on mobile devices. Organizations often have such policies for use inside the facility and often forget to address them in the mobile environment.

Appropriate technologies and techniques for the destruction of sensitive information after use on the device. This should include a time period for destroying the information and the use of a safeguard that can verify the status of the information on a device (specifically mobile device management software).

Appropriate identification of what constitutes sensitive information. Sensitive information is any information that may identify a patient and a particular treatment or diagnosis. Often clinicians will think in terms of an entire medical record being sensitive, while small components are not. It is important to define the term within the organization's policy as a method to establish a common definition as to what constitutes sensitive information.

For example, a text file containing only a name and medical record number may not be considered sensitive if it is labeled "Today's List." It may take on a different level of sensitivity should it be identified as "Today's Cancer Treatment Appointments."

Specific procedures for the reporting of device loss or theft. Each organization should educate its workforce members on how to report loss or theft of a mobile device. Users should note and store the serial numbers for all electronic devices they may possess and store them in a secure location. Such numbers increase the likelihood of finding a device if it is stolen.

In the event of a loss or theft, users should immediately make notes regarding the incident and what took place. These notes will come in handy during the ensuing investigations.

Organizational procedures should detail who to call, what hours to call, and the expected details needed to properly document the incident. A police report should always be made in the event of incident and forwarded to the incident investigation team.

Organizations should consider tools that allow mobile devices to be inventoried for sensitive data. Such inventories will aid investigators when attempting to determine if a breach occurred.

Appropriate data management techniques involving the use of sensitive information on a mobile device. Healthcare organizations should determine and distribute information governing such things as creation of "sole source or unique data," back-up expectations and procedures, transfer of information to and from the device, and how to securely erase traces of sensitive information from the device. Additional considerations should include roles, responsibilities, and expectations regarding access to corporate resources such as e-mail, calendars, and distribution and contact lists.

In addition organizations must set clear workforce accountability and expectations regarding the use of mobile devices. They must:

- Require that employees be familiar with the organization's policies and procedures relative to the appropriate use of mobile devices prior to being assigned mobile equipment.

- Require that employees be familiar with the facility's policies and procedures relative to confidentiality of patient health information.
- Educate employees about the potential risks caused by computer or information theft or loss.
- Require all users sign a copy of the policy statement or guidelines for mobile devices prior to being allowed to use or synchronize a device.
- Educate the employee on how and when to appropriately back up the data on the device. Data should not be backed up to personal workstations, cloud technologies, or other mobile devices.
- Limit the use of the assigned mobile device to the designated employee. Maintain a current list of mobile device users and borrowers, assigned equipment serial numbers, and software. Hold the computer borrower responsible and accountable for the safety and security of the assigned equipment and information.
- Develop sanction policies and educate employees on the sanction policies before the employee is allowed to use or synchronize a device. Make sure the sanction policies apply regardless of device ownership.

Avoid maintaining PHI on mobile devices. Instead, organizations should store the information on the facility's network so the information can be backed up and maintained more securely. When network storage is not possible, information should be encrypted to protect it from unauthorized access should the device be lost or stolen.

Depending on the size of the facility and degree of technical support, it is advisable to consider remote connections from the mobile device to virtual systems within the data center.

Routinely scan mobile devices to ensure safeguards are present and operating, such as operating system and application patches and updates. Some mobile devices may distribute "firmware" upgrades instead of an operating system update. Such devices should be appropriately updated when new software is available. Applications installed on the device should also be checked frequently for updates and the updates installed to reduce exposure of application vulnerabilities.

Organizations must also routinely scan their mobile devices to ensure virus signature files and antivirus engines are up to date.

Organizational password policies should follow the same recommended best practices as computer workstations and server systems. Organizations must ensure that passwords are being used and are not written on the device. They should require the use of strong passwords of at least seven to eight characters, including alphanumeric and special characters.

In the mobile environment, password protections should include automatic device shutdown after multiple unsuccessful log-in attempts. Such protections can wipe the device back to a factory state in the case of loss or theft.

Incorporate appropriate encryption for each device in use. Not all mobile devices support encryption or can be encrypted effectively enough to be used with patient information. Developing use cases will provide an organization with the information needed to establish what devices can be used to transport or handle sensitive information and the type of encryption tools to use. For example, the device may be able to utilize an encrypted container to hold e-mail, while not providing sufficient encryption to meet the need for transporting sensitive files.

Regularly audit policies, procedures, and assigned equipment and software lists. Like other IT technologies, mobile devices should be routinely audited for security controls. Organizations should consider methods for routinely auditing such devices. This may take the form of tool sets that constantly monitor the device for compliance to policy, reporting back to a central server, or the recall of randomly selected devices for personal inspection and compliance evaluation. Some organizations (depending on size and complexity) may chose to do both.

