Security Issues for Mobile Medical Imaging: A Primer[1]

Asim F. Choudhri, MD
Arindam R. Chatterjee, MD[2]
Ramin Javan, MD
Martin G. Radvany, MD[3]
George Shih, MD[3]

RadioGraphics 2015; 35:1814–1824

Published online 10.1148/rg.2015140039

Content Codes: IN SQ

[1]From the Departments of Radiology (A.F.C., A.R.C.), Ophthalmology (A.F.C.), and Neurosurgery (A.F.C.), University of Tennessee Health Science Center, Memphis, Tenn; Department of Radiology, Le Bonheur Neuroscience Institute, Le Bonheur Children's Hospital, Memphis, TN 38103 (A.F.C.); Department of Radiology, Duke University Medical Center, Durham, NC (R.J.); Departments of Radiology, Neurology, and Neurosurgery, Johns Hopkins University School of Medicine, Baltimore, Md (M.G.R.); and Department of Radiology, Weill Cornell Medical College, New York, NY (G.S.). Presented as an education exhibit at the 2011 RSNA Annual Meeting. Received February 17, 2014; revision requested August 25 and received September 26; accepted October 8. The authors have disclosed no relevant relationships. **Address correspondence to** A.F.C. (e-mail: *achoudhri@uthsc.edu*).

[2]**Current address:** Mallinckrodt Institute of Radiology, Washington University School of Medicine, St Louis, Mo.

[3]M.G.R. and G.S. contributed equally to this article.

The end-user of mobile device apps in the practice of clinical radiology should be aware of security measures that prevent unauthorized use of the device, including passcode policies, methods for dealing with failed login attempts, network manager–controllable passcode enforcement, and passcode enforcement for the protection of the mobile device itself. Protection of patient data must be in place that complies with the Health Insurance Portability and Accountability Act and U.S. Federal Information Processing Standards. Device security measures for data protection include methods for locally stored data encryption, hardware encryption, and the ability to locally and remotely clear data from the device. As these devices transfer information over both local wireless networks and public cell phone networks, wireless network security protocols, including wired equivalent privacy and Wi-Fi protected access, are important components in the chain of security. Specific virtual private network protocols, Secure Sockets Layer and related protocols (especially in the setting of hypertext transfer protocols), native apps, virtual desktops, and nonmedical commercial off-the-shelf apps require consideration in the transmission of medical data over both private and public networks. Enterprise security and management of both personal and enterprise mobile devices are discussed. Finally, specific standards for hardware and software platform security, including prevention of hardware tampering, protection from malicious software, and application authentication methods, are vital components in establishing a secure platform for the use of mobile devices in the medical field.

Introduction

With the advent of powerful mobile computing devices such as tablet computers and smartphones, radiology as a field is poised at the helm of the medical field's adoption of such technologies in clinical care (1–7). Of critical importance in the acceptance of these new technologies are the security measures they use to protect critical patient information. Although general principles and more specific security measures for personal computers in clinical medicine have been discussed in the past, specific issues arising from the unique hardware platform that mobile devices represent, as well as the rapid changes taking place in the field of mobile communications, introduce new issues that warrant discussion (8,9).

TEACHING POINTS

- The Health Insurance Portability and Accountability Act (HIPAA) defined Password Management as an addressable (as opposed to required) item without any requirements for changing of passwords, ages of passwords, or number of different passwords before a password may be repeated.
- Longer passcodes become exponentially more secure; however, the security is dependent on the characters being random.
- Communications between the device and the Wi-Fi base station are unencrypted by default, allowing other users on the same network to possibly read the packets of information that are being passed to the different devices, a process known as "packet sniffing."
- Anonymization of medical data transferred using nonmedical applications would be the most prudent means of using these methods of communication when necessary.
- HIPAA is intentionally technologically neutral and provides general reasonable expectations.

Table 1: Some Abbreviations Used in This Article

Abbreviation	Definition
AES	Advanced Encryption Standard
BYOD	Bring your own device
COTS	Commercial off-the-shelf
DHHS	U.S. Department of Health and Human Services
EHR	Electronic health records
FDA	U.S. Food and Drug Administration
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
IEEE	Institute of Electrical and Electronics Engineers
IT	Information technology
OS	Operating system
PACS	Picture archiving and communication system
PHI	Protected health information
PPP	Point-to-Point Protocol
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual private network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

In this article, we review various aspects of mobile security in the leading device platforms and operating systems (OSs) (a list of abbreviations frequently used in this article may be found in Table 1, in particular as they pertain to medical use for the radiologist). Device-based security, including device and passcode access, local encryption, and remote wiping features, is discussed, as well as viruses and malware. Wireless security, security concerns based on application availability, and security issues as they pertain to enterprise implementation are discussed. After a guided how-to for accessing some security features on current smartphone platforms, there is a brief overview of the current regulatory status of this emerging technology.

Platforms

Mobile operating system platforms are rapidly evolving, and our description of mobile security encompasses the features available in the current versions of iOS 9 (Apple Computer, Cupertino, Calif) and Android 5.1 (Google, Mountain View, Calif; the Open Handset Alliance, Mountain View, Calif), which are the dominant mobile platforms, at the time of this writing (September 2015). It is understood that many of these hardware and software features may evolve or change over time.

iOS and Android share many security features. Where applicable, we will describe OS-specific features if they are different. Otherwise, it is implicit that both platforms support these features.

