Use of Mobile Devices for Medical Imaging

David S. Hirschorn, MDa, Asim F. Choudhri, MDb,c, George Shih, MDb, Woojin Kim, MDe

Mobile devices have fundamentally changed personal computing, with many people forsaking the desktop and even laptop computer altogether in favor of a smaller, lighter, and cheaper device with a touch screen. Doctors and patients are beginning to expect medical images to be available on these devices for consultative viewing, if not actual diagnosis. However, this raises serious concerns with regard to the ability of existing mobile devices and networks to quickly and securely move these images. Medical images often come in large sets, which can bog down a network if not conveyed in an intelligent manner, and downloaded data on a mobile device are highly vulnerable to a breach of patient confidentiality should that device become lost or stolen. Some degree of regulation is needed to ensure that the software used to view these images allows all relevant medical information to be visible and manipulated in a clinically acceptable manner. There also needs to be a quality control mechanism to ensure that a device’s display accurately conveys the image content without loss of contrast detail. Furthermore, not all mobile displays are appropriate for all types of images. The smaller displays of smart phones, for example, are not well suited for viewing entire chest radiographs, no matter how small and numerous the pixels of the display may be. All of these factors should be taken into account when deciding where, when, and how to use mobile devices for the display of medical images.

Key Words: Mobile device, Android, iOS, smart phone, tablet, informatics


OVERVIEW

Mobile devices have become an integral part of life in modern society and have achieved high penetration among health care professionals. By comparison, it is almost laughable what used be called a personal computer. Mobile devices are far more personal insofar as they serve as the primary communication devices for many people and are as important as one’s wallet. They are already used to store and access personal information such as contacts and family photos. In places where devices are used to execute payments at stores and in similar tasks, they are beginning to replace wallets altogether.

As these devices have become better connected to the Internet, they have begun to shape the Internet itself. Most organizations devote a considerable amount of resources to their websites to accommodate mobile devices with smaller displays and touch-based interfaces. Core web services such as e-mail, news, weather, mapping, and navigation have become more streamlined and integrated so that users can find the information they seek more efficiently. As this information revolution progresses, physicians have increased expectations regarding device use to enhance the practice of their profession. Doctors have begun to wonder, “Why can I get my banking and credit card information online but not the medical records of my patients?” As displays grow in resolution and brightness, expectations rise surrounding the display of medical images on mobile devices.

The mobile tablet opened up a new class of possibilities. Tablets are decidedly not phones but do provide significantly more space for richer information and tasks, including displaying multiple levels of data (eg, patient demographics, examination history, information about the currently selected examination). Tablets also permit enhanced interaction; a multitouch interface can be used to manipulate a set of images, including window, level, zoom, and pan functions, more effectively on a tablet than on a phone-sized device.

To ensure the safe and effective practice of medicine, however, radiologists need to look before they leap. Several aspects should be considered before selecting one of these devices to incorporate into clinical care. For example, the platform should be sustainable; no matter how attractive a device brand seems, it will not help if it is not adequately supported, available, and around for enough time to be worth the investment. In addition, security protocols must be in place to prevent unauthorized access of patient data.
All too often, this is a foregone conclusion. As for functionality, the history of PACS is replete with software that looked great on the trade show floor but fell flat when put into clinical use. Ultimately, software written for a desktop platform that is “shoved” onto a mobile device will tend not to work well when put to the test of heavy day-to-day use. Although broadband network speeds are reasonably fast and, in fact, are expected to sharply increase in 2014, some programs (“apps”) that are too dependent on strong bandwidth, which is always available during a demonstration, may falter when subjected to real-world network speeds. Finally, not all mobile device displays are created equally. Factors to consider include not only the traditional specifications of resolution and brightness but also reflectivity and susceptibility to distortion from fingerprints.

**BANDWIDTH**

Mobile devices can run programs and access data stored locally or on a separate server. Apps and frequently used information are typically stored locally. When seeking additional information, from a website, a server, or the “cloud,” data must be transferred to the device. When a mobile device is plugged into a computer, data can be directly and rapidly transferred through a cable. Universal serial bus 3.0 protocol cables are most commonly used to connect mobile devices to computers. Wireless connections to computers can be performed using Bluetooth technology and Wi-Fi. When seeking communication with the Internet, including websites and cloud servers, communication usually takes place through Wi-Fi connections or cellular (ie, broadband) networks. Cellular network access can take place on all smart phones and many tablet and handheld devices. Nearly all devices can access Wi-Fi networks.

Transferring data can be rapid but is not instantaneous and is subject to possible bottlenecks. In general, data-transfer speed is related to the slowest point of communication between two devices. The bottleneck usually occurs in the wireless transfer, but in some circumstances it can be a limitation with data reading and writing tasks in the device itself.

