BNA, INC.

PRIVACY & SECURITY LAW

REPORT

BNA Employee-Owned Since 1947

The Proliferation of Mobile Devices and Apps for Health Care: Promises and Risks

By Peter McLaughlin

Peter McLaughlin is senior counsel in the Boston office of Foley & Lardner LLP and is a member of the firm's Privacy and Healthcare practices. He advises health care clients with regard to HIPAA compliance and particularly the use of health information technology. Before joining the firm, McLaughlin was Assistant General Counsel for Privacy and Security at Cardinal Health, Inc., a Fortune 20 health care company. He is vice-chair of the ABA's Information Security Committee.
The opinions expressed in this article are his own and do not necessarily reflect those of the firm or any clients.

1) Introduction

The popularity of smartphones like the Droid and iPhone as well as tablet devices such as the iPad means that people are able to accomplish many things without physically sitting in front of a computer or even being in the office. Apple currently claims over 90,000 apps for the iPad, many of which are in the health and health care category. After weeding out those directed toward consumers, several hundred are intended for physicians, nurses and clinicians. These health apps range from disease reference guides to remote EKG monitoring, which may also be connected to an EHR (electronic health record).

The promise of such devices and applications is that enhanced mobility and access to information will improve the way in which physicians and their teams interact with patient health information. Physician groups and hospitals should consider the implications, however, of how they use these devices. While a small number are regulated to date by the FDA as medical devices, the storage and wireless transmission of PHI (protected health information) to and from these tools means that the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule will impact covered entities and business associates using them.

The benefits of health apps on mobile devices, then, must be balanced against the extra care required to ensure that doctors and others are properly protecting the data on these devices. In addition to the Security Rule, the new Health and Human Services Breach Notification Rule and associated Technology Guidance apply. In an era when people seem to lose portable devices with remarkable frequency, it is important to consider how to incorporate mobile devices into a practice and validate that the device or application(s) can support your compliance with HIPAA and other rules.

2) Proliferation of Devices and Apps

In releasing a study on physicians' use of technology, Manhattan Research reported in May 2011 that thirty percent of doctors are using iPads to access EHRs, to view results such as radiology images, and to communicate with patients. While a search for ''health'' on the iPad App Store yields a wide variety of consumer-oriented tools, an increasing number of these apps facilitate a physician's practice.

A quick review of iPad apps for doctors, nurses and clinicians displays a wide range of these tools. These include apps for drug-interaction checkers, medical dictionaries, diagnostic lab tests tools and disease treatment guides. While most of these apps are used as reference sources and thus would not contain any PHI, an increasing number provide access to EHRs, capture patient data, transmit prescription renewals, and clinical decision support. Many of these apps also provide for the remote monitoring of patient vital signs, such as an EKG-reading app, accessing patient charts and x-ray images. There is also a new blood pressure monitor that has received FDA approval. A recent study by PricewaterhouseCoopers estimated that the annual market for mobile monitoring devices ranges from $7.7 billion to $43 billion.[1]

3) Keep HIPAA in Mind

a) HIPAA Security Rule

Arguably, one of the drivers of mobile devices in health care is the federal government's push to move patient records into digital systems or EHRs for which the Health Information Technology for Economic and Clinical Health Act (HITECH Act)[2] provides significant funding over the coming years. With the financial incentives, however, the HITECH Act expanded portions of HIPAA directly to business associates and initiated breach reporting obligations for covered entities. As physicians increasingly leverage iPads and similar devices for managing patient data, it remains critical that these devices and apps enable health care users to comply with the requirements of the HIPAA Security Rule.

The HIPAA Security Rule applies to electronic PHI held by covered entities[3] and, since the amendments of the HITECH Act, business associates. Section 164.308(a)(1)(ii)(A) of the Security Rule requires that a covered entity conduct a risk analysis to assess the nature and volume of ePHI and the risks of unauthorized use or disclosure of this patient information. A covered entity must then implement administrative, technical and physical safeguards appropriate to the risks and vulnerabilities identified in the risk analysis. The purpose of these safeguards is to assure the confidentiality, integrity and availability of patient information.

The challenge presented by the proliferation of mobile devices and apps storing PHI is that enhanced mobility and remote access to patient information dramatically complicates successful implementation of the safeguards required by the Security Rule. Hospitals and physician groups often struggle to maintain control of PHI in the current environment, if the increasing reports of PHI data breaches are any indicator.

The Security Rule presents a series of required and addressable measures as part of a covered entity's implementation program. These include common security practices such as applying access controls to files and applications, authenticating users to verify that the correct person is logging in, and audit trails to validate access to this sensitive information. Therefore, before using an iPad or similar device to handle patient information, consider how the device and its apps will fit within your security compliance. For example, does the device itself allow for the encryption of some or all of the data files? If the device is lost, is there a way to remotely wipe or erase information? Do specific health apps enable encryption of ePHI on the device? How sophisticated are the password protocols on the device and do they conform to your hospital's or practice group's information security program?