Devices and Operating System

The Devices.—Mobile devices used in medicine are typically consumer devices, most often smartphone devices or tablet computers. Laptop computers can also function as mobile devices; however, they will not be specifically discussed in this article. Netbooks are hybrids between tablet computers and laptops; they have a laptop-like interface but are smaller and have less computing power than a typical laptop.

Smartphone is a loosely defined term used to describe mobile phones that have an interface allowing the user to access programs and functions beyond that of phone calls. Current smartphones have graphical displays with high resolutions (eg, iPhone 5s: 1136 × 640 pixels, iPhone 6 Plus and Google LG Nexus 5: 1920 × 1080 pixels), leading up to pixel densities (starting with Apple's Retina Display), where the pixel sizes are smaller than what a human retina can resolve. These displays can surpass the resolution of many picture archiving and communication system (PACS) monitors (10). Tablet devices are larger than most smartphones, with screens often measuring from 6 to 9 inches diagonally. The dramatic recent hardware improvements to these mobile devices have allowed radiologists to begin incorporating smartphones

and tablets into their workflow and using mobile apps (eg, U.S. Food and Drug Administration [FDA] approved apps for reviewing radiology images) (11–13).

Operating Systems.—The major operating systems for mobile devices have modifications for both smartphones and tablet devices. The iOS operating system is designed by Apple (Cupertino, Calif) and runs on their lines of smartphone and tablet devices known as iPhone and iPad, respectively. iOS is authorized to run only on hardware designed by Apple, and thus some functions are based on both hardware and software features.

The Android operating system is a modification of the Linux family of operating systems (Linux Foundation, San Francisco, Calif) that is maintained by Google (Mountain View, Calif) and the Open Handset Alliance (Mountain View, Calif). Android has some features of an open-source operating system that allow users to modify the software to their needs; however, full access to the code of the current version of the system is limited by licensing agreements (14). There are Google-designed mobile devices and devices designed and manufactured by third parties. There therefore is not a single list of features that can describe all Android OS/device pairs; however, many features are common to most devices.

Device-based Security: Access to the Device.—Physical access to a mobile device can allow others to possibly retrieve data and passcodes stored on the device, or access servers that have preconfigured passcodes. iOS and Android devices have multiple security options for accessing (ie, unlocking) a device with passcode (numeric and alphanumeric) and biometric (eg, fingerprint for iPhone 5s and select Android devices) options (15–17). Android also supports a pattern lock option that provides nine small dots in a square, which is keyed by the user dragging a finger across a pattern of dots.

The Health Insurance Portability and Accountability Act (HIPAA) defined Password Management as an addressable (as opposed to required) item without any requirements for changing of passwords, ages of passwords, or number of different passwords before a password may be repeated (18). There are, however, best-practice guidelines offered by the Office of the National Coordinator for Health Information Technology that recommend that passcodes be eight characters or more long with both upper- and lowercase letters, one or more numbers, and one or more special characters (19,20). If passcode access is activated on an iOS device, the access code in iOS' default Simple Passcode mode is a four-digit number with a maximum of 10,000 options; this is not considered secure under HIPAA standards (19). A more complex passcode can be selected with a variable-length string of alphanumeric characters and symbols. Each character has more than 75 possible options, including 26 capital and 26 lower case letters, 10 digits, and multiple non-alphanumeric symbols; a four-character passcode under this system can have more than 30 million possible options. Longer passcodes become exponentially more secure; however, the security is dependent on the characters being random. Choosing a predictable pattern or word (such as "xray") over a random string (such as "y3+I") reduces the security from the theoretical maximum. Beyond numbers and alphanumeric passcodes, other means of access are possible. Android has configurable options for tracing a pattern to limit access, providing a theoretically infinite number of permutations. Biometric access controls do exist, with the most prominent devices being the Apple iPhone 5s, 6, and 6s models (as well as the iPad Air 2 and Mini 3 models) with a fingerprint scanner marketed as Touch ID. Apple claims the probability of strangers having fingerprints close enough to bypass its sensor are 1 in 50,000, which is approximately five times more secure than the standard four-digit passcode. However, increasing the passcode to six digits makes that approximately 20 times more secure than Touch ID (21).

The passcode can be set to activate immediately upon a device going to sleep, which is recommended for devices being used for medical purposes (for privacy reasons and HIPAA compliance), or at a set time interval. Devices can be set to erase their contents (ie, by local wipe) after a certain number of unsuccessful access attempts. This limits the ability of a "brute-force" attack from trying all passcode permutations to gain access; however, it makes it easy for a device to be intentionally (or possibly unintentionally) erased. If a device is lost or stolen, remote tracking of device location, reset of passcodes, and data erasure are features that are desirable in health care and enterprise settings.

Device-based Security: Local Encryption.—Both the latest iOS and Android releases support encryption of the data on the device at all times. Data on a device is typically stored within nonvolatile flash RAM, which is equivalent to an electronic hard drive. Just as a hard drive can be removed from a computer and directly accessed, the content of storage on a mobile device can sometimes be directly accessed even without knowledge of a device's passcode. This is because the passcode is a software lock that gains access

to the user interface. Protected health information (PHI) on a device will ideally be stored encrypted, so that physical access to the memory of a device does not compromise security.

Encrypted files can also be helpful to prevent malicious apps on a device, such as a virus or worm, from accessing PHI stored by other apps. For instance, a maliciously designed game could send contents of a user's e-mail or digital address book to a server that is collecting stolen information. The most recent versions of both iOS and Android OS are set up so that apps cannot access the memory used by other apps; the apps therefore run in a virtual sandbox. The sandbox technique decreases the chances of apps or Web sites stealing information from the storage on the user's device.