The terminology of data-transfer speeds is based on binary measurement instead of the more familiar base 10 terms. The most basic unit of data is the bit, a contraction of the term *binary digit*. It is a single binary number (either 0 or 1) and is the lowest common denominator in data storage. All electronic data are stored and transmitted as a series of bits. Because a single bit contains very little information, a set of 8 bits is often used as a unit of storage called a byte, which has $2^8$ (256) possible values. Data-transfer rates are often given in bits per second, whereas data file size is typically reported in bytes. Thus, a transfer bit rate divided by 8 represents the byte rate. Eight bits per second equals 1 byte/s.

Similarly, numeric prefixes that denote large values of bits and bytes differ from the more familiar ones used in US measurements. Data files are typically composed of thousands or millions of bytes. In the United States, orders of magnitude are typically labeled as thousands, millions, billions, and so on. However, for data, the metric system is used, wherein the prefix for $10^3$ is *kilo*, for $10^6$ is *mega*, for $10^9$ is *giga*, for $10^{12}$ is *tera*, and so on. Thus, 1,000 bytes are typically referred to as 1 kilobyte, which is the same as 8 kilobits; however, because computers work on a binary system, a kilobyte is considered $2^{10}$ bytes, or 1,024 bytes.

Data-transfer rates are often listed in terms of bits per second, typically megabits per second. A data-transfer rate of 10 megabits/s is the same as 1.25 megabytes/s. An uncompressed CT or MR image typically is approximately 0.5 megabytes, so a 100-image study will require 50 megabytes of space. At this rate, the examination would transfer in approximately 40 seconds if uncompressed. Data compression can reduce the time significantly by summarizing repeating sequences and discarding data that have almost no noticeable effect on the image, but compression may require increased processor use, which affects battery life in a portable device and if improperly implemented can result in decreased image quality.

Data-transfer speeds can vary significantly (Table 1), with wired transfer typically the fastest, followed by short-range wireless transfer such as Wi-Fi and Bluetooth. All wireless transfer speeds, via Wi-Fi, Bluetooth, or a cellular network, can be variable depending on factors such as distance from the transmitter, physical barriers between the transmitter and the device, electromagnetic interference, and the number of other local devices sharing the same bandwidth and connected to the same transmitter. Therefore, typical real-world transfer rates for most forms of wireless communication can be significantly lower than the theoretical maximum.

**SECURITY**

Mobile device security falls into several realms. First, there is the task of securing direct access to the device (ie, who gets their hands on it). Next, there is the need to secure access to the device’s memory, either from different application processes or from external hacking. Additionally, there is communication with other devices, typically performed wirelessly through Wi-Fi or cellular networks. Each of these areas is subject to security vulnerabilities, and an appropriate understanding of the basic terminology and parameters within these areas helps improve awareness of security issues.

Regarding direct device access, devices used for medical work should have password authentication to prevent unauthorized users from accessing their contents. Only a handful of consumer devices (eg, Android tablets running version 4.2 or above) currently allow profiles for different users, so providing one user with access may allow that user to view all the contents of a device. This is especially important in settings in which
devices serve dual purposes, such as mobile entertainment centers for a physician’s children and patient data viewers, a practice that is generally incompatible with appropriate-use practices for a medical device. Existing mobile platforms allow devices to be passcode protected. The default passcode setup on an iOS device, for instance, is a 4-digit numeric code, with $10^4$ (10,000) possible combinations. Ten thousand combinations is large for casual protection of data, but it is easily vulnerable to brute-force attacks, which are attempts to try all possible combinations. For instance, if a code can be entered in 2 seconds, then all codes can be attempted in 5.5 hours. Presumably the actual code will be found earlier, on average at the halfway point. If a brute-force attack preferentially attempts likely passcode combinations first, on the basis of the assumption that codes such as “1234” and “7777” will be more common than a random sequence, then brute-force attacks can succeed more quickly. To prevent the utility of brute-force attacks, devices can be set up to lock their contents, typically after 10 consecutive incorrect code entries. In highly secure settings, a device can be programmed to erase its contents after a series of failed login attempts.

The chances of success for a brute-force attack can be decreased exponentially by using longer alphanumeric access codes. A 4-character, case-sensitive alphanumeric passcode with 26 lowercase, 26 uppercase, and 10 numeric options for each character theoretically has $62^4$ (14.7 million) possible combinations, which would require a 342-day brute-force attack to attempt all combinations. However, the 14.7 million options are not likely random, and it is common for device users to choose familiar words and patterns.