When reviewing the HHS list of reported breaches, many involve portable devices, such as laptops for which disk and file encryption are readily available. The risk to consider is that iPads and similar tablets will increase these numbers if they are not properly configured to secure any PHI they hold. To determine precisely how to apply such configurations, HHS has issued technology guidance to distinguish between secured and unsecured PHI.

b) Impact of HHS Technology Guidance

In conjunction with the HHS Breach Notification Rule, the Office of Civil Rights issued ''Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals'' to assist covered entities and business associates determine when PHI was ''secured'' and thus not subject to the reporting requirements applicable to ''unsecured PHI.'' The guidance from OCR provides that PHI will be rendered unusable, unreadable or indecipherable to unauthorized individuals if the electronic PHI has been protected in accordance with three specifications published by the National Institute of Standards and Technology (NIST). It is important to note that HHS is not requiring the application of this ''guidance,'' but the failure to do so enhances the risk that PHI on mobile devices will not be protected in accordance with the Security Rule.

The Security Rule defines encryption as the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. (45 C.F.R. 164.304). The NIST specifications, which typically apply to government information systems but have increasingly been considered as technology standards for the private sector, have been determined to meet the Security Rule's encryption definition and apply to data when it is at rest (stored),[4] when it is in transit,[5] and when it is ready for destruction.[6]

[1] PricewaterhouseCoopers, ''Healthcare Unwired'' (Sept. 2010).

[2] Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5.

[3] 45 C.F.R. § 164.302.

[4] NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices

Each component of the OCR Technology Guidance applies to mobile devices in the health care space and should be a consideration of their development and selection. iPads and similar devices may be configured to store patient information requiring questions of whether the device itself enables encryption or if that needs to be a feature of any health app. It is also important to validate that the encryption used conforms to the relevant NIST standard, as OCR has not indicated that encryption tools meeting other specifications will be acceptable.

Likewise, the benefit of mobile devices is precisely the fact that you are now untethered from a desk or cable connection. The OCR Technology Guidance states that ePHI in transit—winging its way across a wireless network—be sent and received through a secure link. Applying security to the WiFi network of a hospital or physician practice is manageable and highly recommended. But if the physician reading the EKG report is at home or at an airport or a coffee shop, then how is that connection secured? The iPad and similar devices have apps that allow for these secure sessions (much like when you see the closed padlock symbol on your browser when logging in to your bank account). The question remains, though, of how carefully the iPad and its health apps have been configured. For most people, we are happy enough that we need only click ''download'' and the app market delivers.

c) Breach Notification Rule

The health care sector has been subject to a lot of scrutiny following commencement of the Breach Notification Rule on Sept. 23, 2009. While the requirements of the interim final rule published by HHS in the *Federal Register* on Aug. 24, 2009, have been discussed extensively, the implications for patient data on mobile devices and the attendant risks should be evident. The rule applies to breaches of unsecured PHI, which is defined in the regulations as ''protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the [Technology Guidance] . . . .'' (45 C.F.R. § 164.402). The features of devices and applications to enable protection of patient data in accordance with the Technology Guidance will significantly affect whether a lost device constitutes a notifiable event.

Of course, a prerequisite to any such notification is understanding what patient information is on the device or accessible through applications. As mentioned earlier, a significant number of physicians surveyed access an EHR through an iPad or similar tablet. If remote access to patient files does not typically involve saving patient data onto the device, then loss of an iPad may involve some risk (of unauthorized access to the EHR via the app) but potentially less risk than if PHI had been in the device memory. A challenge, however, is that many apps enable the saving of files onto the iPad. How, then, is one to know whose data and precisely what information was on the device? This has presented a challenge for laptops, and because iPads and similar technologies are less likely to be synchronized with centralized systems, it may be much more difficult to respond to a security incident because of uncertainties about the data involved.

4) Risks and Liability

As with the ubiquitous use of laptops, the popularity of iPads and other mobile devices in the health sector will present compliance challenges for professionals. The benefits of mobility and remote access to patient information cut both ways, as mobility and remote access mean that PHI can be collected, reviewed, and lost that much more easily than when restricted to an office environment. Ensuring that devices and their apps enable encryption will go a long way toward compliance. Training users with respect to secure wireless communications will also be essential. Unfortunately, initial reports do not bolster confidence in the proper implementation of either encryption or wireless security.

In the PricewaterhouseCoopers ''Healthcare Unwired'' report, more than a third of doctors surveyed expressed concern over privacy and security as their chief barrier to using mobile health applications. The recent report from the HHS Office of the Inspector General, released May 16, did little to allay these concerns.[7] In reviewing enforcement of the HIPAA Security Rule, the HHS OIG found that oversight and enforcement was not sufficient to ensure that covered entities effectively complied with the rules. Furthermore, OIG conducted audits of seven hospitals and identified 151 vulnerabilities within information systems and controls intended to protect PHI. Some of the high-impact vulnerabilities identified by OIG included wireless access controls, audit controls, and device and media controls. These are precisely the areas implicating mobile devices.

