Lesson 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.
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). 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. 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. Since 2009, HIPAA-covered entities have been required to report breaches of unsecured health information affecting 500 or more individuals. 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

The key Security Rule standards relevant to patients’ use of mobile devices to generate and share health information are listed in Figure 1.

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

*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. 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:

**Figure 1: Key Security Rule Standards Relevant to Patients’ Use of Mobile Devices to Generate and Share Health Information.**

![Figure 1: Key Security Rule Standards Relevant to Patients’ Use of Mobile Devices to Generate and Share Health Information.](image-url)
Complexity and cost. Does a patient’s smartphone come with built-in security tools (e.g., encryption), or would the patient 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. The Security Rule allows for ePHI to be sent over an electronic open network as long as it is adequately protected. Encryption is the “addressable” implementation specification most relevant to patients’ use of mobile devices to communicate with their healthcare providers.

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 grantees suggest the following strategies. First, providers that give patients mobile devices should investigate whether they can pre-set 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-
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. 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); (ii) use of automatic logoff (addressable); and (iii) encryption/decryption (addressable and discussed previously). With respect to authentication, healthcare providers must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

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.

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.

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

4. 45 c.F.R. Part 160 and Subparts A and c of Part 164.
9. 45 C.F.R. § 164.306(d).
11. 45 § 164.312(e)(1).
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)(ii).
17. 45 C.F.R. § 164.312(a)(2)(iv).
18. 45 C.F.R. § 164.312(d).