Viruses and Malware.—The major platforms do not currently have virus protection software built in, although the app store process likely provides some kind of virus screening. The iOS platform will not allow third-party software to access memory assigned to the system and other apps, which would be required of a virus protection program; however, sandboxing and digital signatures of the apps themselves can improve security. As with desktop computers, viruses and malicious applications (known as *malware*) exist on mobile devices; although they have not been as widespread an issue on mobile devices as on desktops yet, this is rapidly changing. Threats from mobile malware were up 58% in 2012 (22), and about one-third of the attacks appeared to involve stealing information, perhaps leading to identity theft. Infected devices also potentially pose a higher risk for uninfected devices on the same network, such as on a secure health care network.

Google's Android platform has seen much more mobile malware than Apple's iOS (23). One reason is that Android has a much larger market share, which may attract more malware writers who prefer to target as many devices as possible. In addition, the openness of Android and the multiple distribution methods of apps (eg, ability to sideload apps from a Web site or from your computer instead of downloading from the Google Play app store) make it the most popular target platform for creators of malware.

Apple iOS is not immune from malware. Indeed, Symantec's Internet Security Threat Report (24) notes that there are 387 documented vulnerabilities on Apple iOS, compared with only 13 in Android in 2012. However, as pointed out in their report, the number of vulnerabilities does not necessarily translate into threats (only one known threat has been found to be created for all iOS vulnerabilities).

Both Android and iOS have screening processes for mobile apps in their respective app stores; however, this does not prevent hidden features in those apps. Many mobile apps have documented "Easter Egg" functionality that contains surprise features not always detected by the app review team. In iOS, two apps were discovered in late 2012 to have sneaked in wireless tethering functionality in seemingly innocuous apps with the names DiscoRecorder and FlashArmyKnife (25). One might imagine that malware can also sneak through this review process.

For Android, it was discovered in April of 2013 that a new malware family called BadNews was in 32 apps across four developer accounts, and the combined affected apps have been downloaded between 2 million and 9 million times (Google does not give exact download numbers). This particular malware, masquerading as a mobile advertising network, can send fake news messages asking users to install apps and can steal sensitive information about the user and device. This new family of malware poses the threat even without the knowledge of the developers, appearing to be a third-party ad framework, with its malicious behavior controlled by a server. The delayed malware attacks made it difficult to detect while the apps were going through the standard vetting process. Thus, ensuring security in the health care environment is becoming more complex, and responsibility lies with both the app developers, who must be aware of third-party libraries they use, as well as the enterprise information technology managers, who should have ongoing security monitoring to detect malicious behavior of even vetted and approved apps.

Apps distributed from the iTunes app store for iOS require the programs to have a digital signature from a registered developer. Native apps for iOS otherwise cannot be distributed by official means, and although some feel this limits user flexibility, it is clear this method significantly limits the effect of malicious apps. The Android ecosystem is more open than the iOS system by design and has multiple software forks (unofficial Android versions such as the one used by Amazon Kindle devices), which gives considerable flexibility to developers and users but also has provided a pathway for a multitude of malicious apps.

Device-based Security: Remote Wipe.—In the event that an iOS or Android device is lost or stolen, remote tracking and wipe features can both help locate a lost device and permanently delete all data. Apple has both a Find My iPhone app and a Web site *(http://www.icloud.com)* that allow for geolocation of a user's device as well as

remote wipe. Android also has Android Device Manager (available as a native app or by the browser at *http://android.com/devicemanager*), which allows the same remote tracking and wipe features as Apple.

Wireless Security

A computer network is a group of two or more computer systems that are linked together. A network can be created using hardwired connections, wireless connections (usually using Wi-Fi, an Institute of Electrical and Electronics Engineers [IEEE] 802.11 wireless protocol), or a combination of both. Networks can be classified as public networks and private networks. The difference between a public network and a private network is that anyone can access a public network, whereas a private network typically has restricted access and requires some sort of authentication to gain access.

A simple example of a private network would be a home network. The Internet provider installs a device in the user's home, referred to as a router. This device acts as a firewall, separating the private network inside the user's home from the public network outside the user's home. The flow of data to and from the internal network is controlled by the firewall. The private network is created by directly connecting computers to the router with a cable, or using a Wi-Fi connection with a passcode to connect to the router.

For the purposes of this discussion, cellular networks are wireless, private networks. Data transfer to mobile devices is typically performed in a wireless manner, either through cellular networks or through Wi-Fi networks.

Successive generations of cellular technology have been labeled numerically, with a majority of the United States currently having coverage under third-generation (3G) protocols, including Universal Mobile Telecommunications System (UMTS), which is an update of the second-generation (2G) Global System for Mobile Communications (GSM) protocols protocol, and CDMA2000. Fourth-generation protocols (4G) (LTE [Long-Term Evolution] and WiMax) offer faster communication; however, the networks are still currently being deployed (26). Data sent between a mobile device and a cellular tower does include an encryption layer, although as the origin of the data comes from a server, there typically is still another layer of encryption (eg, VPN [virtual private network] or SSL [Secure Sockets Layer]) imposed on sensitive data (such as PHI).