The details of the OIG report present a list of ineffective safeguards for PHI. The wireless vulnerabilities included ineffective encryption, a failure to separate wireless from internal wired networks, the lack of user authentication, and the inability to detect unauthorized devices intruding on the wireless network. Similarly, the audited hospitals did not always have an accurate inventory of computer equipment and devices authorized to access the hospital network. Many of these also presented no policy for removing ePHI from devices. These operational challenges are difficult enough when the hospital owns the computer equipment. Because the evolving use of iPads and other tablets in the health care sector almost certainly means work applications on personally owned devices, it will become more difficult for covered entities and business associates to protect PHI in their control.

The results of the OIG report are consistent with concerns raised by the Ponemon Institute in its November 2010 Benchmark Study on Patient Privacy and Data Security. The Ponemon Institute examined privacy and data protection compliance activities across health care organizations. This included reviews of policies, program management activities, enabling security tech-

[5] NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 (Security Requirements for Cryptographic Modules) validated.

[6] NIST Special Publication 800-88, Guidelines for Media Sanitization.

[7] HHS ''Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight'' (May 2011), available at http://oig.hhs.gov/oas/reports/region4/40805069.pdf.

nologies and security governance practices. Among other observations, the report stated that ''[the] massive shift to digitized records makes patient data available to many more individuals within and outside the provider organization and leaves the data more vulnerable to the growing threat of cyber crime.'' The report added that one of the top three causes of data breaches is lost or stolen computing devices.[8]

In parallel with the subsequent OIG report, the Ponemon study found that while 85 percent of respondents believe they comply with HIPAA's requirements, fewer than half were confident that the organization properly secured network access points, secured patient data at rest or in transit.[9] Mobile devices holding patient data complicate this effort dramatically. Tools do exist to secure files on iPads and similar devices, as well as enabling secure wireless communications. The challenge may lie with the human component, how well we follow the policies and how well we avoid ''convenient'' work arounds to the perceived ''inconvenience'' of security.

5) Improving Compliance

Mobile devices have the potential to enhance the way that doctors and their teams deliver health care and interact with patients. There is the opportunity to reduce office visits, to improve the timeliness and accuracy of patient communications, to continually monitor patient vital signs, and to manage treatment protocols. However, if the increased use of mobile devices results in greater risk to patient information, these benefits will be slow in coming.

The most successful information security programs often take a broad view of managing data within the system. This involves the combination of policies, technologies, and physical safeguards mentioned earlier. Those covered by the HIPAA Security Rule can take a series of steps to enhance the prospect of successful mobile health tools and reduce the risk of security incidents.

Secure Wireless Transmissions

Before allowing portable devices access to any PHI or practice management files, make sure that the wireless access points are properly secured and not broadcasting their identifier (SSID). When doctors are in the office using mobile tools, this will improve the security of patient data in transit.

When accessing patient files or data from outside the hospital or office and across the public internet, it is important that there be some way to secure the communication. If accessing a web-based system, Secure Sockets Layer (SSL) and Transport Layer Security (TLS) may protect data during that session. Other tools available for the iPad and similar devices allow use of a virtual private network (VPN), which provides a secure tunnel of sorts.

In either event, the technologies to secure these wireless communications should implement the NIST specifications identified in the OCR Technology Guidance.

Secure ePHI on Devices

Encryption is no longer as complicated and expensive as in the past, so protecting health information on mobile devices is not only feasible but practical. Consider using mobile health apps that do not allow for the storage of PHI on the device if this meets the needs of the user. If it is essential to see patient files without an internet connection, then check the features of each health app to determine whether it enables encryption of patient data. Simply applying a password is not the same as encryption. If the app will not adequately protect data at rest on the device, consider a tool to protect all files on your tablet or smartphone.

Store Minimum Necessary

While the minimum necessary rule applies to disclosures of PHI, a corollary is relevant to mobile devices: do not store any more patient information on a device than necessary. Simply enough, the more ePHI on a device, the greater the potential impact if there is a security incident. An important aspect of limiting this data flow is understanding exactly what (or whose) data is on the device at any time. This should be manageable if the iPad is connected to an EHR, as the EHR should have the ability to track access and transfers. For mobile monitoring apps that store data on the device, it will be important for there to be an audit trail to readily identify sensitive information. While this is mitigated by the application of encryption so that the patient data is not considered unsecured PHI, an important part of any data protection program is understanding what data is where and why.

Training and Awareness

Finally, never underestimate the potential for human error. Before an individual user is granted access to any patient information via a mobile device, the person should have a solid understanding of how organizational safeguards apply to the device. This may be particularly important because so many of these products are personal devices and subject to all that is on the internet, ranging from malware to apps that do not protect information as you think they might.

The opportunities of the mobile health market are tremendous for developers of devices, health apps, health care providers, and patients. But it will require some thought and effort to properly incorporate iPads and other devices into a hospital's or practice group's system so that the benefits are not outweighed by the risks.

[8] Ponemon Institute, Benchmark Study on Patient Privacy and Data Security (November 2010) at 2.

[9] Ponemon at 12.