Bloomberg BNA

Privacy and Security Law Report®

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

By Peter McLaughlin and Melissa Crespo

1. Introduction

The proliferation of mobile devices and health care-related mobile applications is radically changing the way health care services are delivered. 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. However, app developers and health care providers must be aware of the implications of designing and utilizing mobile devices and health apps.

Physician groups and hospitals should consider how they use these devices. While the Food and Drug Administration (FDA) regulates as medical devices only a small number of mobile apps and recent guidance indicates that FDA regulation will remain limited, the storage and wireless transmission of protected health information (PHI) 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. Mobile app developers should also be aware of those features that may trigger FDA regulation and may implicate the HIPAA rules, so that developers can structure functionality and product support appropriately. In an era when people seem to lose portable devices with remarkable frequency, it is important for developers to create medical mobile apps that facilitate compliance. It is also important for health providers 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.

Peter McLaughlin is of counsel at the New York City office of Morrison & Foerster LLP, and Melissa Crespo is an associate at the firm's New York City office. They are members of the firm's Global Privacy and Data Security Practice Group. They advise health care clients, cloud providers, and app developers with regard to HIPAA compliance, particularly regarding health information technology. The opinions expressed in this article are their own and do not necessarily reflect those of the firm or any clients.

2. Proliferation of Devices and Apps

The popularity of mobile health apps is evident: as of March 2013, there were 97,000 mobile health applications available across major application download services, and 59 percent of patients in emerging markets use mobile health applications and services.[1] These health apps range from calorie counters and pedometers to blood glucose monitors and remote electrocardiogram (EKG) monitoring, which may also be connected to an electronic health record (EHR).

In releasing a study on physicians' use of technology, Manhattan Research LLC reported in May 2011 that 30 percent of doctors were using tablets to access EHRs, to view results such as radiology images, and to communicate with patients.[2] PricewaterhouseCoopers reports that eight out of 10 doctors recommend mobile health services.[3] Although an online search for ''health'' apps yields a wide variety of consumer-oriented tools, an increasing number of these apps facilitate a physician's practice.

A quick review of mobile apps for doctors, nurses, and clinicians displays a wide range of these tools.

[1] research2guidance, *Mobile Health Market Report 2013-2017: The Commercialization of mHealth Applications* (Mar. 4, 2013), *available at* http://www.research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/.

[2] PricewaterhouseCoopers, *Healthcare-Emerging Markets Trailblazers*, *available at* http://www.pwc.com/gx/en/healthcare/mhealth/opportunities-emerging-markets.jhtml.

[3] PricewaterhouseCoopers, *mHealth: What Do Patients, Doctors and Other Stakeholders Say About It?* (2012), *available at* http://www.pwc.com/gx/en/healthcare/mhealth/report-findings.jhtml.

 ISSN 1538-3423

These include apps for drug-interaction checkers, medical dictionaries, diagnostic lab test tools, and disease treatment guides. While most of these apps, like VisualDX, Logical Image Inc.'s digital medical image library, 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 facilitate clinical decision support. Many of these apps also provide for the remote monitoring of patient vital signs, such as an apps for reading EKGs or accessing patient charts and X-ray images.

3. FDA Regulation of Mobile Devices

Section 201(h) of the Federal Food, Drug, and Cosmetic Act (FDCA) defines a medical device as ''an instrument, machine, or other apparatus which is (i) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man . . . .''[4] Although not expressly identified in the statute, software is considered a device. Since 1976, the FDA has regulated devices subject to a three-tier system.[5] Class I devices are considered low risk and do not require pre-market approval. Class II devices are considered to represent an intermediate level of safety risk, and manufacturers of such devices are required to file a pre-market notification showing that the device is ''substantially equivalent'' to another Class II device. Class III devices are the highest risk and require pre-market approval, which can be quite complex and costly. The FDCA generally requires that any device marketed for the first time after 1976 is automatically considered a Class III device; however, the FDA has classified various specific devices first marketed after 1976 in Class I and Class II.