For this reason, an alphanumeric code of at least 6 characters (without using words from the dictionary) is typically recommended for medical use. Devices can be configured with a centralized institutional password server, such as lightweight directory access protocol, which allows a user to gain access to a device, an application on the device, or a specific service such as access to an e-mail account with an institutional login. Compared with managing a specific password for each device, lightweight directory access protocol servers have an improved password management workflow and also allow users to update the password for all devices at once, from one central location. Although it seems obvious, it is worth noting that a password is not secure if it is written in a notebook (unless the notebook itself is secured) or on a card in a wallet. Encrypted password management tools, electronic wallets per se, exist with military-grade encryption (such as 1,024-bit encryption). Individuals who worry about remembering their multitude of passwords should use a tool such as this, but it is critically important to have a very secure password to access the electronic wallet (and it goes without saying that this password should not be written in a notebook!).

Devices that have been lost or stolen are especially susceptible to data security compromise. Major platforms often have remote Global Positioning System localization features for lost devices and may have the ability to remotely enter a command to deactivate a device and delete all data it contains. If available, these features should be implemented for devices that may be used for access to protected health information (PHI).

Additionally, some applications within a device require passwords, and this is especially important for shared-use devices. Using an application password that differs from the device password is required if individuals who should not have access to application-specific data, such as PHI, have the device-access password. In other words, if a doctor allows her husband to use her smart phone, he should not have access to patient data.

Mobile device data are typically stored, at least in part, on the device. This is true even in situations in which data are accessed through a remote server because local copies of the data (“cache”) are typically stored for rapid retrieval. Applications that access PHI should use data encryption when storing data on the local device to prevent other applications and viruses from accessing the information. With encrypted and compartmentalized storage areas for data from separate applications, a process known as “sandboxing,” the chances of either

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Other Names</th>
<th>Wired/ Wireless</th>
<th>Maximum Range</th>
<th>Maximum Speed</th>
<th>Typical Speed†</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB 2</td>
<td></td>
<td>Wired</td>
<td>Length of cable (signal loss after ~1.5 m)</td>
<td>480 Mbit/s</td>
<td>280 Mbit/s</td>
</tr>
<tr>
<td>USB 3</td>
<td></td>
<td>Wired</td>
<td>Length of cable (signal loss after ~1.5 m)</td>
<td>5 Gbit/s</td>
<td>~3 Gbit/s</td>
</tr>
<tr>
<td>Bluetooth 3</td>
<td></td>
<td>Wireless</td>
<td>100 m</td>
<td>24 Mbit/s</td>
<td>~10 Mbit/s</td>
</tr>
<tr>
<td>Bluetooth 4</td>
<td></td>
<td>Wireless</td>
<td>100 m</td>
<td>24 Mbit/s</td>
<td>~10 Mbit/s</td>
</tr>
<tr>
<td>Wi-Fi–g</td>
<td>802.11/g</td>
<td>Wireless</td>
<td>140 m</td>
<td>54 Mbit/s</td>
<td>~10 Mbit/s</td>
</tr>
<tr>
<td>Wi-Fi–n</td>
<td>802.11/n</td>
<td>Wireless</td>
<td>250 m</td>
<td>600 Mbit/s</td>
<td>50 Mbit/s</td>
</tr>
<tr>
<td>Cellular 2.5G</td>
<td>EDGE</td>
<td>Wireless</td>
<td>Several miles</td>
<td>1 Mbit/s</td>
<td>20 Mbit/s</td>
</tr>
<tr>
<td>Cellular 3G</td>
<td></td>
<td>Wireless</td>
<td>Several miles</td>
<td>14 Mbit/s</td>
<td>2–4 Mbit/s</td>
</tr>
<tr>
<td>Cellular 4G*</td>
<td>LTE</td>
<td>Wireless</td>
<td>Several miles</td>
<td>300 Mbit/s</td>
<td>20 Mbit/s</td>
</tr>
</tbody>
</table>

*The 4G designation has different industry and legal definitions in different countries.
†Typical speed based on real-world performance can vary significantly.
unintentional or surreptitious access to application data by outside sources are decreased significantly. These features are typically implemented by the developers of both the mobile operating system and the specific app, so the individual user may not have control over these issues but should nonetheless be aware of them. Those individuals seeking to develop or contract applications for their institutions should be aware of this and require developers to adhere to appropriate security practices.

The major mobile device platforms do not currently have built-in virus protection software, and the iOS platform will not allow third-party software access to memory assigned to the system and other applications, which would be required for a virus protection program to function. However, sandboxing and digital signatures of the applications themselves can improve security. As for desktop computers, viruses and malicious applications (“malware”) exist for mobile devices, and though such applications have not been as widespread as in their desktop counterparts, this is rapidly changing. Threats from mobile malware increased by 58% in 2012, and about a third of the attacks appear to involve stealing information, which may lead to identity theft [1].

