mHealth Data Security: The Need for HIPAA-Compliant Standardization

David D. Luxton, Ph.D., Robert A. Kayl, M.S.E., and Matthew C. Mishkind, Ph.D.

National Center for Telehealth and Technology, Tacoma, Washington.

The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or as reflecting the views of the Department of the Army or Department of Defense.

Abstract

The rise in the use of mobile devices, such as smartphones, tablet personal computers, and wireless medical devices, as well as the wireless networks that enable their use, has raised new concerns for data security and integrity. Standardized Health Insurance Portability and Accountability Act of 1996 (HIPAA)–compliant electronic data security that will allow ubiquitous use of mobile health technologies is needed. The lack of standardized data security to assure privacy, to allow interoperability, and to maximize the full capabilities of mobile devices presents a significant barrier to care. The purpose of this article is to provide an overview of the issue and to encourage discussion of this important topic. Current security needs, standards, limitations, and recommendations for how to address this barrier to care are discussed.

Key words: *security, HIPAA, encryption, telehealth, mobile health*

Introduction

Although protection of patient data has always been a principal concern within the telehealth field, the evolution of modern technology platforms, communication capabilities, portability, and user patterns and preferences have made the issue more complex. In particular, the rise of mobile devices such as smartphones, tablet personal computers, and wireless medical devices, as well as the wireless networks that enable their use, has raised new concerns for data security and integrity. Special attention to these issues is necessary because of the shared use of modern wireless devices, mobility of users, and the ability to access multiple and shared networks from home or public locations. Moreover, mobile device applications, or apps, have created a new era of health-related capabilities that bring with them new privacy concerns.[1] Protected health information can be stored on these mobile devices, processed within these apps, and transmitted over networks to and from providers. As a result, security threats occur during both storage and transmission of electronic patient data and can jeopardize patient data as well as the integrity of entire data networks. Secure handling of data is necessary to assure compliance with the Health Information Portability and Accountability Act of 1996 (HIPAA)[2] as well as the operability of mobile devices and networks.

Current Standards

The American Telemedicine Association[3] has provided high-level guidance on what should be required to be consistent with HIPAA[4] and good practice during synchronous care delivery from a distance. In brief, the guidelines specify that synchronous audio/video sessions shall be secured to the greatest practical extent and that protected health information shall be secured through use of a private, point-to-point circuit, Integrated Services Digital Network, Advanced Encryption Standard (AES)[5] encryption, or virtual private network (VPN) for Internet transmissions. In addition to specific compliance with state and foreign privacy requirements for telemental health services provided in other countries, the guidelines call for network and software security protocols, for accessibility and authentication protocols, and for measures to safeguard data against intentional and unintentional corruption during both transmission and storage of data.

The need for standardized methods of protecting electronic patient data has resulted in the development and use of several standardized encryption methods for secure exchange of information over the Internet and other networks. In particular, data transfer of the Internet is secured by transport layer security (TLS) and its predecessor, secure sockets layer (SSL), by using asymmetric cryptography with 128-bit or even more secure 256-bit encryption methods. The current encryption standard used by the U.S. Government is called AES (National Institute of Standards and Technology).[5] The current AES specifies a cryptographic algorithm that is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. The intent was for the standard to be adopted and used by both the Federal government as well as commercial and private organizations. Because HIPAA requires 128-bit encryption of electronic protected health information, AES has provided a useful solution to data encryption needs in the health field. The standard is also commonly used by commercial companies. The popular program Skype™, for example, uses 256-bit AES.

VPNs are an option for transmitting voice, video, or data over the Internet. VPN provides a secure way of connecting to a private local area network at a remote location, using the Internet or any unsecure public network to transport encrypted network data packets. Mobile VPNs can be applied in settings where the end point of the VPN is not fixed to a single Internet protocol address, but instead roams across

DOI: 10.1089/tmj.2011.0180

various networks such as data networks from cellular carriers or between multiple Wi-Fi access points.[6]

The adoption of the aforementioned encryption and secure communication standards has provided a level of data transmission security for many situations. There are several particular issues, however, that threaten the security of patient data with the use of mobile devices. The main concern with wireless technology, such as Wi-Fi, is that it is easier for third parties to monitor and record unencrypted data (including protected health information) than on VPN or traditional wired networks. Although there are current security standards such as Wi-Fi Protected Access (WPA and WPA2), end-users must setup this security feature for it to be effective. In real-world applications, there is no guarantee that this has occurred, particularly within in-home or public environments. Ultimately, electronic data encryption must occur before transmission in order to prevent threats to privacy in wireless environments. Although there are technical solutions to accomplish this, there is not a standardized business process in place for doing so at this time.