In July 2011, the FDA issued draft guidance proposing the criteria by which the FDA intended to apply its authority to mobile apps.[6] The guidance indicated that the FDA would regulate ''mobile medical applications''—defined as an app that meets the FDA's definition of ''device'' and is either used as an accessory to a regulated medical device, or transforms a mobile platform into a ''regulated medical device.'' According to the FDA guidance, this would include regulation of a subset of mobile apps that connect to and act as an extension of a medical device, and mobile apps that have been traditionally considered medical devices, like an app that turns a tablet into an ultrasound display.

In response to the draft guidance, the House Committee on Energy and Commerce sent a letter to the FDA in March 2013 expressing concern over uncertainty created by the draft guidance.[7] The committee presented several questions, including whether smartphones and tablets that run the mobile medical app would be considered medical devices. Such regulation would have the added burden of subjecting the devices to a medical device tax under the Affordable Care Act.

In an effort to gain further clarity on the questions posed in the letter, House lawmakers conducted three days of hearings on the proposed guidance. The Subcommittee on Communications and Technology held the first hearing March 19 and focused on how FDA regulations and taxes could affect the mobile health apps industry. On March 20, the Subcommittee on Health focused on the use of health information technologies, including medical apps, and the benefits to patients.[8] On March 21, the Subcommittee on Oversight and Investigations focused on the positions of the FDA (and the Department of Health and Human Services (HHS)) on emerging technologies.[9] At the third hearing, Ms. Christy Foreman, director of the FDA's Office of Device Evaluation in the Center for Devices and Radiological Health, confirmed that the final guidance would not ''regulate the sale or general consumer use of smartphones or tablets'' and would not consider entities that exclusively distribute mobile medical apps, such as application download platforms, to be medical device manufacturers.[10] During the hearings, FDA representatives provided examples of apps that would fall outside the scope of the anticipated final guidance, including calorie counters, and apps that perform the functionality of an EHR, or personal health record systems.

Foreman acknowledged that many mobile health apps carry minimal risks, but noted that the FDA is concerned with regulating those apps that can pose a significant risk to patients if they do not operate them correctly. For example, a mobile app that affects the programming of a drug infusion pump or a CT scanner could lead to a drug or radiation overdose. Likewise, an app that behaves as a monitor or display for a medical device must present an accurate image for diagnostic purposes.

The final guidance, which is expected to be issued later this year, will provide further clarity on the type of mobile apps that would fall within the FDA's scope of enforcement, as well as additional examples of mobile apps that will be covered. In her statement, Foreman noted that the FDA has received more than 130 comments on the July 2011 guidance.

---

[4] 21 U.S.C. § 201(h).

[5] *See* Medical Device Amendments of 1976 § 513(a), Pub. L. No. 94-295, § 513(a), 90 Stat. 539, 540–41 (1976) (codified as amended at 21 U.S.C. § 360c(a) (1994)).

[6] FDA, *Draft Guidance for Industry and FDA Staff—Mobile Medical Applications* (July 21, 2011), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf (10 PVLR 1068, 7/25/11).

[7] Letter from House Comm. on Energy and Commerce to Margaret A. Hamburg, Comm'r, FDA (Mar. 1, 2013), *available at* http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/letters/20130301FDA.pdf.

[8] Memorandum from Comm. on Energy and Commerce Majority Staff to Health Subcomm. Members (Mar. 18, 2013), *available at* http://docs.house.gov/meetings/IF/IF14/20130320/100535/HMTG-113-IF14-20130320-SD002.pdf.

[9] Memorandum from Subcomm. on Oversight and Investigations Staff to Members, Subcomm. on Oversight and Investigations (Mar. 19, 2013), *available at* http://docs.house.gov/meetings/IF/IF02/20130321/100544/HHRG-113-IF02-20130321-SD002.pdf.