Google’s Android platform has experienced more mobile malware than Apple iOS. The Android platform and device have a much larger market share, which may attract more malware writers to target as many devices as possible. In addition, the openness of the Android platform and multiple distribution methods for apps (eg, the ability to sideload apps from a website or from a personal computer instead of downloading from the Google Play store, which is a more trustworthy source) make it the most popular platform for malware creators. However, Apple iOS is not immune to malware. Indeed, Symantec’s Internet Security Threat Report 2013 [2] noted 387 documented vulnerabilities in 2012 on Apple iOS, compared with only 13 in the Android system. However, as noted in the report, vulnerabilities do not necessarily translate into threats (only one known threat has been found to be created for all the iOS vulnerabilities).

Both the Android system and iOS have screening processes for mobile apps in their respective app stores, but 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 late 2012, it was discovered that two iOS apps had tethered undetected functionality using such seemingly innocuous app names as DiscoRecorder and FlashArmyKnife [3]. One might imagine that malware can also slip through this review process. In fact, in April 2013, BadNews, a new malware family, was discovered in 32 Android apps across 4 developer accounts. The combined affected applications had been downloaded between 2 million and 9 million times (Google does not provide exact numbers). This particular malware masquerades as a mobile advertising network, which can send fake news messages asking users to install applications and can steal sensitive information about users and their devices. This new family of malware exists without the knowledge of the developers, appearing as a third-party ad framework, and its malicious behavior is controlled by a server. Apparently, the delay of these malware attacks, which go into effect only long after the apps are released and downloaded, made it difficult to detect while the apps went through the standard vetting process. In summary, ensuring security in the health care environment is becoming more complex, and responsibility lies with both app developers, who must be aware of third-party libraries used, and enterprise IT managers, who should monitor security continuously to detect malicious behavior of even vetted and approved apps.

Applications distributed from the iOS iTunes App Store require digital signatures from registered developers. Native applications for iOS otherwise cannot be distributed via official means, and although some individuals feel this limits user flexibility, it is clear that this method also significantly limits the impact of malicious applications. The Android ecosystem is more open than the iOS system by design, which gives developers and users significant flexibility but also provides a pathway for a multitude of malicious apps. Mobile devices typically access information wirelessly, most commonly through Wi-Fi and cellular networks. The data-transfer signals are detectable by other devices in the area. Data encryption is critical for any communications using PHI.

Data-transfer security is generally understood to be as strong as the weakest link, so encrypting the entire series of communication between the remote server and the mobile device is required, which is known as end-to-end encryption. Publically accessible Wi-Fi networks, whether complimentary or available for a fee, typically send unencrypted data that can be read by other individuals on the network using freely available tools known as “packet sniffers.” For this reason, it is unadvisable to access medical information using public Wi-Fi networks such as those at libraries, coffee shops, and airports, without using additional security measures. Home Wi-Fi networks should be secured using an encryption protocol. The earliest implementation of home Wi-Fi encryption is known as wired equivalency protocol, which is no longer considered appropriately secure for medical purposes. Wi-Fi protected access, a more secure variant, should be implemented. Version 2 of Wi-Fi protected access further increases security.

A virtual private network (VPN) can make these unsecured public networks safe. A VPN is an encrypted tunnel of data between two devices. Typically, this is used by a device connecting to an institutional server. When this is performed, the encrypted tunnel of data can be transferred over a public network without compromising data security. A packet sniffer may be
able to intercept the communications, but because the communications are encrypted, the data will be unusable without an enormous amount of computing prowess and power. VPNs are most often administered by institutions, but more recently, some home routers offer VPN capabilities.

In sum, to ensure adequate security when using a mobile device:

1. Use a strong password for the device.
2. Use app passwords for a second layer of defense (especially if an app has PHI).
3. Ensure that apps store encrypted data.
4. Ensure that apps transmit encrypted data.
5. Be wary of other downloaded apps; do not assume they are virus free.
6. Recognize that vetted software can contain viruses if such software relies on third-party components.
7. Consider using a VPN to secure all communications with your institutional server.

REGULATION

In the United States, the practice of medicine is regulated by state governments, not the federal government. Each state government decides what is considered the standard of care, normative practice, and substandard care and malpractice. Medical devices, on the other hand, are regulated by the FDA. Doctors are at liberty to use both medical and nonmedical devices to practice medicine and treat patients. For example, a stethoscope is a regulated medical device, but a general purpose magnifying glass that a doctor uses to examine a patient’s skin is not, assuming it was not sold for that specific purpose.