Another threat to data security comes from the mobile device apps themselves. Data security for apps is typically based on an application security model in which the developer (e.g., Apple, Google, etc.) of the app verifies the integrity of the application and then makes it available for download through an online store. It is not possible, currently, to guarantee that an app's storage and transmission of patient data will meet necessary security requirements to be HIPAA-compliant. Moreover, many apps on the market gather and send user information, such as name, passwords, location, demographic, or any other information, back to the software developers, which raises additional security concerns.[1,7] It is important to note that, in general, HIPAA does not apply to end-users who store or share data between other end-users on a personal mobile device; the burden is placed on the provider to not share information. If a healthcare provider is a HIPAA-covered entity, however, the provider must make sure that the mobile device is HIPAA-compliant if personal health information is to be exchanged or stored.

What Security Standards Must Accomplish

There are several key requirements that must be met for optimal use of mobile telehealth platforms. For one, security standards must support interoperability among disparate systems. Interoperability is the ability of two or more systems to interact with one another and exchange information in order to achieve predictable results. The need for security standards implementation has led to an increase in private companies that offer solutions for secure data storage and transmission. These solutions are, for the most part, proprietary, and although they may help to solve some immediate security needs, proprietary data security methods inhibit interoperability of devices. Also, given the rapid turn cycle of technology platforms, secure mobile telehealth systems must allow for future interoperability of legacy systems. These systems also need to work with upgrades in communications standards, such as upgraded transmission protocols and speeds.

Secure mobile telehealth systems must also allow for efficient storage and transfer of multimedia content. That is, they must encrypt all of the data to allow audio, video, and file sharing. This requirement can present difficulties for real-time encryption because it typically requires more bandwidth and complex real-time encryption/decryption to work efficiently. HIPAA specifies 128-bit encryption; thus, these systems must have this minimum level of encryption and preferably without the need for outside encryption or firewall devices. Software-based encryption can allow sessions to be securely conducted from any Internet connection, thus allowing users in home or in any other location where Internet access is available. Furthermore, these systems must also be transparent and seamless to the user, and consumers and healthcare providers must feel confident that their information is secure.

Technical Mobile Health Data Security Options

There are various modern data security information technology techniques that can be used to meet HIPAA compliance requirements. Some of these techniques involve existing technologies, others are new, and others are not yet existent (*Table 1*). The end state of each technique is to assure the security and integrity of data in all of its states: "data at rest," "data in use," and "data in motion."[8] The technique must also be flexible enough to meet healthcare requirements and ultimately to allow the provider and patient to build rapport and work together without worrying about data security. In this section,

Table 1. Security Option Pros and Cons

SECURITY OPTIONS	PROS	CONS
Web server	• Security standards for transmission exist.	• Lack of native functionality of mobile devices
	• Data stored on secure server, not mobile devices	• Dependent on server access
Mobile framework	• Standardized method between applications and operating systems	• Costs for development and testing
	• Not dependent on operating systems	• Working across different mobile platforms
OS	• Security standards built in	• Different OS companies
	• Shared costs	• Complexity for common standards
	• Partnerships	
Combination	• Strengths of each option	• Time consuming to build
	• Partnerships	• Many dependencies
	• Standardized across platforms	

OS, operating system.

we provide an overview of several of these methods as well as discussion of their pros and cons.

One method is to remove the responsibility of data encryption and security from the mobile platform by not storing data on it. Instead, a secure Web server can be used to host the viewable Web pages that use Web programming techniques such as HTML 5, CSS 3, and JavaScript. Secure Web connections between the mobile client and the Web server using TLS or SSL will meet the industry standard 128-bit encryption requirement. Thus, the data security (at rest, in use, and in motion) responsibility will reside with the Web server rather than the hardware device. This method may be utilized cross-platform and therefore has the ability to connect mobile device platforms and increase flexibility of use. Although this may meet the needs for most content-driven mobile applications, it fails to use the mobile device's native capabilities[9] and relies on an outside source that may require its own security considerations.

Another method is to create a secure mobile framework that uses external tools such as Phone Gap, Sencha Touch, JQuery Mobile, or iUI that reside between the applications and the mobile device operating system. This framework affords the opportunity to serve as the container that controls the applications data security (at rest, in use, and in motion) while not being dependent on operating system security controls. Creation of a secure mobile framework gives the operating system independence but comes with the high cost of development time as well as the need for testing to make sure that no security holes exist in the code.

A third method involves the development of secure mobile versions of operating systems for use within the medical community. This option could create partnerships and trust among smartphone companies, app developers, and end-users and also benefit from shared costs. The U.S. Government's use of the Research in Motion operating system on the BlackBerry® platform is an example of this. This method requires proper procedures for software updates to be carefully versioned to prevent mixture of secure and nonsecure operating system patches. This method has the advantage of controlling access to the native functionality of the mobile device while leaving application capabilities up to developers. The operating system manages responsibility of data security (at rest, in use, and in motion), which can unfortunately slow updates and application loading processes to maintain the secure operating system.