[10] House of Representatives Comm. on Energy and Commerce, Subcomm. on Oversight and Investigations, *Transcript of Hearing on Health Information Technologies Administration Perspective*, 2013 WL 1178928 (Mar. 21, 2013); *see also Health Information Technologies: Administration Perspectives on Innovation and Regulation*: Hearing on Health Information Technologies Administration Perspective Before the Subcomm. on Oversight and Investigations of the H. Comm. on Energy and Commerce, 113th Cong. (2013) (statement of Christy L. Foreman, Director, FDA Office of Device Evaluation), *available at* http://www.fda.gov/NewsEvents/Testimony/ucm344395.htm.

  PVLR ISSN 1538-3423

The FDA has reviewed approximately 100 mobile medical apps through its regulatory process, and about 20 mobile apps per year are reviewed through this process.[11]

Numerous mobile medical apps have received FDA approval, including the following:

- **AliveCor** snaps onto the back of a smartphone and turns the device into an EKG. To take cardiac measurements, the user presses the device against the skin near the heart. The FDA classified the app as a Class II device and issued 510(k) clearance[12] in November 2012.[13]
- **DiabetesManager by WellDoc Inc.** captures blood-glucose information and transmits it in real time. WellDoc's system analyzes the data and offers a personalized coach to help patients manage their medication and treatment. The FDA issued 510(k) clearance for the app in July 2010.[14]
- **Welch Allyn iExaminer Adapter and Ophthalmoscope** is an app and ophthalmoscope that plugs into a smartphone and can detect conditions like retinal detachment and glaucoma. The accompanying examiner app allows health providers to store the pictures to a patient file or print or email them. The FDA issued 510(k) clearance for the app in December 2012.[15]

4. Keep HIPAA in Mind

Although mobile app developers and health care providers may find some comfort in the limited scope of mobile health apps to which the FDA's final guidance will likely apply, HIPAA compliance should still be a significant consideration.

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)[16] provides significant funding over the coming years. The HITECH Act, and the more recent implementation of the final omnibus rule (''Omnibus Rule''), expanded portions of HIPAA directly to business associates and established breach-reporting obligations for covered entities. As physicians increasingly leverage tablets 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, regardless of whether the FDA regulates the app as a mobile medical app.

On Jan. 17, HHS issued the Omnibus Rule, which became effective March 26 and, subject to certain exceptions, requires covered entities and business associates to comply with the Omnibus Rule by Sept. 23.[17] Among many significant changes, the Omnibus Rule expanded the definition of a ''business associate'' to include any person who ''creates, receives, maintains, or transmits PHI on behalf of a covered entity''[18] as well as a subcontractor who ''creates receives, maintains, or transmits'' PHI on behalf of a business associate.[19] The Security Rule and certain provisions of the Privacy Rule apply directly to business associates.

The HIPAA Security Rule applies to electronic PHI held by covered entities or business associates.[20] Section 164.308(a)(1)(ii)(A) of the Security Rule requires that a covered entity or business associate conduct a risk analysis to assess the nature and volume of electronic PHI (ePHI) and the risks of unauthorized use or disclosure of this patient information. A covered entity or business associate 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 ensure the confidentiality, integrity, and availability of patient information.

The challenge presented by the proliferation of mobile devices and apps potentially storing PHI is that enhanced mobility and remote access to patient information dramatically complicates successful implementation of the safeguards required by the Security Rule. If app developers provide remote support or maintain any of the health data processed by the app, these developers may become business associates. Hospitals, physician groups, and their business associates often struggle to maintain control of PHI in the current environment, if the increasing reports of PHI data breaches are any indicator.

---

[11] *Id.*

[12] Class II devices generally cannot be marketed until they have received 510(k) clearance from the FDA. The 510(k) process also applies to a limited number of Class II and Class III devices. The 510(k) clearance is the FDA's acknowledgment that the device is substantially equivalent to another Class II device that is already on the market. 21 U.S.C. § 510(k).

