FOCUS MOBILE HEALTH

Lessons from Project HealthDesign

Strategies for Safeguarding Patient-Generated Health Information Created or Shared through Mobile Devices

By Deven McGraw, JD, MPH, LLM; Helen R. Pfister, JD; Susan R. Ingargiola, MA and Robert D. Belfort, JD

ABSTRACT

Robert Wood Johnson's Project HealthDesign is exploring a vision of personal health records as tools for improved health decision-making by both patients and providers. In the latest phase, researchers are providing patients with smartphones to aggregate and send observations of daily living (ODLs) to healthcare providers, providing a richer picture of a patient's day-to-day health status. Patients' use of mobile devices to generate and communicate health information subjects this information to unique security risks for which solutions have not yet been discussed. When healthcare providers handle electronic, identifiable health information, they are subject to the HIPAA Security Rule. But HIPAA regulates providers, not patients. This paper discusses the factors that should be considered when protecting patient-generated health information created on or shared through mobile devices. It also recommends strategies for securing patient health information on mobile devices and implementing technical safeguards to ensure general device security.

KEYWORDS

mHealth, HIPAA, security, patient-generated health information, mobile device.

LEVERAGING THE power of new technologies, researchers funded by the Robert Wood Johnson Foundation's Project HealthDesign are encouraging patients to track and share with clinicians observations of daily living (ODLs) and other information that can serve as important indicators of a patient's health.1 Previous phases of Project HealthDesign focused on making personal health records more effective tools for patient self-care.2 The current phase takes the next step and tests the impact of patients' use of smartphones and mobile devices to collect and share self-care information like ODLs with their healthcare providers.3 While ripe with potential to improve patients' health, the use of mobile devices to generate and communicate health information subjects this potentially sensitive information to security risks. These risks, if unaddressed, pose a

TABLE 1: Project HealthDesign Grantee Teams' Use of Mobile Devices

	San Francisco State University	University of California, Irvine	RTI International and Virginia Commonwealth University	University of California, Berkeley, Healthy Communities Foundation and University of California, San Francisco	Carnegie Mellon University
Project Name	*iN Touch*	*Estrellita*	*BreathEasy*	*Crohnology.MD*	*dwellSense*
Project Description	The iN Touch team is examining how collecting ODLs via an iPod Touch impacts low-income youth who are managing obesity.	The Estrellita team is creating a mobile application for collecting information from high-risk infants and their primary caregivers that will allow the caregivers to more easily interface with clinicians to improve care and communication.	The Crohnology.MD team is helping young adults who have Crohn's disease create visually-aided narratives of their conditions and responses to treatment.	The Crohnology.MD team is helping young adults who have Crohn's disease create visually-aided narratives of their conditions and responses to treatment.	The dwellSense team is developing and evaluating new technologies that will monitor the routine of elders who have arthritis and are at risk for cognitive decline.
Devices Given to Patients	iPod Touches	Smartphones and scales	Smartphones	Smartphones and sensors	Sensors and laptops
Information Flow	ODLs are sent from iPod Touch to TheCarrot.com through an app on the iPod Touch. TheCarrot.com generates reports, which patients view through an online portal from TheCarrot.com and which are sent to healthcare providers' EHRs.	ODLS are sent from smartphone to HealthVault through Estrellita app on phone. Patients access reports through an app on the smartphone.	ODLs are sent from smartphones to the RTI server. Clinicians view reports/dashboards through a portal or EHR. Patients may also view reports through dashboard on smartphones.	ODLs are sent from smartphones to project servers (data from sensors flow separately). Patients can access reports through an app on the smartphone. Patients can send healthcare provider a 30 day read-only invite to view patient data in report mode via an iPad.	ODLs are sent from laptops to HealthVault. Reports are generated, which clinicians and patients may view on their laptops.
Use of SMS/Text Messaging?	Yes. Health coaches send and receive SMS messages to patients.	No.	No.	No.	No.

potential obstacle to more widespread use of such tools by patients to generate and share health information.

Healthcare providers are subject to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which outlines the safeguards that must be used to secure electronic, individually identifiable electronic health information (known as ePHI).[4] But HIPAA regulates providers, not patients. When patients generate health information using applications on their mobile devices—whether they share it with their healthcare providers or simply use it to engage in their own self-management activities—the Security Rule does not apply.