States’ departments of health (DOHs) and the FDA play a role in the use of mobile devices for patient care. State governments can hold a doctor accountable for improper use of a device if the doctor fails to use it in a medically acceptable manner and adversely affects patient care. The FDA regulates the manufacturers of mobile medical devices, ensuring that they are safe and effective to use.

Clearly, smart phones and tablets are not made to be medical devices, and neither are computers. What transforms a regular device into a medical device is the intended use to diagnose or treat a patient. Such intended use in the case of mobile devices is an attribute of the software (the app), not the device itself. To illustrate, if a physician bought headphones to listen to music from her smartphone, the state DOH or the FDA has no issue. If the physician were to buy a microphone, attach it to the phone, and then use it to listen to a patient’s heartbeat, the FDA would have no issue with the manufacturer of the headphones, smart phone, or microphone because none of those items was marketed as a medical device. The DOH, on the other hand, can hold the doctor accountable if she misuses the instrument she created and thereby improperly cares for the patient. However, if a company were to sell just the headphones and microphone as a package and market it as a solution for physicians to listen to heart sounds in conjunction with a smartphone, then that company would be subject to regulation and held accountable by the FDA for selling a medical device.

The regulation is similar when viewing radiologic images on a mobile device. If radiologists use nonmedical software to view patient images, such as the photo gallery software on the phone or tablet, there is no FDA regulatory issue. However, radiologists are required by federal law to protect the confidentiality of patient data, and their practice of medicine is regulated by the DOH. If the software is marketed as an adjunct to PACS to enable mobile radiologic image viewing for primary diagnosis, then that software company must obtain FDA approval, typically as a class III medical device, which requires premarket approval. Image viewers meant only for clinical review and not primary diagnosis more likely fall under class I or II.

Therefore, to protect both patients and doctors, patient images not deidentified and viewed for diagnostic purposes should be viewed using only FDA-approved software. This approval should ensure that when used properly, the software provides appropriate security and will render images in a diagnostically acceptable format.

PLATFORMS

Introduction

From social media to maps to politics, the importance of mobile apps has never been greater, and they will continue to have a huge impact in health care. In the consumer world, the quality of mobile apps often determines the rise or fall of a company, and indeed, many startup companies have mobile-first (or mobile-only) strategies. In late 2010, Facebook had an HTML5-driven mobile native app, which many people considered slow and unstable.

Around that time, a small startup called Instagram, with only 13 employees, created a very useful native app for sharing photos and had more than 30 million users after just 18 months. Facebook eventually acquired Instagram, a company with no revenue, for $1 billion in April 2012 because photo sharing was considered one of Facebook’s main strengths.

What can health care learn from the Instagram story? You will likely need a high-quality mobile app with consistent performance. Otherwise, you should be prepared to lose market share to other organizations with better apps and to damage your reputation as a hospital or company that delivers high-quality products and services. Another lesson might be that native apps are much more popular than web apps. At least initially, web apps will sometimes make more sense to develop because they run in a web browser and will work on almost all desktop
(Windows and Mac) and mobile (iOS and Android) devices. However, most people prefer the user experience of native apps, which were designed specifically for a device—native buttons, animations, responsiveness, and so on. It is more work to customize the design of an app for each of these device types, but it has been shown to significantly increase the appeal of the app.

**Mobile Health (mHealth)**

It is projected that by 2015, 500 million people will use health care apps, so organizations will likely need mobile strategies, whether they are companies, large hospitals, or small radiology practices [4]. Some potential economic benefits from adopting a mobile strategy include lower costs for elderly care, better access to doctors for rural patients, and improved health data collection. These benefits stem largely from the camera, location sensor, and other sensors on board mobile devices, which can be used to track chronic conditions without necessitating a physical office visit.

At a minimum for the radiology specialty, health care providers will want to use mobile apps to access images and reports. Radiologists will want apps to improve daily workflow, such as the protocling of examinations or looking up patient information. Patients will also want mobile access to their imaging results.

A survey showed that there is a large percentage of potential mobile health care app users, including 62% of doctors who use tablets (50% at the point of care) and 71% of nurses who use smart phones at work [5]. There were 13,000 health apps in 2012 (6,000 for medical professionals), with 44 million apps downloaded in 2012 and a projected 142 million downloads by 2016 [6].

Currently, mHealth use by health care organizations is dominated by more general apps, such as those to access call centers for hospitals and insurance companies, because they are easier to deploy. mHealth for tasks such as patient monitoring and decision support is not as common, likely because such programs or apps have more complex requirements [4].

For patients, health and wellness apps help manage medication adherence, diet, stress, sleep, fitness, chronic conditions, smoking cessation, personal health records, and so on. In many ways, the fact that patients are adopting consumer health mobile apps will make it easier for health care professionals to also transition to mobile.