Additional considerations for safeguarding mobile devices and related ePHI include:

Encryption. Organizations should purchase and install a suitable "whole-disk" encryption product for mobile devices such as laptop computers. Not all mobile devices can support encryption products. An organization must determine if the mobile device can support encryption and in cases where encryption is not available, evaluate the risks of using the device.

Organizations should ensure encryption products have a central key management infrastructure to enable the recovery of encryption keys. Central key management is critical if the organization has to recover information from a device. If an employee leaves the organization without releasing the encryption keys, the only hope for recovery of the encrypted information is from the central key depository.

In addition, organizations should consider the type of mass storage device and the availability of encryption. They should look for devices that provide hardware-based encryption and do not require administrative rights on the host computer in order to operate. This is critically important for staff that travel and may need access to the device from a coffee shop or hotel computer.

Software-encrypted devices usually require software to be loaded from the portable device onto the host system (in this example, the coffee shop or hotel computer). Such host systems are generally "locked down" to deny the operation of such applications, resulting in the inability to access the software-encrypted mobile device.

Hardware-encrypted devices perform the encryption function within their own hardware, without the need to execute code on the hotel or coffee shop system.

Organizations should also make sure the use of any encryption technology is compliant with NIST and FIPS 140-2.

Tracking software with capabilities to remotely wipe the device if it is lost or stolen. When purchasing mobile devices, organizations should consider vendors with local repair facilities to avoid potential theft or loss during shipment to or from the factory when devices are sent for repair. Local repair facilities should complete a business associate agreement or similar agreement if they are to service mobile equipment.

In the event equipment must be sent off site to a manufacturer for repair organizations should consider the following:

- Removing the hard drive prior to return. This would be advisable if the support issue is a repair item other than the hard drive.
- If the equipment is being returned as part of an equipment exchange or trade in, work with the vendor to keep the hard drive. Dispose of the hard drive using an acceptable destruction method such as a NIST-approved secure overwrite method, magnetic degaussing, or physical destruction of the hard drive. The best practice technique would be a physical destruction of the drive in such a way it could not be reconstructed (shredding or crushing the drive).
- Return the equipment through a delivery service that will properly record the signature of the receiving party and will not leave the parcel unattended.

User and device controls. Organizations should purge user data on mobile devices after each use and prior to assigning to the next user. Use NIST-approved secure deletion tools. Simply deleting data does not necessarily eliminate it.

Organizations should restrict workstation access to organizationally approved devices, based on the analysis from the above steps. They should audit for compliance and review policy decisions as the market for these devices changes frequently.

In addition, facilities should restrict the use of CD/DVD writers. They should consider the use of self-contained encryptable CD/DVD media in areas that have a legitimate need to create CD/DVD materials.

Secure mobile devices when not in use, including offices and meeting rooms when equipment is left unattended. Arrange the devices so they are not readily observable.

Inventory. Organizations should inventory the use of USB mass storage devices. They should consider products that can run on workstations and other computer devices that can audit the movement of data to and from a USB device. Many such products can also control USB port usage based on policy.

Organizations should also examine all avenues of product acquisition of mobile devices. If there are purchasing contracts with vendors for mass storage devices, collaborate to enforce the organization's choice of mass storage products.

In addition, facilities should analyze inventory findings for the types of devices being used and the types of data being moved among the devices. Some of the port tools that audit and allow control of USB devices on workstations and laptops can also make shadow copies of the actual data moved between them. This can be an enormous asset to determining the type of data and usage patterns for mobile devices and media.

Organizations should centralize the oversight for media destruction and reallocation where possible. Media destruction and disposal should be cross-referenced to inventory and appropriately tracked.

Theft/Loss. Organizations should perform loss investigations on all lost or stolen equipment. They should also create an incident response team and conduct exercises to prepare for the possibility of lost or stolen devices.

Part of this incident response plan should include plans to deal with breach notifications in compliance with the breach notification rule. In such cases, it may be necessary to identify the data that were lost in order to ascertain who will need to be notified.

Members of the incident response team should include (but are not limited to) risk management, corporate compliance, media relations, legal, and representatives of senior management.

In terms of theft awareness and education, it is critical for healthcare facilities to ensure the organization's media cleaning and destruction policies and procedures consider all types of media and educate the workforce on the proper handling of each. They should also provide employees with computer and data theft precaution and deterrent information. Examples might include instructions to:

- Avoid using mobile devices where they can be easily stolen.
- Transport mobile devices in a car's trunk rather than on a seat, thereby keeping it hidden (i.e., do not leave mobile devices in a visible location inside a vehicle).
- Carry mobile devices in something other than a readily identifiable computer carrying case.
- Use only encrypted external drives if data transport outside the device is required.
- Place mobile devices on an airport conveyor after clearing the metal detector (when possible). Unless specifically requested to remove a mobile device other than a laptop from a carry-on bag during screening, leave the device in the bag. This will reduce the likelihood of the device being stolen or left behind in the screening area.
- Place unattended mobile devices in room safes when leaving a hotel room. (Some hotel room safes include an AC adapter so that the computer can be recharged while locked away.)
- Remove portable devices from their docking stations in offices and lock them in a desk drawer or cabinet.
- Lock the room or place the mobile device in a laptop depository when leaving a mobile device in an unattended meeting room. (A laptop depository is a portable safe in which computers can be placed. An alarm will sound if the depository is moved after it is closed.)