[13] FDA, *Nov. 2012 510(k) Clearances*, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ucm330634.htm (last updated Dec. 10, 2012); *see also* Brian Dolan, *FDA Clears AliveCor Heart Monitor, Doctors Can Pre-Order*, MobiHealthNews, Dec. 3, 2012, *available at* http://mobihealthnews.com/19306/fda-clears-alivecor-heart-monitor-doctors-can-pre-order/.

[14] FDA, *July 2010 510(k) Clearances*, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ucm221473.htm (last updated Apr. 12, 2013); *see also* Brian Dolan, *FDA Clears WellDoc for Diabetes Management*, MobiHealthNews, Aug. 2, 2010, *available at* http://mobihealthnews.com/8539/fda-clears-welldoc-for-diabetes-management/.

[15] FDA, *Dec. 2012 510(k) Clearances*, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/DeviceApprovalsandClearances/510kClearances/ucm334768.htm (last updated Jan. 9, 2013); Jonah Comstock, *FDA Clears Welch Allyn's iPhone-Enabled Opthalmoscope*, MobiHealthNews, Jan. 24, 2013, *available at* http://mobihealthnews.com/20018/fda-clears-welch-allyns-iphone-enabled-opthalmoscope/.

[16] Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, 123 Stat. 226 (2009).

[17] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5565 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf (12 PVLR 123, 1/28/13).

[18] 45 C.F.R. § 160.103(1).

[19] *Id.* § 160.103(3).

[20] *Id.* § 164.302.

b. HIPAA Implications for App Developers and Health Care Providers

One of the primary concerns for developers of mobile health apps is the regulatory framework that will inevitably guide the specific design of the end product.

A developer should first determine whether HIPAA will apply to the way in which the product will be used and what information will be stored in the application. An application that will be used solely by the individual consumer, for example, may not implicate HIPAA. An app developer should consider whether the app will be used by a covered entity and whether it will include PHI. If the app is solely used by the individual consumer to, for example, follow a medication schedule, then it would not likely implicate HIPAA. However, if, as part of the patient's treatment plan, the physician instructed the patient to use the app to send PHI to the physician, the app may need to incorporate the HIPAA safeguards.

The Security Rule presents a series of required and addressable measures as part of a covered entity's and business associate'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. When developing an app that will be used by a covered entity and involve PHI, developers should be aware of the measures set forth in the Security Rule and include such functionality.

Health providers, before using a tablet or similar device to handle patient information, should consider how the device and its apps will fit within their security compliance. For example, does the device store data locally and 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?

Among reported breaches listed by the HHS, many involve portable devices, such as laptops for which disk and file encryption are readily available. Businesses must consider that tablets and similar mobile devices will increase these numbers if they are not properly configured to secure any PHI they hold or enable remote access. To determine precisely how to apply such configurations, HHS has issued technology guidance to distinguish between secured and unsecured PHI.

c. Impact of HHS Technology Guidance

In conjunction with the HHS Breach Notification Rule, the Office for Civil Rights (OCR) issued *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (''Technology Guidance'') to assist covered entities and business associates in determining when PHI was ''secured'' and thus not subject to the reporting requirements applicable to ''unsecured PHI.''[21] The guidance from OCR provides that PHI will be rendered unusable, unreadable or indecipherable to unauthorized individuals if the ePHI 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 and will constitute a reportable breach.

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.[22] 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 they are at rest (stored),[23] when they are in transit,[24] and when they are ready for destruction.[25]

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. Mobile 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 they untether the user from a desk or cable connection. The OCR Technology Guidance states that ePHI in transit—winging its way across a wireless network—should be sent and received through a secure link. Applying security to the Wi-Fi 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? Tablets and smartphones 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, how carefully the mobile device and its health apps have been configured. Most people are happy enough to just click ''download'' and

[21] HHS, *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[22] 45 C.F.R. § 164.304.

[23] NIST, *Guide to Storage Encryption Technologies for End User Devices*, SP 800–111 (Nov. 2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf.