A wireless link between a mobile device and the Internet can take place through Wi-Fi, in particular the IEEE 802.11 family of protocols. Communications between the device and the Wi-Fi base station are unencrypted by default, allowing other users on the same network to possibly read the packets of information that are being passed to the different devices, a process known as "packet sniffing." Several protocols exist to secure the communication between a Wi-Fi base station and the end device. WEP (Wired Equivalent Privacy) is the simplest protocol, which typically uses a 40-bit encryption key (27). All WEP communications take place using the same encryption key, so once the single key is divulged the entirety of communications can be intercepted; WEP is therefore not considered a secure protocol (28,29). WPA (Wi-Fi Protected Access) was developed to overcome limits of WEP, in which a distinct encryption key of from 40 to 128 bits is used for each packet of data that is transmitted (30,31) (Table 2). If a key for a given packet of information were to be compromised, all other packets of information would remain secure. WPA2 (Wi-Fi Protected Access II) is a more recent variation of WPA that markedly increases the level of security over WEP and WPA, and should be used when possible. If WPA2 is not possible, WPA should be used. WEP should be avoided for medical purposes, or any scenario where security is desired.

It is important to realize that n-bit encryption has 2^n possibilities, so 40-bit encryption has 2^{40} possible combinations (more than 1 trillion); 41-bit encryption has two times as many possible combinations as 40-bit encryption ($2^{41} = 2 \times 2^{40}$).

Transfer of data between software on a mobile device, such as a Web browser or an e-mail client, and the wireless communications chip on the device, also may not be encrypted, allowing a malicious app to packet sniff the communication of information within the device. Packet sniffing is the interception of unencrypted data being sent to another location, similar to reading the contents of a postcard addressed to another individual.

Encryption associated with cellular and Wi-Fi data transfer provides security for the portion of communication between the device and the transmitter. Transfer of data from the cellular tower or Wi-Fi transmitter over the data network to the end server, such as a hospital server, is not encrypted by default regardless of the level of security used between the device and the transmitter. Additional software protocols can be implemented, creating a superimposed encryption layer between the mobile device and the back-end server using a VPN, further discussed in the next section.

Applications

Having covered the technical safeguards required in accessing the physical mobile device, protect-

Table 2: Comparison of IEEE 802.11 Encryption methods

Protocol	Encryption Key Length	Passcode Requirement (Minimum Length)	Current Status	Authentication Type*	Encryption Type*
WEP Low	40 or 64 bits	5 characters	Retired 2004	None	WEP
WEP High	104 or 128 bits	13 characters	Retired 2004	None	WEP
WPA-Personal	64–128 bits	8–32 characters	Retired 2006	PSK	TKIP
WPA-Enterprise	64–128 bits	8–32 characters	Retired 2006	802.1X	AES (handled by authentication server)
WPA2-Personal	64–256 bit	8–64 characters	Current (as of 2015)	PSK	AES (TKIP as fallback method)
WPA2-Enterprise	64–256 bit	8–64 characters	Current (as of 2015)	802.1X	AES

Note.—The retired status of a protocol does not indicate they are not still in use, only that new devices are not certified for this. Existing network equipment may be limited to the protocols available at their time of manufacture.
*AES = Advanced Encryption Standard, PSK = preshared key, TKIP = Temporal Key Integrity Protocol.

ing its operating system, and ensuring safe transmission of wireless data, we now discuss how to establish robust technical safeguards when transmitting electronic PHI between the electronic health records (EHR) or PACS server and the individual device. An understanding of the strength of different safeguards requires an understanding of the various applications used to transfer this information. These applications include VPNs, direct access through an Internet Web browser, virtual desktop environments, and commercial off-the-shelf (COTS) nonmedical applications such as e-mail or instant messaging systems.

A VPN is a network that uses a public network to provide secure access to a private network behind a firewall. The VPN works by encrypting the data at one end, sending it over the public network, and decrypting the data at the other end. An analogy would be the use of the public postal service to transmit sensitive documents between two offices. The information on these documents could be placed on postcards and mailed, but the information would be insecure and visible for anyone handling the mail to see. A VPN would be akin to placing the document in a secure envelope with a seal that no one could break except for the intended recipient. One could then use the public postal service for the transmission of secure private documents. The private network could include such entities as a hospital system's EHR or a radiology department's PACS network (32).

In contrast to using VPNs, organizations can connect their private networks using owned or leased lines. This is significantly more expensive than using the Internet. In our analogy, this would be akin to the private company starting its own shipping company to send secure documents. These networks have traditionally been implemented by dial-up modem to use a leased individual phone line and have been limited in speed and scalability.

The advantage of VPNs are that they are easily scalable and allow the expansion of remote access to any location that has access to the public Internet. VPNs require specific software at the server side as well as at the client remote user side. This software is responsible for encrypting the individual packets of information that are transferred over the public network. This server-side software is often incorporated into a dedicated hardware device known as a VPN gateway. This gateway is responsible for authorizing and maintaining the VPN tunnel connection between the server and client as well as maintaining a firewall to protect the private network from unauthorized users in the public network.

A VPN is only as secure as its protocol for encryption of the information packets and only as fast as the public network infrastructure connecting the server to the client. Although the encryption protocols vary between different VPN gateway vendors, most use protocols based on PPP (Point-to-Point Protocol). This is the standard encryption protocol for the secure transmission of encrypted data over the public Internet. The most popularly available implementations include those provided by Microsoft Windows and Windows Phone, OS X and iOS, and Android, which use iterations of this protocol. There are also vendors with proprietary standards implemented through their own hardware and software packages such as Juniper Networks, which sells their own Enterprise routing hardware running their Junos operating system, which is implemented by many hospital systems for its ease of use.