A final method is a hybrid approach that optimizes the strengths of each of the aforementioned approaches. The benefit of an integrated approach is the ability to share the responsibility of data security and even provide for redundancy to reduce single design failure. It also allows for the potential to implement security standards that utilize a stepped approach. The optimal integrated mobile environment would begin by including frameworks with HTML 5, mobile JQuery type software, such as JQuery Mobile or Sencha Touch, and a framework that works with the native environment, such as Phone Gap. This can be accomplished while steps are made to approach and coordinate with the companies that currently control the most used operating systems. The end point would be a robust system of data security that is not subject to a single point of failure. This also removes the data security burden from individually developed applications, allowing for more rapid and robust development of healthcare-oriented apps. This method requires work with the operating system companies, however, which is potentially time consuming and may delay rapid dissemination of other effective solutions.

Mobile Health Technical Authentication Options

Regardless of the technical data security method that is used, user authentication is another integral step to maintain data security and integrity. Even though HIPAA does not explicitly define the required authentication level, it may be time for this to be considered and discussed within the field. The industry standard of two-factor authentication should be the minimum acceptable level. RSA,[10] a security solutions company, describes two-factor authentication as strong encryption that meets two of the three requirements of something known (e.g., personal identification numbers [PINs], passwords), something possessed, or something unique about the person (*Table 2*). This leaves room for several options to properly authenticate mobile devices users.

PINs or passwords are a common "something known" requirement for strong encryption. HIPAA does not specify which method to use, but PINs are typically associated with numerals only, although some incorporate letters, and many can include as few as 4 characters. Passwords typically specify longer alphanumeric character sets. The development of PINs and passwords may be conducted through a static method that allows the individual to control the actual PIN or password or a dynamic method that provides one-time access for specific work products. Minimum PIN and password length, expiration time, and allowable and required characters should be developed and met regardless of the method used.

Table 2. Authentication Methods

AUTHENTICATION CATEGORY	METHODS
Something known	• Password
	• Personal identification number
	• Pass phrase
Something possessed	• Mobile device identification number
	• Tokens (USB, cryptographic, authentication, key fob)
	• Dongle
	• Smart card
	• Radiofrequency identification
Something unique to the person	• Fingerprint
	• Iris scan
	• Retina scan
	• Voice print

Security token systems are viable options for meeting the requirement for something possessed. In order to authenticate, the user must physically have the token card or device in his or her possession, such as the mobile device and its identification number. Stronger techniques involve the use of digital certificates and signatures to assure the integrity of the session. Some security token methods may require a reader and use USB or the medical Bluetooth® protocol (Bluetooth SIG). Use of IEEE Standard 11073-20601[11] and the Health Device Protocol stacks help meet medical device communication requirements.

Biometrics, such as voice, facial recognition, hand gestures, fingerprints, or retinal scans are methods that can fulfill the something unique requirement for authentication. Combinations of these biometric verifications can improve authentication techniques.[12] In particular, voice printing and facial recognition have the most potential for mobile health (mHealth) applications because of current audio and visual recording standards on many of the latest mobile devices. Biometric readers can also use USB and/or the medical Bluetooth protocol to communicate with a mobile device. For instance, a device may be able to recognize hand gestures or perform retina scans and securely send values to the mobile device via the secure medical Bluetooth protocol for authentication.

Acceptable mHealth strong authentication can include any of the methods described above if two of the three categories of something known, something possessed, and something unique to an individual are used. Careful selection and implementation of the chosen authentication methods must comply with HIPAA requirements and may extend to USB and Bluetooth protocols and devices, which must also meet these requirements. Overall, proper authentication and data security methods provide confidentiality and integrity as well as accountability by providing an auditing trail.

Given the increased use of newer technology tools among developers, a cross-platform mobile framework is possible. More focus on these technologies as well as collaboration with the individual companies to create standardized policies and a secure mobile framework that is cross-compatible with current operating systems would be beneficial. Optimally, software developers should be able to write software connecting to the secure mobile framework's interfaces without concern about the mobile device's underlying operating system. If the development of a secure mobile framework and HIPAA-compliant authentication is left up to the operating system companies or each application developer, too many dependencies may result that will likely reduce the success of the application.

Conclusions

With this article, we have provided an overview of potential data security solutions and have suggested a stepped approach to implementing data security methods to provide for flexible and robust app development. The solution must include standardized policies, technologies, and administrative practices to assure data security. There continues to be debate, however, about the development of standards to assure the security of data during storage and transmission. To a large degree this debate has lost focus in the field through ongoing discussion about the standards rather than focus on how to assure the standards are met. As we have detailed in this article, data security standards for HIPAA compliance have been defined (e.g., 128-bit encryption). What has not been established is a standardized methodology to make sure that these standards are met and enforced in a manner that does not place the burden on each individual app that is developed.