The majority (up to 75%) of physicians are using iOS devices, according to a 2011 survey [7]. Although doctors by far prefer the Apple iPhone, consumers are adopting Google Android smart phones by a wide margin. In the third quarter of 2012, Android purchases accounted for 72% of worldwide smart phone sales, whereas Apple iPhone sales were only about 14% [8]. Therefore, any mobile strategy in the near future must include support for these platforms to include both health care providers (mostly iOS) and also patients (mostly Android).

Although a number of platforms are available, including a few relatively new ones such as Windows 8 Mobile, we focus on the two dominant platforms: Apple iOS and Google Android.

**Current Platforms**

**Apple iOS.** The Apple iOS (originally iPhone OS) launched in 2007 with the iPhone 1. A new iPhone has subsequently launched every year since, with the iPhone 6 being the latest model at press time. The iPhone has consistently been the best-selling smartphone. Year after year, with each new iPhone model, the number of phones sold have increased. In the recent release of the iPhone 6 and 6 plus, over 10 million phones were sold in the first weekend, compared with 9 million phones for the first weekend in the launch of the iPhone 5s and 5c [9]. The Apple iPad is also the best-selling tablet device, with more than 225 million of these tablets sold since 2010 [10].

**Google Android.** Android launched in 2008 with the G1 Android. Google’s approach has been very different from Apple’s; the core components of the Android platform are open source. As a result, Android has been adopted by several different manufacturers as well as more wireless carriers (compared with Apple iOS when the iPhone went on the market in 2007), with many more price plans, including prepaid options. By 2011, only 3 years after its initial release, Android became the dominant mobile platform, with support by more than 230 carriers in more than 120 countries and 39 manufacturing partners [11].

Many more models of Android smart phones exist compared with Apple (which, as of press time, has only released one flagship model per year). Numerous Android devices present consumers with choices and different pricing options but also present challenges for manufacturers and Google to be able to support the hardware and keep devices up to date with the latest software (ie, fragmentation). Indeed, software updates for the latest Android vary dramatically by device, and it is mostly up to the manufacturer to provide these updates. A large number of devices thus remain on older versions of Android.

In contrast, Apple will typically support much older hardware with its iOS releases, until the hardware is incapable of such support. Although the Android system itself provides developers with flexibility in developing apps, the many models and specifications (eg, screen size) of Android devices also create a challenge. Companies developing Android apps often have to test apps on several (if not hundreds, especially in Asia) Android devices to ensure quality assurance.

In addition, because Android is open source, any company can download the Android code base and start its own customized version of Android, which may no longer be compatible with Google’s version of Android (called “forking”). Two of the most commonly known Android forks are for the Amazon Kindle Fire device and the Barnes and Noble Nook device.
APPs
Mobile apps for radiology can be categorized into one of the following: image viewing, education, decision support, and journals and societies.

Image viewing apps allow referring physicians to access imaging studies anywhere. Although many of these applications are self-described as “not for diagnostic use,” the FDA and Health Canada have cleared a number of iOS applications, such as MobileMIM, for diagnostic reading when no dedicated workstation is available. These applications typically provide basic image manipulations such as scrolling, adjusting window and level, zooming, panning, and measuring length.

Radiology reports can also be viewed using some of these applications, and there are even applications dedicated to viewing reports, allowing referring physicians to receive encrypted imaging interpretation report documents.

In a survey conducted by Korbage and Bedi [12], 74% of radiology residents own smart phones, and 37% own tablet devices. The surveyed residents spent nearly an equal amount of time learning radiology from printed textbooks as from electronic resources. The survey results demonstrate considerable use of online and electronic resources and mobile devices among the current generation of radiology residents.

Under the category of education, there are textbooks, case reviews, syllabi, encyclopedias, and quiz applications. Text can be highlighted in some of these applications, and notes can be added. Built-in search capability allows rapid information look-up within these texts. Some of these applications provide embedded animations and videos to further enhance education. By allowing users to interact with the images (such as scrolling and adjusting window and level), some of these applications enhance learning by simulating real-life reading situations. Additionally, other educational materials exist, such as guides on meaningful use in radiology. Moreover, applications on anatomy can serve both educational and decision-support purposes.

Various decision-support applications exist and perform such tasks as providing differential diagnoses, facilitating communication between radiologists and referring physicians, and calculating laboratory values and other measurements such as glomerular filtration rate, amount of contrast needed for examinations, and even bone age.

Many medical journals, such as RadioGraphics and Radiology, allow users to view journal articles through mobile apps. Various societies have also created applications that support respective annual meetings.

Display
Image Types
To understand the appropriateness of using mobile devices to view radiologic images, it is worthwhile to review the varieties of radiologic images and their relevant digital image display parameters.