Although VPNs allow a secure connection between a remote user and a server, they do require that the remote user have specific software installed to use the transferred data. In mobile radiology, that would require a specific imaging app installed on the user's mobile device that would have to be device specific. As an alternative, an imaging app can be developed in computer languages such as Java that are made to be machine-independent and downloaded as part of a Web viewing session, adding more complex imaging functionality to a Web browser. This adds the advantage of portability but requires often trading off computing performance and the security benefits of VPNs. To address the security of information transferred using Web browsers, a popular implementation of encryption is SSL, used by Internet browsers and Web servers when transmitting sensitive information as part of a broader category of security standards for Web browsers known as TLS (Transport Layer Security). Web sites such as banks and credit card companies use SSL to transfer account information on a Web browser, and a user can tell that SSL is being used by noting that the "http://" in the site's Web address is replaced by "https://." Web browsers also have the image of a padlock on their status bar, indicating that SSL is being used to encrypt the transmitted data.

The third alternative to VPNs and Web-based applications is using virtual desktop apps. These apps essentially transform a mobile device into a mobile monitor. The remote computer simply transfers the information it would ordinarily send to its monitor to the remote user to use as though they were sitting at the computer. This implementation does not require any imaging-specific software on the remote user's mobile device, and it does not transfer any patient-specific data that is saved on the mobile device. Although this offers the full computing power and security protocols available on imaging workstations, it is too cumbersome for practical application in routine clinical practice because it requires an unachievable amount of bandwidth with currently available technology. In fact, virtual desktops are often implemented by intentionally reducing the transferred image quality to deal with available bandwidth, and this may directly affect its utility and usefulness in radiology. However, virtual desktops may be useful in specific situations where the value of a clinical interpretation by a remote radiologist outweighs the time cost required to access the data. There are also no security standards established for virtual desktop applications, as they are application developer–specific, and a clinician should carefully evaluate the security protocols implemented by the application and the quality of the transmitted images before using it for clinical interpretation.

Finally, nonmedical COTS applications represent the most broadly used general communications protocols, including e-mail, short message services (SMS; also known as text messaging), and videoconferencing applications. Because of their convenience, these applications are becoming increasing used to transfer radiologic images. There are currently no standard encryption mechanisms between e-mail providers, and standard e-mail is therefore not considered HIPAA-secure. Specific e-mail providers have services available to create a secure e-mail network that is HIPAA-secure for additional fees, including Google's service for Google Apps (33), among others. Similarly, standard SMS is not considered HIPAA-secure, but a number of medical communication application developers have text messaging applications that are advertised as HIPAA-compliant. Videoconferencing applications such as Skype and Apple's FaceTime have AES encryption protocols, but these companies have intentionally avoided marketing these applications for health care purposes because then they could fall under the FDA's emerging "intended use" regulations. Anonymization of medical data transferred using nonmedical applications would be the most prudent means of using these methods of communication when necessary.

Enterprise Security

Bring Your Own Device.—Bring your own device (BYOD) is an industry term for having institutional support for users providing their own devices. This has become commonplace over the last few years during the rapid adoption of mobile smartphones and tablet devices by consumers. Hospitals vary widely in their acceptance of personal devices used at work, but most are currently tolerating these devices on their network, provided that they adhere to institutional security policies. BYOD results in unique security challenges for institutional IT officers due to the possible variety of devices, lack of control over other software installed on the device, and increased likelihood of individuals using the device for personal reasons or sharing the device with family members.

Mobile Device Management and Security Policies.—Before these mobile devices are allowed on the enterprise network, options exist to enforce an institutional security policy for iOS (eg, Configuration Profile) and Android devices (eg, Android Device Policy for Google Apps for Business, Government and Education).