Project HealthDesign involves activity that is neither provider activity subject to HIPAA nor autonomous patient activity for which providers could not conceivably be held responsible.[5] Instead patients are collecting and transmitting ODLs and other health information in a research environment administered and overseen by healthcare organizations. This unique environment raises challenging questions regarding the responsibility of these organizations for information security.

As part of Project HealthDesign, each grantee team collects a variety of ODLs from patients using different technologies. **Table 1** summarizes how each team is using mobile devices to collect ODLs and incorporate them into clinical care. While these activities are part of a research study, it is not hard to envision an environment in which healthcare providers routinely encourage patients to use mobile devices to collect and share clinically relevant information such as ODLs. As reimbursement models for healthcare providers move toward episode of care-based bundling, shared savings incentives and capitation, there will be greater incentives for providers to more actively engage patients in daily self-management and care coordination.

This paper suggests strategies for promoting the security of health information generated by patients and shared with healthcare providers using mobile devices, an area where clear legal standards

do not exist. The paper draws on lessons learned by the Project HealthDesign grantee teams as they have attempted to strike a balance between data security and clinically effective information exchange by patients. The strategies reflect the unique "middle ground" environment in which Project HealthDesign grantees operate, with patient-generated information not subject to the HIPAA Security Rule, but maintained and transmitted as part of a research study designed, promoted and financially subsidized by healthcare organizations. While this environment may not be frequently encountered today, it may become a more prevalent framework for managing chronic illness in the future. Thus, the strategies discussed herein may have broader application in the future.

SPECIAL RISKS PRESENTED BY MOBILE DEVICES

Mobile devices such as smartphones pose unique risks to health information, such as loss or theft, unauthorized access, malware (viruses) and cloning.[6] Since 2009, HIPAA-covered entities have been required to report breaches of unsecured health information affecting 500 or more individuals.[7] These breach reports strongly suggest that risks related to the loss, theft and unauthorized access of mobile devices are likely to be more significant than sophisticated external threats. This threat assessment is an important consideration in determining the type of safeguards that are appropriate in properly balancing security and clinical efficacy.

STRATEGIES FOR SAFEGUARDING PATIENT-GENERATED HEALTH INFORMATION CREATED OR SHARED THROUGH MOBILE DEVICES

HIPAA Security Rule. Even where the HIPAA Security Rule does not apply, it is a useful starting point for understanding the types of safeguards that may be appropriate. At the same time, any set of strategies must take into account the differences between an environment of provider-generated information, for which the Security Rule was designed, and an environment of ODLs and other information collected and transmitted by patients. Healthcare providers have direct control over their workforce and can require compliance with various security measures, but providers have no such authority over their patients. Thus, while both environments may warrant consideration of the same types of issues, in the world of patient-generated information the Security Rule's safeguards should be evaluated and implemented in a manner not necessarily contemplated under HIPAA.

A complete explanation of the HIPAA Security Rule is beyond the scope of this paper, but a few elements are worth highlighting. The Security Rule is designed to be flexible and scalable so a covered entity can implement strategies that are appropriate for the entity's particular size and organizational structure, as well as the nature of the risks to its EPHI.[8] Thus, some specific safeguards are required by the Rule; others are listed as "addressable" specifications.[9] The key Security Rule standards relevant to patients' use of mobile devices to generate and share health information are listed in **Figure 1**.

FIGURE 1: Key Security Rule Standards Relevant to Patients' Use of Mobile Devices to Generate and Share Health Information.[19]

Standards	HIPAA Security Rule Section	Implementation Specifications	(R) = Required (A) = Addressable
Access Control	164.312(a)(1)	▪ Unique User Identification ▪ Emergency Access Procedure ▪ Automatic Logoff ▪ Encryption and Decryption	▪ (R) ▪ (R) ▪ (A) ▪ (A)
Audit Controls*	164.312(b)		▪ (R)
Integrity*	164.312(c)(1)	▪ Mechanism to Authenticate Electronic Protected Health Information	▪ (A)
Person or Entity Authentication	164.312(d)		▪ (R)
Transmission Security	164.312(e)(1)	▪ Integrity Controls ▪ Encryption	▪ (A) ▪ (A)

*We have identified "audit controls" and "integrity" as security rule standards relevant to patients' use of mobile devices to generate and share health information. However, based on the experiences of the Project HealthDesign grantee teams, there does not appear to be a need for a patient to log and audit the use of his or her mobile device, since it is generally only the patient who will have access to the device (the provider has access to the information sent by the patient from the device). Likewise, there should be no need for a patient to take steps to ensure the integrity of the EPHI the patient stores and/or transmits through the mobile device since the risk of alteration or destruction is low.