Radiographs are typically the largest images radiologists view in terms of the number of pixels. A full-resolution image ranges from 4 to 12 megapixels (MP), and 1 MP accounts for 1 million pixels. Furthermore, to properly assess such an image usually requires a view somewhat close to life sized. Contrast this with a whole-body nuclear medicine image, in which the spatial resolution is so low that there is no loss of diagnostic information when viewing an image of the whole body, from head to toe, within a few inches. Furthermore, the inherent contrast of diagnostically significant findings in radiographs tends to be low; radiologists look for subtle calcifications, nodular opacities, and luencies that may represent pneumothorax or fracture.

CT, MR, ultrasound, and nuclear medicine images have many fewer MP per image, usually no more than 0.25 MP, and the inherent contrast of diagnostically significant findings in these images is typically high. Small locules of gas in a CT scan are quite conspicuous when viewed with the proper window and level settings.

Mammograms are of even higher resolution than regular radiographs, and almost all findings within such images are of subtle contrast.

Display Size
Typical desktop PACS displays are approximately 21 inches in diagonal, tablet displays are about 10 inches, and phones are about 3.5 inches. No matter how many pixels are crammed into that area, the display size of a phone is just too small to adequately view a radiographic image. Even with repeated zooming and panning, one can see neither a zoomed-out view of the image with enough detail nor a zoomed-in image with enough context, for primary diagnosis. A phone’s hand-sized viewing area is too small to properly assess a full chest or abdominal radiograph. Although tablet displays are also significantly smaller than the true size of a chest, for example, the mismatch is not as severe. As such, viewing a chest radiograph on a tablet versus a desktop display does require more zooming and panning to perform a full diagnostic survey of the image data, but if given the proper time to do so, the outcome is likely equivalent. This is fortuitous because the primary purpose of mobile devices is to trade the large scale of desktop displays for a more compact display to be used only occasionally while on the go.

Few radiologists would prefer a tablet versus a full-size desktop display to interpret a daily load of diagnostic radiographs. Tablets were not designed or intended to supplant larger desktop displays in such contexts. Rather, the main benefit of tablet displays is the ability to look at one or two examinations for consultation while not at work or in front of a full-size workstation. A classic example is the radiology resident on call who has a question about a difficult case requiring subspecialty expertise to view radiologic images, it is worthwhile to review the varieties of radiologic images and their relevant digital image display parameters.
expertise from a pediatric radiologist or neuroradiologist who is not at home but is reachable by phone. In that case, the attending radiologist can use his or her tablet to spend enough time looking at the images to answer the particular clinical question. The additional viewing time beyond that required for a full-size desktop display does not pose a problem because it is only for one or two examinations, and it is negligible given the overall amount of time spent on the ad hoc consultation. This mobile viewing is also much more worthwhile than forcing the attending radiologist to drive home or to the hospital to answer the clinical question. Thus, for the primary use case of ad hoc consultation, it is adequate to view radiographs on a tablet, although perhaps not on a handheld phone.

For CT, MR, ultrasound, and nuclear medicine images, though, with their much smaller native spatial resolution, the 3.5-inch display of a smart phone is likely adequate for the on-call consultation scenario. Again, it is not enough to work with when trying to interpret a daily workload of examinations, in which efficiency requires the display of multiple image stacks—current versus prior, pre- versus postcontrast, axial versus coronal views, and so on. If a radiologist is simply trying to answer a focused clinical question, it will take more time to reach the answer with the reduced display size of a smart phone, but it can reasonably be done. Tablets are even more suitable, but they are less convenient and therefore less available than smart phones.

Pixel Pitch

Pixels, a contracted form of the phrase “picture elements,” are generally square, and the length of one side of the square is the pixel pitch. The pixel pitch ranges from 270 μm for low-resolution desktop displays to 78 μm for the latest iPhone with “retina display.” The greater the number of pixels, the more information can be displayed in a fixed area.

However, note that the entire purpose of a display is to convey information to the human eye. Once the pixels are so small that they are below the threshold of human perception, there is no point in making them smaller. They can display more information, but it will not be perceived. Whether a pixel, which may be very small, is perceptible depends primarily on the viewing distance. The farther the display from the eye, the larger the pixels may as well be because making them smaller does not help.

The viewing distance is also related to the size of the display. That is, the smaller the display, the closer it tends to be held to the eye. Likewise for smaller displays, the pixels are made smaller to avoid pixilated images. This is why the smallest pixels are in phones (phones are often held a mere 6–8 inches from the eyes). The latest tablets boast a 3-MP display, which yields a pixel pitch of 96 μm, which makes sense because this is slightly larger than that of phones.