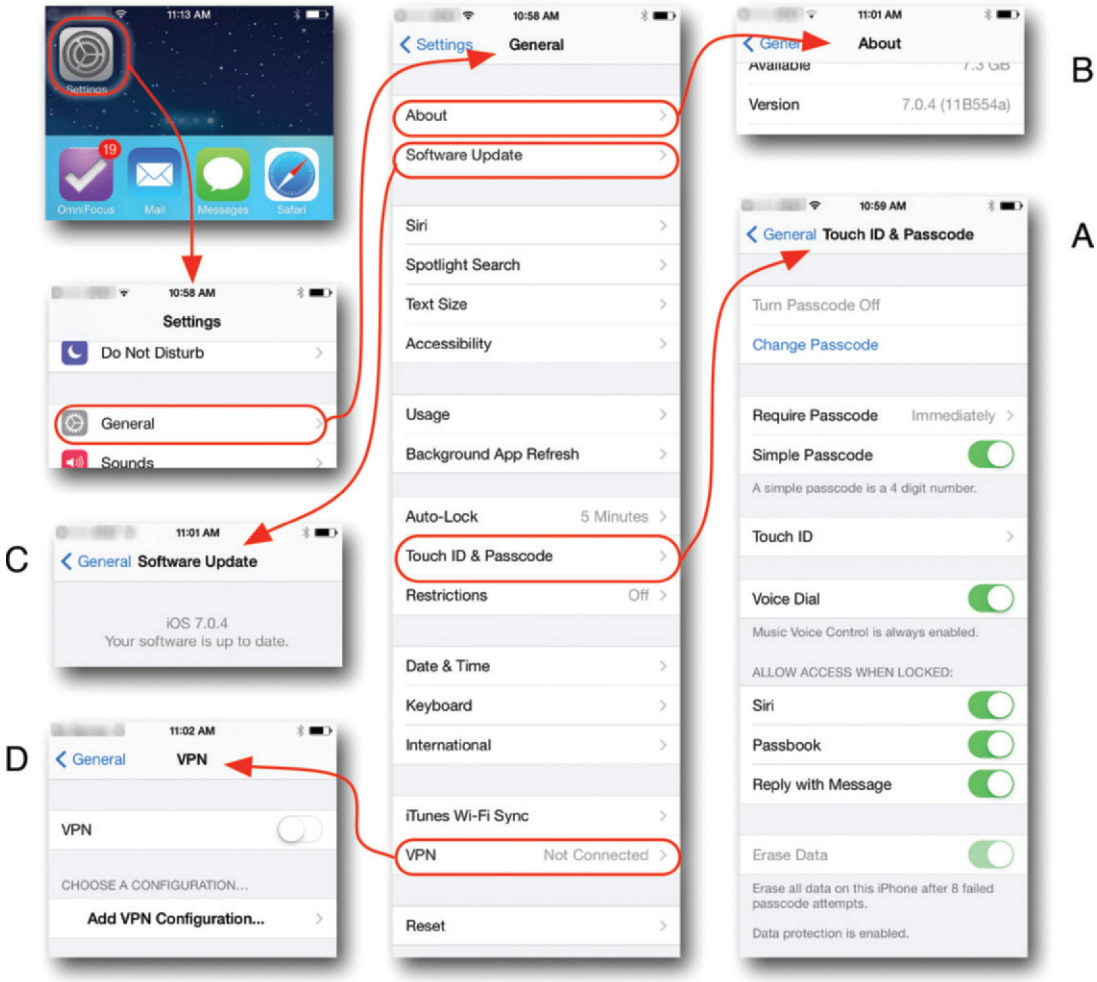

Figure 1. Implementing security features in iOS. Starting from the home screen on the top left, the settings app provides access to all of the security features. Implementing a startup passcode lock involves visiting the "Touch ID & Passcode" screen *(A)* and toggling the passcode option "On" and entering a passcode. The passcode can be made more complex than the four-digit Simple Passcode by toggling "Simple Passcode" to "Off." One can also set the device to erase all of its data following eight unsuccessful login attempts by toggling "Erase Data" to "On." This "Erase Data" feature may not be available if a Microsoft Exchange e-mail account is being used and the system administrator for that account restricts this particular feature. The "Touch ID" menu accessible from this screen gives the fingerprint recognition options available on the iPhone 5s and above. The software on the device should be routinely updated to the latest version to take advantage of both security and stability updates to the OS. The latest software version can be confirmed by accessing the "About" screen *(B)*, and the software can be updated by accessing the "Software Update" menu *(C)* while connected to a Wi-Fi network for Internet access. A VPN connection with a host server can be established by accessing the "VPN" screen *(D)*.

Third-party mobile device management solutions are also available to provide customized solutions that support multiple mobile platforms (eg, Apple, Android, and Blackberry). More and more hospitals are using these third-party solutions to manage and enforce security policies for personal mobile devices (BYOD) as well as hospital-owned mobile devices.

Guided How-To

A guide regarding finding and implementing security settings is provided for Apple's iOS (Fig 1) and for Android devices (Fig 2). Mild variations in appearance will be noted between individual devices, in particular on Android devices due to the greater variety of available devices. As the platforms evolve and newer versions of operating systems are released, additional variations will invariably arise; however, the general trends remain intact.

Regulatory Concerns

It is important for radiologists to have a basic understanding of the implications of HIPAA and U.S. Federal Information Processing Standards (FIPS) (18,19,34–39). The federal regulation covering specified HIPAA regulations dealing with technical safeguards, 45 CFR 164.312(a)(2)(iv), states that covered entities must set standards for access control by implementing specifications