The Security Rule also requires providers to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.[10] In a "risk analysis," providers must often evaluate and weigh competing concerns. The experiences of the Project HealthDesign grantee teams indicate that securing patients' health information without overburdening information-sharing by patients is a challenge. Patients do not want to be inconvenienced, and their ability (in terms of knowledge and resources) to implement security measures on their mobile devices is limited. Taking the grantee teams' experiences into account, the following key questions should be considered in a risk analysis related to the protection of patient-generated health information created on or shared through mobile devices:

- **Complexity and cost.** Does a patient's smartphone come with built-in security tools (e.g., encryption), or would the patient would have to buy, download and install third-party software?
- **Patient ability.** Could the patient reasonably install and implement the software?
- **Effect on clinical care.** Will implementing an access measure—like a password—lessen the patient's willingness to report health information?
- **Measure of risk.** Will ePHI included on or transmitted through a patient's mobile device cause the patient harm or embarrassment if breached?

When healthcare providers are providing their patients with mobile devices and encouraging them to share their health information as part of a provider-led initiative, they may take responsibility for implementing certain security activities on the patient's behalf. While patients using mobile devices outside of a provider-led initiative will likely make security decisions with minimal provider involvement, providers can and should be more involved in security when the provider is designing and subsidizing the information exchange. These facts are critical to the risk analysis.

For example, if a provider expects patients will simply not use smartphones that automatically log off after a specified period of time, or if patients will feel inconvenienced by having to input a password, the provider should take these facts into account when determining what security measures to implement directly or to recommend a patient implement. Because the decision to protect the patient's health information ultimately rests with the patient, security measures should be recommended with the likelihood of patient compliance in mind.

TRANSMISSION SECURITY AND ENCRYPTING DATA AT REST

Healthcare providers must implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network.[11] The Security Rule allows for ePHI to be sent over an electronic open network as long as it is adequately protected.[12] Encryption is the "addressable" implementation specification most relevant to patients' use of mobile devices to communicate with their healthcare providers.[13]

FIGURE 2: Text Message Encryption Background

Encrypting Data at Rest	▪ Many smartphones include built-in encryption capabilities for data at rest. For example, through the Blackberry Enterprise Server, Blackberry enables an enterprise to set the security policies for its employees' phones. Patients who have smartphones that are not provided by their employer or are not otherwise part of an enterprise system would probably have to work with their wireless carrier or device provider to enable their options for encrypting data at rest on their phones. Alternatively, healthcare providers providing the smartphones could take responsibility for enabling encryption options for them. ▪ Many smartphones allow patients or enterprises to add third party applications, including encryption/decryption and other security tools, to their phones. There are a number of third-party applications available in the iPhone App Store, for example, that will further encrypt data at rest on a smartphone. The price of these applications varies, and the difficulty of installation/use can be high.
Encrypting Data in Motion	▪ Unlike wireless Internet, the network channels over which text messages are sent in the United States are not encrypted via Secure Sockets Layer ("SSL") or Transport Layer Security ("TLS") encryption methods. This means that text messages are not automatically encrypted as they transverse carriers' wireless channels en route to another smartphone (or elsewhere). ▪ Unless an enterprise or a patient buys a third-party software tool that scrambles the text message before it leaves his/her phone and unscrambles it upon reaching its destination, text messages can be intercepted in transit and read. ▪ Third-party software applications to encrypt text messages in transit are available in the iPhone App Store, for example. The cost of these software tools varies. Most tools require the user to configure various options after the software is downloaded, to obtain additional keys, and to engage in other activities that make installation and use of these software applications challenging. ▪ It is probably not realistic to assume that individual patients would be capable of installing third-party text message encryption software on their smartphones for the purposes of protecting ODLs or other information they communicate to their healthcare providers through their smartphones.

Mobile devices can transmit data in various ways, such as Internet protocols (used by many of the software applications developed by Project HealthDesign grantee teams), e-mail (which uses traditional Internet protocols), voice (traditional telephone) and SMS/text messaging. Text messaging holds significant promise for bidirectional communication between healthcare providers and patients. However, the sensitivity of patients' health information and the risk that such information may be inappropriately accessed either while at rest or in transit suggest that encryption should be employed—or at least evaluated—to protect patient-generated health information.