However, recognize that other factors come into play when it comes to the threshold of human perception, such as visual acuity and the effect of aging. Radiologists who routinely use magnification to overcome reduced visual acuity are not likely to benefit from displays with smaller pixel pitches. Similarly, those who are more comfortable looking at tablets on their laps or a little farther away than average will not benefit from smaller pixel pitches.

Luminance

The ability to discriminate contrast in radiologic images is highly dependent on sufficient display luminance, or brightness. Radiologic images typically contain about 256 shades of gray that are meant to be perceived by the human eye. If some gray shades are too close to each other to the point that a photometer can distinguish them, but the eye cannot, then the display has failed to serve its purpose. Fortunately, mobile devices are designed to emit high luminance to compete with high ambient light. Imagine being unable to use your phone outdoors in direct sunlight. The advent of light-emitting diode displays has enabled mobile devices to output luminance of 400 to 500 cd/m², which is on par with desktop medical displays. However, mobile devices are also designed with extensive power management features, which can dim the display during periods of nonuse or if the device senses low ambient light. Therefore, care must be taken to determine if display dimming is controlled by the viewing application. If not, the radiologist may need to take other steps to prevent it, such as periodically manipulating the app to prevent the phone from entering standby mode and dimming the display.

Calibration

All displays have an output function, also called a gamma. The DICOM standard sets a specific grayscale display function that is designed to preserve contrast at the edges of the contrast spectrum—the darkest grays and brightest grays—and allow the radiologist to perceive a smooth transition from one end of the spectrum to the other. This is akin to creating a road that goes up a mountain at fixed angle, with no sudden sags and no sudden inclines. This way, all the contrasts in the digital image are conveyed, none are lost, and none are over- or underemphasized.

Traditional methods of calibrating a display cannot be applied to mobile devices because unlike desktop machines, mobile video subsystems cannot be altered by software. Moreover, most of them do not have a method of attaching a photometer, which is needed to allow the device to measure how much light is actually produced from a digital input. This feedback is necessary for the device to correct its output, much like giving people mirrors so they can see themselves and make adjustments to their appearance.

Necessity is the mother of invention, and instead of using a photometer to adjust a device and determine if its
output is correct, methods were developed to use something even better: humans themselves. After all, it is the human user for which these adjustments are made (to ensure the perception of all image contrasts). As such, tests such as the tap test were devised to determine if the display accurately portrays the grayscale range and to give the display feedback to make adjustments if it does not. One way of doing this is to present the user with subtle computer-generated discs on the screen that simulate pulmonary nodules and differ slightly from the background shade of gray, and ask the user to tap on them when they appear. The accuracy of the user’s taps is an indicator of the perceptibility of the contrasts at different disc and background levels. The beauty of this method is that it takes into account not only the device but also the ambient light and the eyesight of the radiologist. If initial tests fail, the device will attempt to alter the way it presents contrasts to compensate and find a gamma that allows proper contrast perception. If it cannot compensate, it indicates this to the user, and the user is told not to use the device under these circumstances.

What should the user do if the calibration fails? First, he or she can try moving to a place with less ambient light, such as indoors or a shaded area. If that does not work, perhaps the device needs service. If the device is found to be in working order, perhaps it is the radiologist who needs a new eyewear prescription. What makes mobile device calibration in some ways superior to traditional methods is that it includes the user as part of the test. As such, it actually determines what we really want to know when we calibrate a device: can he or she really see what is supposed to be seen?

**SUMMARY**

Mobile devices are here to stay and are already in the pockets and handbags of most physicians, radiologists, referring clinicians, and patients. Radiologists need to consider a mobile strategy that not only enables viewing images for diagnosis on a consultative basis but also enriches referring clinicians’ electronic medical record experience and the personal health records of the patients they serve. Solutions abound from both PACS and electronic medical record vendors, but careful product selection and judicious use are necessary to advance medical care while protecting patient confidentiality. Sustainability and ease of use are equally important to consider given the rapid growth and fluctuation of this societal technology. It is the responsibility of the radiologist to securely and effectively use mobile technology in the best interests of patient care, and these guidelines are intended to facilitate this process.

**TAKE-HOME POINTS**

- Every radiology facility needs a strategy to make its images accessible for mobile viewing for both doctors and patients.
- Medical image viewing software needs to be intelligently designed to make effective use of the low bandwidth of mobile networks; poorly designed software will cause frustration, especially when trying to navigate large image sets.
- Mobile software needs to ensure the security of patient data, preferably by using encryption during transmission and not keeping any data on the device after the viewing session has ended.
- Regulation is needed to ensure the safety and clinical efficacy of mobile medical software.
- The minimum size of a mobile display depends on the image type and the clinical use case.

**REFERENCES**