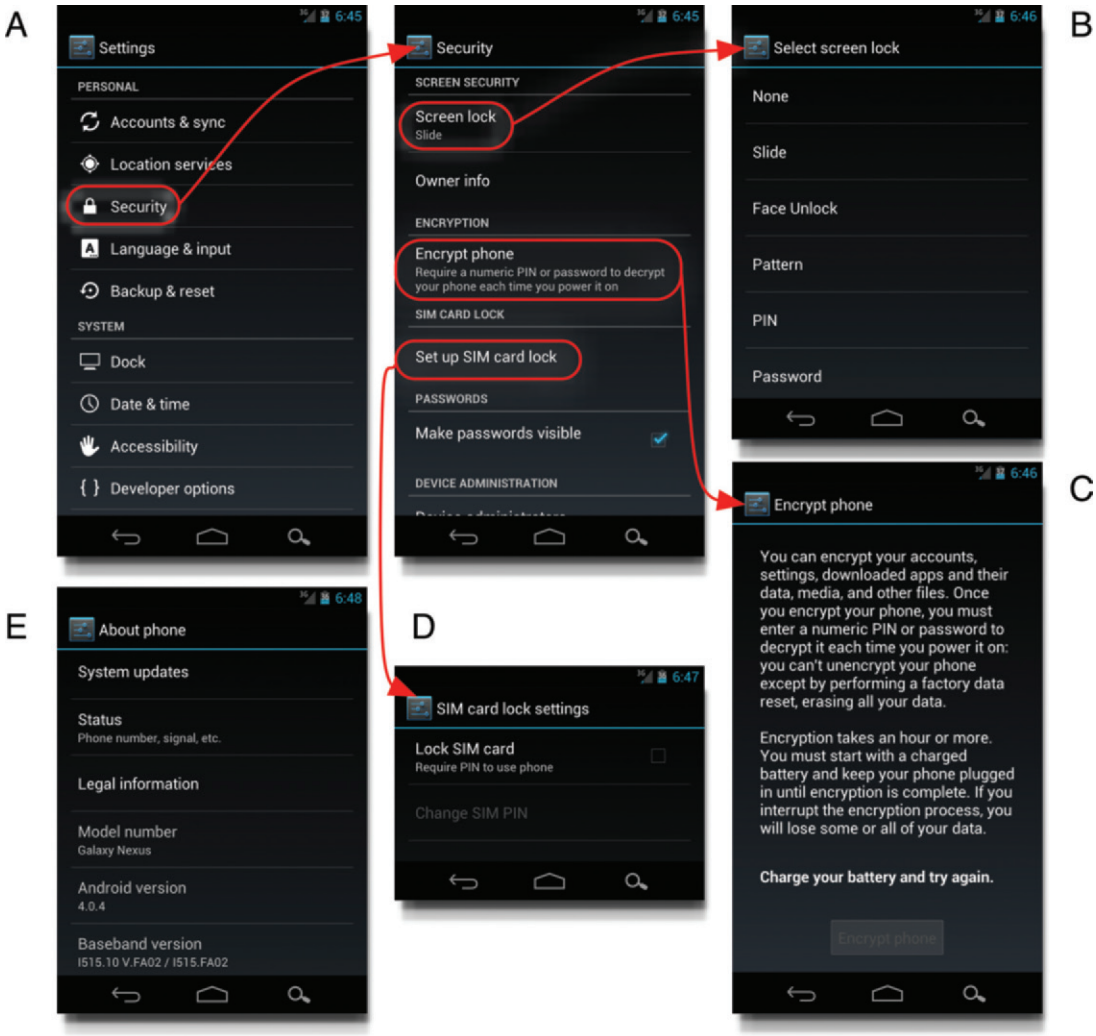

Figure 2. Implementing security features in Android. From the "Security" option in the "Settings" menu *(A)*, "Screen Lock" *(B)* options are available to implement a passcode or alternative method for securing access to the device. All of the data on the device can be encrypted by accessing the "Encrypt phone" menu *(C)*. This would prevent data on the device that may have been copied off the device or otherwise somehow accessed by bypassing the screen lock passcode from being easily readable without the proper passcode to decrypt the information. Additionally, a SIM (subscriber identity module) card that belongs to the mobile device can be locked with a PIN (personal identification number) code with the "SIM card lock settings" menu *(D)*. The "About phone" menu *(E)* provides access to system updates that should be routinely performed to ensure that the latest and most secure version of the operating system is being used.

for unique user identification, have the ability to automatically log-off the authorized user after a reasonable time of inactivity, and implement a mechanism to encrypt and decrypt electronic PHI. HIPAA is intentionally technologically neutral and provides general reasonable expectations (18). However, according to the U.S. Department of Health and Human Services (DHHS) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, any health care provider under the umbrella of covered entities is required to get signed business associate agreements with all partners and vendors that have contact with an organization's PHI, and these agreements ensure that all parties understand the HIPAA requirements for PHI (38). It is currently unclear to what extent these requirements will be required of service providers such as Apple, Google, or Skype when health care providers use their online services for the transmission of PHI. These companies have been unwilling to declare that they are officially HIPAA-compliant or provide business associate agreements (39). These companies are therefore not required to disclose security breaches or findings from security audits. This places the onus of responsibility for security standards on the health care providers and organizations that transmit this PHI. Failure to comply with HIPAA regulations can result in civil and criminal penalties. 42 USC 1320d-5 states that the secretary of DHHS may impose a civil penalty of up to $50,000 per violation for a violation not cor-

rected within 30 days with an annual maximum of $1.5 million for a violation not corrected within 30 days (34,35).

The FDA is in the process of drafting a white paper on regulation of mobile medical devices (36). The American College of Radiology has participated in joint workshops with the FDA to determine standard operating procedures for medical use of mobile devices (12).

Conclusion

Mobile devices have become a common way of accessing medical information within the hospital and outside the hospital setting. Use of these devices in a manner that maintains the security of PHI is important; however, little guidance exists for physicians choosing to use mobile devices. This is particularly true for those who use their personal devices, such as mobile phones. Effective implementation of security settings on mobile devices, and within the enterprise setting, can maximize the effect of this new technology in a manner protecting patient privacy.