[24] NIST, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, SP 800–52 (June 2005) (withdrawn by NIST March 13, but referenced by HHS for data in motion: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html); NIST *Guide to IPsec VPNs*, SP 800–77 (Dec. 2005), *available at* http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf; *see also* NIST, *Guide to SSL VPNs*, SP 800–113 (July 2008), *available at* http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf, or others which are Federal Information Processing Standards (FIPS) 140-2 (*Security Requirements for Cryptographic Modules*) validated.

[25] NIST, *Guidelines for Media Sanitization*, SP 800–88 (Sept. 2006), *available at* http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf (5 PVLR 1266, 9/11/06).

   ISSN 1538-3423

have the mobile app almost instantly delivered to their devices.

d. Breach Notification Rule

The health care sector has been subject to a lot of scrutiny following commencement of the Breach Notification Rule Sept. 23, 2009, and the interim final rule published by HHS in the *Federal Register* Aug. 24, 2009. The Breach Notification Rule, as amended and made final by the Omnibus 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] . . . .''[26] 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 using a tablet. If remote access to patient files does not typically involve saving patient data onto the device, then the loss of such mobile device 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 mobile device. 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 tablets 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.

5. Risks and Liability

As with the ubiquitous use of laptops, the popularity of tablets 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 its 2010 *Healthcare Unwired* report, PricewaterhouseCoopers found that more than a third of doctors surveyed expressed concern over privacy and security as their chief barriers to using mobile health applications.[27] However, 80 percent of physicians use mobile technology of some sort to deliver patient care, and over 90 percent use mobile devices in everyday operations.[28] It is inevitable that these concerns will remain prevalent as the use of mobile devices and mobile health apps continues to grow.

Two recent OCR settlements highlight the result of ineffective safeguards and the importance of taking proper measures to ensure that mobile devices comply with the HIPAA Security Rule.

In February 2010, a Massachusetts Eye and Ear Infirmary (MEEI) doctor's laptop containing the health information of approximately 3,526 patients was stolen during a lecture tour. Upon notification of the theft, OCR conducted an investigation. OCR's resolution agreement details the categories of noncompliance, including that MEEI did not conduct a proper risk analysis and specifically did not sufficiently assess the risks posed by mobile devices; that MEEI's security measures for mobile devices were not at a ''reasonable and appropriate level''; and that MEEI failed implement adequate policies to allow only authorized persons to access ePHI using portable devices. In October 2012, OCR reached a $1.5 million settlement with MEEI.[29] In addition to the settlement, MEEI was required to execute a three-year corrective action plan that requires the use of an outside monitor and the production and implementation of monitor reports, as well as semiannual inspections.

Also notable is an investigation that resulted in the first settlement involving a breach of ePHI affecting fewer than 500 individuals. OCR began its investigation of the Hospice of North Idaho (HONI) after HONI reported to HHS that an unencrypted laptop computer containing the ePHI of 441 patients was stolen in June 2010. Over the course of its investigation, OCR discovered that HONI had not conducted a risk analysis to safeguard ePHI, and it had not implemented policies or procedures for mobile device security, in contravention of the HIPAA Security Rule. HONI agreed to pay HHS $50,000 to settle these violations and has since taken extensive additional steps to improve HIPAA compliance.[30]

Beyond regulatory enforcement, several legislative initiatives are in the works and, if adopted, will further impact the creation and use of mobile health apps and devices.

In December 2012, Rep. Mike Honda (D-Calif.) introduced the Healthcare Innovation and Marketplace Technologies Act (HIMTA) (H.R. 6626) to foster more innovation in the health care industry by removing barriers in wireless health.[31] The bill would establish an Office of Wireless Health at the FDA to coordinate with other governmental agencies and private industry, and provide recommendations to the FDA Commissioner on how to develop and maintain a regulatory framework

[26] 45 C.F.R. § 164.402.

[27] PricewaterhouseCoopers, *Healthcare Unwired*, 6 (Sept. 2010), *available after registering at* http://pwchealth.com/cgi-local/hregister.cgi/reg/healthcare-unwired.pdf.

