Use of Mobile Devices for Medical Imaging

David S. Hirschorn, MD[a], Asim F. Choudhri, MD[b,c], George Shih, MD[d], Woojin Kim, MD[e]

Mobile devices have fundamentally changed personal computing, with many people forgoing 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

J Am Coll Radiol 2014;11:1277-1285. Copyright © 2014 American College of Radiology

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.

[a]Department of Radiology, Staten Island University Hospital, Staten Island, New York.

[b]Department of Radiology, University of Tennessee Health Science Center, Memphis, Tennessee.

[c]Department of Radiology, Le Bonheur Neuroscience Institute, Memphis, Tennessee.

[d]Department of Radiology, Cornell University Medical Center, New York, New York.

[e]Department of Radiology, Hospital of the University of Pennsylvania, Philadelphia, Pennsylvania.

Corresponding author and reprints: David S. Hirschorn, MD, Staten Island University Hospital, 475 Seaview Avenue, Staten Island, NY 10305; e-mail: hirschorn.david@mgh.harvard.edu.

1546-1440/14/$36.00 • http://dx.doi.org/10.1016/j.jacr.2014.09.015

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