References

1. Choudhri AF, Radvany MG. Initial experience with a handheld device digital imaging and communications in medicine viewer: OsiriX mobile on the iPhone. J Digit Imaging 2011;24(2):184–189.
2. Choudhri AF, Carr TM 3rd, Ho CP, Stone JR, Gay SB, Lambert DL. Handheld device review of abdominal CT for the evaluation of acute appendicitis. J Digit Imaging 2012;25(4):492–496.
3. Engelmann U, Schröter A, Borläv E, Schweitzer T, Meinzer H. Mobile teleradiology: all images everywhere. Int Congr Ser 2001;1230:844–850.
4. Choudhri AF, Norton PT, Carr TM 3rd, Stone JR, Hagspiel KD, Dake MD. Diagnosis and treatment planning of acute aortic emergencies using a handheld DICOM viewer. Emerg Radiol 2013;20(4):267–272.
5. Tang FH, Law MY, Lee AC, Chan LW. A mobile phone integrated health care delivery system of medical images. J Digit Imaging 2004;17(3):217–225.
6. Andrade R, Wangenheim Av, Bortoluzzi MK. Wireless and PDA: a novel strategy to access DICOM-compliant medical data on mobile devices. Int J Med Inform 2003;71(2-3):157–163.
7. Rosset A, Spadola L, Ratib O. OsiriX: an open-source software for navigating in multidimensional DICOM images. J Digit Imaging 2004;17(3):205–216.
8. Caruso RD. Personal computer security: part 1. Firewalls, antivirus software, and Internet security suites. RadioGraphics 2003;23(5):1329–1337.
9. Caruso RD. Personal computer security: part 2. Software configuration and file protection. RadioGraphics 2004;24(5):1503–1512.
10. Li M, Wilson D, Wong M, Xthona A. The evolution of display technologies in PACS applications. Comput Med Imaging Graph 2003;27(2-3):175–184.
11. McNulty JP, Ryan JT, Evanoff MG, Rainford LA. Flexible image evaluation: iPad versus secondary-class monitors for review of MR spinal emergency cases, a comparative study. Acad Radiol 2012;19(8):1023–1028.
12. Hirschorn DS, Choudhri AF, Shih G, Kim W. Mobile medical devices. In: Wald C, Padi J, eds. IT reference guide for the practicing radiologist. Reston, Va: American College of Radiology, 2013.
13. John S, Poh AC, Lim TC, Chan EH, Chong R. The iPad tablet computer for mobile on-call radiology diagnosis? Auditing discrepancy in CT and MRI reporting. J Digit Imaging 2012;25(5):628–634.
14. Stallman R. Android and users' freedom. http://www.gnu.org/philosophy/android-and-users-freedom.html. Published 2012. Updated December 17, 2013. Accessed February 10, 2014.
15. iOS: Using passcodes. http://support.apple.com/kb/HT4113?viewlocale=en_US&locale=en_US. Accessed February 10, 2014.
16 Android security overview. http://source.android.com/devices/tech/security/index.html. Accessed February 10, 2014.
17. Does the device passcode on iOS, Android and BlackBerry prevent someone from accessing device data? http://viaforensics.com/mobile-security/question-device-passcode-ios-android-blackberry-prevent-accessing-device-data.html. Accessed February 10, 2014.
18. HIPAA administrative simplification. http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf. Accessed February 10, 2014.
19. CyberSecurity. 10 best practices for the small health care environment. http://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf. Accessed February 10, 2014.
20. Herley C. So long, and no thanks for the externalities: the rational rejection of security advice by users. http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf. Accessed February 10, 2014.
21. Suleman K. How secure is Apple's Touch ID. http://www.itpro.co.uk/mobile/20728/how-secure-apples-touch-id. Published October 8, 2013. Accessed February 10, 2014.
22. Bell L. Apple's iOS had more security vulnerabilities than Android in 2012. http://www.theinquirer.net/inquirer/news/2262231/apple-ios-had-more-security-vulnerabilities-than-android-in-2012. Published April 17, 2013. Accessed February 10, 2014.
23. When malware goes mobile. http://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile/why-ios-is-safer-than-android.aspx. Accessed February 10, 2014.
24. Internet security threat report 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. Published April 2013. Accessed February 10, 2014.
25. Another hidden tethering app, first 12 Days of Christmas gift, EA Games sale. http://9to5mac.com/2012/12/26/another-hidden-tethering-app-first-12-days-of-christmas-gift-ea-games-sale/. Accessed February 10, 2014.
26. LTE and the evolution to 4G wireless design and measurement challenges. http://www.3g4g.co.uk/Lte/LTE_Security_WP_0907_Agilent.pdf. Accessed February 10, 2014.
27. 802.11: IEEE standard for information technology. Telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements—part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. http://ieeexplore.ieee.org/servlet/opac?punumber=5258. Published 1997. Revised August 6, 2002. Accessed February 10, 2014.
28. Vibhuti S. IEEE 802.11 WEP (Wired Equivalent Privacy) concepts and vulnerability. http://www.cs.sjsu.edu/~stamp/CS265/projects/Spr05/papers/WEP.pdf. Published Spring 2005. Accessed February 10, 2014.
29. Sandirigama M, Idamekorala R. Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys. IEEE International Conference, Sept 2009, 433–438.
30. Lashkari AH, Mansoor M, Danesh AS. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). 2009 International Conference on Signal Processing Systems, May 2009, 445–449.
31. Benton K. The evolution of 802.11 wireless security. http://itffroc.org/pubs/benton_wireless.pdf. Published April 18, 2010. Accessed February 10, 2014.

32. Methodist Hospital System keeps network secure with Juniper Networks. http://newsroom.juniper.net/manual-releases/2006/Methodist-Hospital-System-Keeps-Network-Secure-wit. Accessed February 10, 2014.
33. Google HIPAA encryption information. https://static.google-usercontent.com/media/www.google.com/en/us/work/apps/terms/2015/1/hipaa_implementation_guide.pdf. Accessed September 10, 2015.
34. Enforcement rule: final rule FR Doc 06-1376. http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enforcementfinalrule.html. Accessed February 10, 2014.
35. HIPAA violations and enforcement. http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page. Accessed February 10, 2014.
36. Mobile medical applications: guidance for industry and Food and Drug Administration staff. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf. Accessed February 10, 2014.
37. HIPAA security rule: frequently asked questions regarding encryption of personal health information. http://www.ama-assn.org/resources/doc/washington/hipaa-phi-encryption.pdf. Accessed February 10, 2014.
38. Notice of proposed rulemaking to implement HITECH Act modifications. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechnprm.html. Accessed February 10, 2014.
39. Health information privacy: sample business associate agreement provisions. http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. Accessed February 10, 2014.