[28] HIMSS Analytics, *2nd Annual HIMSS Mobile Technology Survey* (2012).

[29] Resolution Agreement between OCR and Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates Inc. (Sept. 13, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf (11 PVLR 1445, 9/24/12).

[30] Resolution Agreement between OCR and Hospice of North Idaho (Dec. 28, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf (12 PVLR 41, 1/7/13).

[31] Healthcare Innovation and Marketplace Technologies Act, H.R. 6626, 112th Cong. (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr6626ih/pdf/BILLS-112hr6626ih.pdf.

on wireless health issues. The bill would also establish a mobile health developer-support program at HHS to help mobile application developers build their devices in line with current privacy regulations. Because the measure was introduced during the lame-duck session of the 112th Congress, Rep. Honda has indicated he will reintroduce HIMTA this year.

Additionally, on May 9, Rep. Hank Johnson (D-Ga.) introduced the Application Privacy, Protection, and Security (APPS) Act of 2013 (H.R. 1913), which seeks to address the public's growing concern with data collection on mobile devices.[32] The APPS Act would require that app developers provide transparency through consented terms and conditions, reasonable data security of collected data, and users with control to cease data collection by opting out of the service or deleting the user's personal data to the greatest extent possible.

6. Compliance Recommendations

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, improve the timeliness and accuracy of patient communications, continually monitor patient vital signs, and manage treatment protocols. The extensive benefits of mobile devices have created an ever-growing demand for mobile medical apps. However, if the increased use of mobile devices and mobile medical apps results in greater risk to patient information, these benefits will be slow in coming. Developers and medical service providers should make efforts to ensure that the devices and apps facilitate HIPAA compliance.

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 Service Set 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 mobile 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. Health care providers should 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. If an app will not adequately protect data at rest on the device, health care providers should consider a tool to protect all files on a tablet or smartphone.

Additionally, mobile health app developers should make efforts to encrypt user data stored on mobile devices and data in transit to protect against interception, as well as implement authentication tools to verify the identity of the user. Simply applying a password is not the same as encryption.

Store the Minimum Necessary

Although 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 put, 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 are on the device at any time. This should be manageable if the tablet 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 to have an audit trail to readily identify sensitive information. Although this is mitigated by the application of encryption so that the patient data are not considered unsecured PHI, an important part of any data protection program is understanding what data are 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 user 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.

In order to assist with improving organizational safeguards and security compliance, in December 2012, the Office of the National Coordinator for Health Information Technology launched a mobile-device HIPAA compliance website that offers advice for health care providers, as well as videos, fact sheets and even educational materials, such as a series of posters to hang in the break room reminding employees of their duty to protect patient data.[33]

7. Conclusion

A recent report indicates that by the end of 2017, the total mobile health market will have grown by 61 per-

[32] Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (2013), *available at* http://op.bna.com/pl.nsf/r?Open=kjon-97kpmp (12 PVLR 833, 5/13/13).

[33] HealthIT.gov, *Your Mobile Device and Health Information Privacy and Security*, http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security (last visited May 13, 2013).

  PVLR ISSN 1538-3423

cent to an estimated $26 billion.[34] The popularity of mobile devices and health apps promises that enhanced mobility and access to information will improve the way in which health providers, insurers and their teams interact with patient health information.

App developers and medical service providers should keep in mind the type of data the app will be managing, and, depending on the sensitivity of the information, ensure that the data are properly secured. Developers should also be aware of FDA regulatory requirements in the event the app may be deemed a medical device.

The FDA will provide significant guidance in the upcoming months as to the regulation of mobile health apps, with final guidance due to be published by the end of 2013. Covered entities and business associates will be required to comply with the Omnibus Rule by Sept. 23. Under current rules, though, both developers and users of health apps need to be alert to the potential trade-off between convenience and the use of apps that might not handle PHI properly.

[34] research2guidance, *supra* note 1.