In addition, facilities should train staff on how to report the loss or theft of a mobile device and designate who they should contact and the importance of timely notification. If the device is stolen during travel, have the local police complete an investigation report immediately. Organizations should take this as an opportunity to develop policies and procedures for incident response and management.

In terms of making investments in electronic accessories that will minimize the risk of theft, facilities should provide employees with the best accessories available to protect their mobile devices and require use of these devices. Examples of these electronic accessories include:

- Carrying cases that do not appear to contain computers.
- Cables that lock to desks or tables and that once removed do not allow a thief to turn the computer on.
- Lockdown enclosures, proximity alarms, and software programs that instruct computers to "phone home" to report their location.
- Appropriate password, security, and encryption programs.
- An anti-theft plaque or etching tool to engrave the company name/ID on all portable computers. (Some anti-theft plaques contain a metallic bar code and registration number. If a thief tries to pry off the plaque, the computer casing will be damaged, decreasing the resale value. If the thief succeeds in removing the plaque, the computer will still bear the imprint of the words "Stolen Property" on its shell.)
- Tracking software that can remotely erase the mobile device.

References

American Recovery and Reinvestment Act of 2009. Section A, Title XIII, Health Information Technology. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf.

Briggs, Bill, ed. *Comprehensive Guide to Electronic Health Records.* New York, NY: Faulker and Gray, 2000.

Centers for Medicare and Medicaid Services, Department of Health and Human Services. "Medicare Conditions of Participation for Hospitals." Code of Federal Regulations, 2004. 42 CFR Ch. IV.

Department of Health and Human Services. "Breach Notification for Unsecured Protected Health Information; Interim Final Rule." *Federal Register* 74, no. 162 (Aug. 24, 2009). http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.

Department of Health and Human Services. "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009; Request for Information." April 27, 2009. www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf.

Department of Health and Human Services. "Health Insurance Reform: Security Standards; Final Rule." *Federal Register* 68, no. 34 (Feb. 20, 2003). http://aspe.hhs.gov/admnsimp/final/fr03-8334.pdf.

Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 67, no. 157 (Aug. 14, 2002). www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrulepd.pdf.

The Joint Commission. *2012 Comprehensive Accreditation Manual for Ambulatory Care.* Oakbrook Terrace, IL: Joint Commission, 2012.

The Joint Commission. *2012 Comprehensive Accreditation Manual for Hospitals: The Official Handbook.* Oakbrook Terrace, IL: Joint Commission, 2012.

Updated By

Terrell W. Herzig, CISSP, MSHI

Acknowledgments

Carrie Ayala, RHIT, CPC-I
Barbara Beckett, RHIT
Sheila Burgess, RHIA, RN
Ben Burton, JD, MBA, RHIA, CHP
Jill S. Clark, MBA, RHIA
Linda Darvill, RHIT
Nancy A. Davis, RHIA
Angela K. Dinh, MHA, RHIA, CHPS
Cris V. Ewell, PhD
Lisa R. Fink, MBA, RHIA, CPHQ
Jean T. Foster, RHIA
Elisa R. Gorton, MAHSM, RHIA
Judi Hofman, CAP, CHP, CHSS
John T. Jensen, CHPS, CIPP
Priscilla Komara, RHIA, CCS, CCS-P
Michele T. Kruse, MBA, RHIA, CHPS
Laurie A. Lutz, RHIA, CHPS
Melissa Martin, RHIA, CCS
Jennifer McCollum, RHIA, CCS
Kelly McLendon, RHIA, CHPS
Mona Nabers, MBA, RHIA
Godwin O. Odia, PhD, RHIA, NHA
Deanna Peterson, MHA, RHIA
Daniel J. Pothen, MS, RHIA, CPHIMS
Mary Poulson, MA, RHIT, CHC, CHPC
Nancy E. Prade, RHIA
Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA
Theresa Rihanek, RHIA, CCS
Diana Warner, MS, RHIA, CHPS, FAHIMA

Lydia M. Washington, MS, RHIA, CPHIMS
Lou Ann Wiedemann, MS, RHIA, CPEHR, FAHIMA

Updated By (2003)

Carol Ann Quinsey, RHIA

Prepared By (Original)

Gwen Hughes, RHIA

The information contained in this practice brief reflects the consensus opinion of the professionals who developed it. It has not been validated through scientific research.

Article citation:
AHIMA. "Mobile Device Security (Updated) - Retired." *Journal of AHIMA* 83, no.4 (April 2012): 50-55.