Figure 2 provides background information related to the encryption of text messages.

The experiences of the grantee teams suggest the following strategies. First, providers that give patients mobile devices should investigate whether they can preset any built-in encryption tools for data at rest. Providers and patients should also investigate the availability, effectiveness, and price of third party tools that encrypt data being transmitted through text mes-

FIGURE 3: Spotlight on Project Health Design Grantees

Project Name	Description
iN Touch	▪ Project HealthDesign's iN Touch grantee team is examining the potential of collecting ODLs from youth suffering from obesity and depression. Under the project, participating youth enter ODLs into their iPod Touch, which sends the ODLs to TheCarrot.com via a wireless Internet connection. The Carrot.com generates weekly summary reports based on the ODLs and sends them to the participants' healthcare providers' EHRs. The reports are encrypted via SSL when they are transmitted to healthcare providers' EHRs. To prevent inadvertent or unauthorized access to patient health information, the iN Touch team pre-set the participants' iPod Touches to automatically lock after five minutes of inactivity. They also installed the Find iPhone and MobileMeapplications on the iTouches to help locate and remotely erase data from devices reported lost or stolen, and asked the individual project participants to do their part to safeguard their iTouches and their personal information. ▪ The iN Touch grantee team also notes that patient's ability to refrain from sharing his or her phone with family members may depend on socio-economic status. Patients with low-incomes may have only one phone that is used by all family members. Thus, the grantee team did not feel they could stress, as an absolute, not sharing the phone with family members but instead advised participants on the risks of sharing.
dwellSense	▪ Project HealthDesign's dwellSense grantee team is developing and evaluating technology to monitor the routines of older individuals who have arthritis and are at risk for cognitive decline. The grantee team has placed wireless sensors that capture routine daily activities (e.g., using a telephone, making coffee, taking medications) throughout patients' homes. The sensors send data to a nearby laptop computer, which enables the process to occur automatically and unobtrusively. The sensor data is then transmitted from the laptop into a PHR, where custom applications turn it into individualized visualizations for both the patients and their clinicians. ▪ Because the sensors are small and unobtrusive, they have limited computing and battery power. As a result, the grantee team undertook a risk analysis and decided not to encrypt the data as it moves from the sensor to the laptop (the data is encrypted as soon as it enters the laptop and remains encrypted thereafter). To do so would have required more computing power and a stronger, larger and more obtrusive battery, which would have to be changed daily. The grantee team took these operational issues into consideration when performing its security measure risk analysis. For example, it looked into a more secure radio signal to combat security risks to the unencrypted data, but this also would have required greater battery power. After a thorough analysis, the grantee team determined that sending unencrypted data from the sensor to the nearby laptop presented a reasonable risk that was worth taking in order to facilitate the project.

saging. If implementation of encryption is not feasible, providers giving patients mobile devices should engage in alternative protections, such as limiting the nature and extent of ePHI transmitted via unencrypted channels (e.g., careful wording of messages to and from patients),and direct patients to obtain detailed information through a web portal or other secure means. Further, providers that have supplied patients with mobile devices should offer education and training to patients on the risks of transmitting EPHI through text messages.

ACCESS CONTROLS AND PERSON/ENTITY AUTHENTICATION

Healthcare providers must implement technical safeguards to limit access to EPHI only to those authorized.[14] There are a variety of access control methods and technical controls that are available within most smartphones and other mobile devices. The access control implementation specifications most relevant to patients' use of mobile devices to communicate with their healthcare providers are (i) use of unique user identification (required);[15] (ii) use of automatic logoff (addressable)[16] and (iii) encryption/decryption (addressable and discussed previously).[17] With respect to authentication, healthcare providers must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.[18]

As the Project HealthDesign grantee teams learned, convenience and usability are key factors influencing a patient's willingness to use a mobile device to collect and share patient-generated health information. Patients generally view security measures like passwords and automatic log-off features as obstacles, and they may be resistant to complying with these security measures or their compliance may interfere with the effective flow of patient-generated health information to providers.