A successful move towards standardized data security methodology will require partnerships among consumers, private industry, advocacy groups, and governments. Consumers have significant influence given the growing use of smartphones for healthcare access as well as demand for service providers that offer the most trusted data security precautions. Recent decisions by the industry to standardize mobile phone chargers, for example, suggest that consumer demand can lead to voluntary decisions of private companies to standardize technical requirements. A standard methodology may be seen as removing competitive advantage; however, in many ways it increases competition by emphasizing development on truly unique features, rather than those deemed ubiquitous across an industry. Advocacy and trade groups such as the American Telemedicine Association and CTIA—The Wireless Association can also play a significant role because they are well organized and positioned to consolidate the demands of consumers with industry experts to define and recommend strategies. Expert panels, workgroups, and annual association meetings are excellent platforms to release policy and position papers that can clarify and set a course for requirements and data security methodology and policy. Ultimately, governments have the mandate and authority to formalize recommendations that protect citizens. Thus, we recommend a coordinated expert review and opinion to inform government acceptance and implementation of mHealth data security requirements.

In conclusion, modern mobile telehealth platforms and smartphone apps provide new opportunities for delivering care to any location. Current mobile telehealth requires sophisticated technological safeguards to mitigate the risk of unauthorized access, disclosure, or threats to data integrity, and it can be expected that future technologies will require modifications to maintain privacy requirements. The lack of standardized data security to assure interoperability and to maximize the full capabilities of mobile devices presents a significant barrier to care. Until the data security issue is resolved, the field will not be able to maximize the capabilities that mHealth technology affords.

Disclosure Statement

No competing financial interests exist.

REFERENCES

1. Luxton DD, McCann RA, Bush NE, Mishkind MC, Reger GM. mHealth for mental health: Integrating smartphone technology in behavioral healthcare. *Prof Psychol* **2011;**42:505–512.

2. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA): Security standard. Available at www.cms.hhs.gov/SecurityStandard/ (last accessed August 22, 2011).

3. American Telemedicine Association. Practice guidelines for videoconferencing-based telemental health. October **2009**. Available at www.americantelemed.org/files/public/standards/PracticeGuidelinesforVideoconferencing-Based%20TelementalHealth.pdf (last accessed August 22, 2011).

4. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Available at www.cms.hhs.gov/HIPAAGenInfo/ (last accessed August 22, 2011).

5. National Institute of Standards and Technology. Federal information processing standards publication 197. **2001**. Available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (last accessed August 22, 2011).

6. Phifer L. Mobile VPN: Closing the gap. SearchMobileComputing.com. 2006. Available at http://searchmobilecomputing.techtarget.com/tip/Mobile-VPN-Closing-the-gap (last accessed August 22, 2011).

7. Thurm S, Kane YI. Your apps are watching you. Wall Street Journal. **2010**. Available at http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html (last accessed August 22, 2011).

8. The Health Information Technology for Economic and Clinical Health (HITECH Act) of 2009. HITECH breach notification sec. 13402. Notification in the case of breach. Available at www.hipaasurvivalguide.com/hitech-act-13402.php (last accessed August 22, 2011).

9. W3C. Mobile Web application best practices. **2010**. Available at www.w3.org/TR/mwabp/ (last accessed August 22, 2011).

10. RSA. Information security glossary: Two-factor authentication. 2011. Available at www.rsa.com/glossary/default.asp?id=1056 (last accessed August 22, 2011).

11. IEEE Standards Association. IEEE health informatics—personal health device communication part 20601: Application profile—optimized exchange protocol amendment 1. IEEE 11073-20601a-2010 (Amendment to IEEE Std 11073-20601-2008). Piscataway, NJ: IEEE. **2011;**1–119. doi: 10.1109/IEEESTD.2011.5703192. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5703192&isnumber=5703191 (last accessed August 22, 2011).

12. Varchol P, Levicky D, Juhar J. Multimodal biometric authentication using speech and hand geometry fusion. Bratislava, Slovakia: IEEE. *15th International Conference on Systems, Signals and Image Processing, 2008. IWSSIP 2008.* **2008;**57–60. doi: 10.1109/IWSSIP.2008.4604366. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4604366&isnumber=4604343 (last accessed August 22, 2011).

Address correspondence to:
David D. Luxton, Ph.D.
National Center for Telehealth and Technology
9933 West Hayes Street
Joint Base Lewis-McCord
Tacoma, WA 98431

E-mail: david.luxton@us.army.mil

Received: August 30, 2011
Revised: September 15, 2011
Accepted: September 16, 2011