With this in mind, healthcare providers providing patients with mobile devices should probably not require patients to password protect their mobile devices. Instead, providers should educate their patients about the risks of unauthorized access to mobile devices, make recommendations about proper access control measures and try to help patients make thoughtful and informed choices. Healthcare providers who have the resources to do so should offer education and training on use of passwords and proper device handling. (Those without such resources should consider providing fact sheets or informally educating their patients during visits.) Healthcare providers may want to ask patients to sign a statement indicating they understand the heightened risks if they do not protect their mobile devices with passwords, enable their device's automatic logoff function and refrain from sharing their device

Project HealthDesign has demonstrated that it is possible to implement workable, technology-forward security protections for information in and shared through mobile devices.

with friends and family. **Figure 3** spotlights some transmission security and access control activities undertaken by two Project HealthDesign grantee teams.

CONCLUSION

While the collection and transmission of patient-generated health information using mobile devices is occurring today primarily under tightly controlled research circumstances, all signs indicate that patients' use of such devices to manage their health will increase. And as reimbursement models for healthcare providers incorporate cost containment incentives, there will be greater interest by healthcare providers in leveraging smartphones and other technologies to prevent costly complications. Project HealthDesign has demonstrated that it is possible to implement workable, technology-forward security protections for information in and shared through smartphones or other mobile devices, and they are critical to facilitate the widespread use of these tools by patients and healthcare providers. **JHIM**

Deven McGraw, JD, MPH, LLM, is the Director of the Health Privacy Project at the Center for Democracy & Technology (CDT), where she develops and promotes policies that ensure individual privacy as health information is shared electronically.

Robert Belfort, JD, is Partner at the law firm Manatt, Phelps & Phillips, LLP. He advises hospitals, community health centers, medical groups, managed care plans and other healthcare stakeholders on regulatory and transactional matters. He assists clients with managing health information in compliance with HIPAA and state confidentiality laws and advises on Stark law, anti-kickback and other fraud and abuse matters.

Helen Pfister, JD, is Partner at the law firm Manatt, Phelps & Phillips, LLP. She specializes in advising healthcare providers and nonprofit organizations on legislative, regulatory and transactional matters, and is involved in a range of projects involving use of health IT to facilitate the secure and timely exchange of information to improve the quality and efficiency of healthcare delivery.

Susan Ingargiola, MA, is Director at Manatt Health Solutions. She provides strategic business, regulatory and reimbursement advice to healthcare providers, nonprofit organizations and pharmaceutical/biotechnology companies She specializes in health information privacy and confidentiality laws and health information technology.

REFERENCES

1. Pioneer Portfolio Page. The Robert Wood Johnson Foundation. [website] Available at: www.rwjf.org/pr/product.jsp?id=18915. Accessed November 10, 2011.

2. Brennan PF, et al. Project HealthDesign: Rethinking the power and potential of personal health records. *J Biomed Inform*. 43(2010) S3-S5.

3. Projects Page. Project HealthDesign. [website]. Available at: www.projecthealthdesign.org/projects. Accessed November 10, 2011.

4. 45 C.F.R. Part 160 and Subparts A and C of Part 164.

5. Cushman R et al. Ethical, legal and social Issues for personal health records and applications. *J Biomed Inform*. 43(2010) S51-S55.

6. National Institute of Standards and Technology. *Guidelines for Cell Phone and PDA Security*. Special Publication 800-124. October 2008; U.S. Department of Health and Human Services. *HIPAA Security Guidance for Mobile Devices*. December 18, 2006.

7. U.S. Department of Health and Human Services. *Breaches Affecting 500 or More Individuals*. Available at: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html. Accessed November 10, 2011.

8. U.S. Department of Health and Human Services. *HIPAA Security Series: Security 101 for Covered Entities*. March 2007.

9. 45 C.F.R. § 164.306(d).

10. 45 C.F.R. § 164.308(a)(1)(ii)(A).

11. 45 § 164.312(e)(1).

12. U.S. Department of Health and Human Services. *HIPAA Security Series: Security Standards: Technical Safeguards*. March 2007.

13. 45 C.F.R. § 164.312(e)(2)(ii).

14. 45 C.F.R. § 164.312(a)(1).

15. 45 C.F.R. § 164.312(a)(2)(i).

16. 45 C.F.R. § 164.312(a)(2)(iii).

17. 45 C.F.R. § 164.312(a)(2)(iv).

18. 45 C.F.R. § 164.312(d).

19. National Institute of Standards and Technology. *Guidelines for Cell Phone and PDA Security*. Special Publication 800-124. October 2008; U.S. Department of Health and Human Services. *HIPAA Security Guidance for Mobile Devices*. December 18, 2006.