

HIPAA Security Rule Compliance When Communicating with Patients Using Mobile Devices

January 26, 2011

Agenda

- Increase in health care providers' and patients' use of mobile devices
- Overview of select Health Insurance Portability and Accountability Act ("HIPAA") Security Rule requirements
- Special security risks presented by mobile devices
- Initial best practice suggestions for grantee review and discussion

NOTE: When we say "mobile device" in this presentation we mean a pocket-sized computing device, which typically has a display screen with touch input and/or a miniature keyboard. This generally includes "smart phones," and personal digital assistants (e.g. the IPOD Touch and the IPAD). This does not include laptop computers.



Increasing Physician Use of Mobile Devices Can Help Inform Discussion of Patient Use of Mobile Devices

“By 2012, all physicians will walk around with a stethoscope and a smart mobile device, and there will be very few professional activities that physicians won't be doing on their handhelds.”

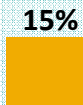
Monique Levy, Sr. Dir. Of Research at Manhattan Research, October 2009

81%

of American physicians will own smart phones by 2012
(Manhattan Research October 2009)

85%

Are you looking to use tablets or other mobile devices?
(Impravata Inc.)



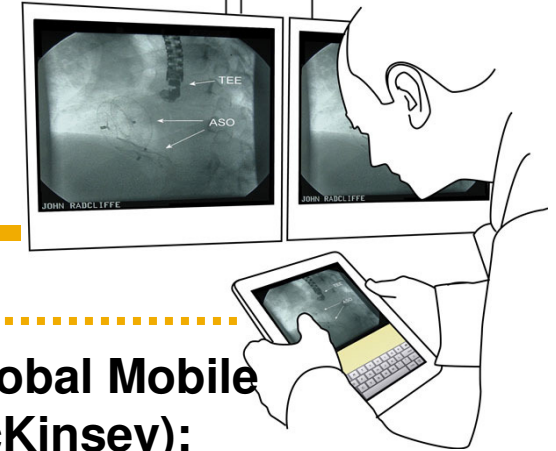
Yes

No

Full citations listed in back.



A Growing Market of Patients



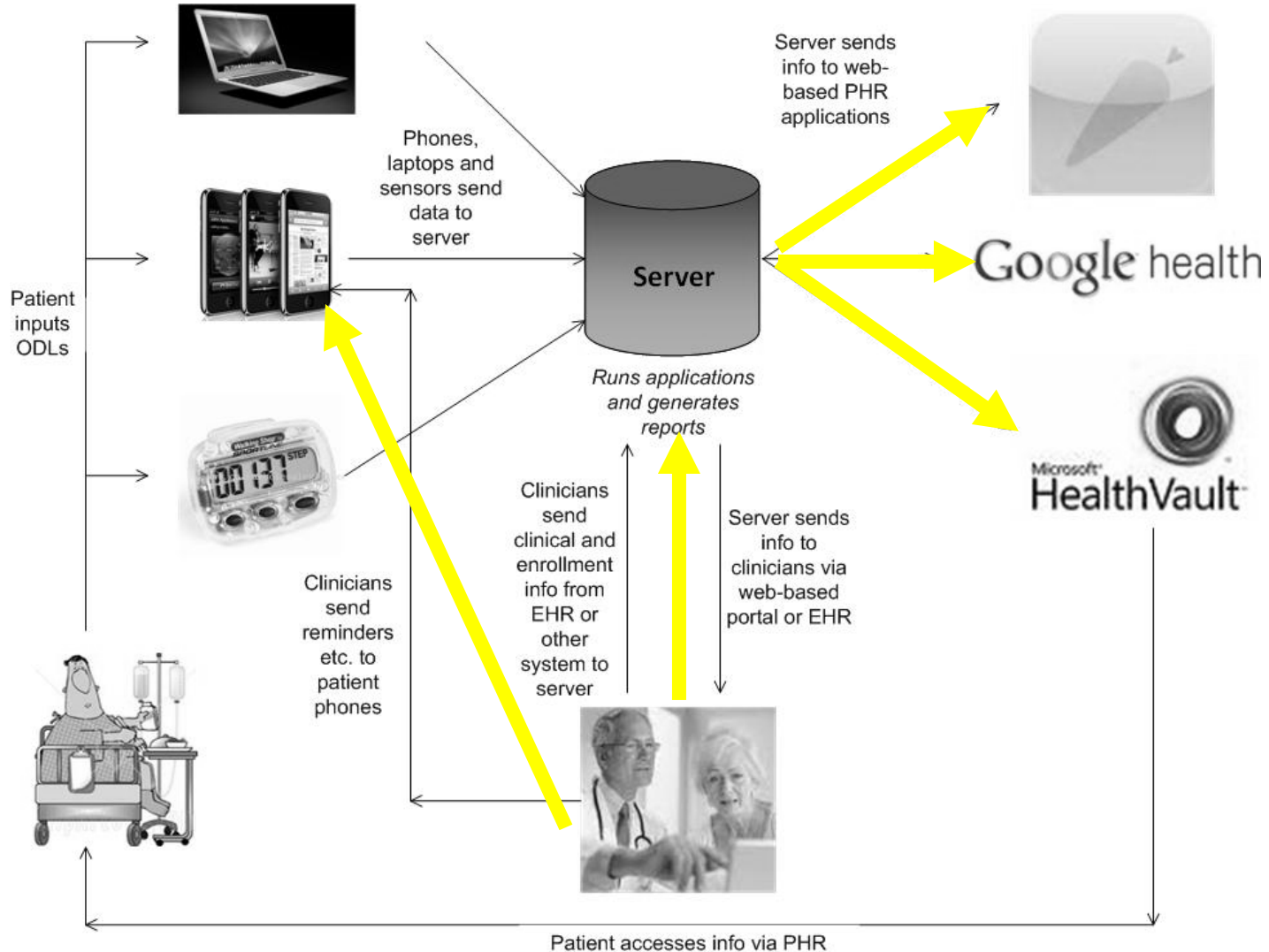
The \$60 Billion Global Mobile Health Market (McKinsey):

- In the next five years, an estimated 1.4 billion people will use smart phones worldwide; more than 1 out of 3 people with a smart phone will have a health-related app on their phone.
- A global market survey from McKinsey & Company suggested that mobile health opportunities in 2010 could be worth \$20 billion in the US alone.
- Another study conducted by the Euro RSCG Life Group found that over 44% of American smart phone users expect to use more mobile health and wellness applications in the near future.

Project HealthDesign Grantees' Use of Mobile Devices

	San Francisco State University	University of California, Irvine	RTI International and Virginia Commonwealth University	University of California at Berkeley (To be confirmed)	Carnegie Mellon
Name of Project	<i>ODLs Via Mobile Platforms for Youth with Obesity and Depression</i>	<i>Use of ODLs among Low Birth Weight Infants and Their Caregivers to Improve Care and Reduce Incidence of Chronic Conditions over the Lifespan</i>	<i>BreathEasy- A PHR for Adults Living with Asthma and Depression</i>	<i>Crohnology.MD</i>	<i>Embedded Assessment of Elder Activities (Cognitive Decline and Arthritis) for Augmenting PHRs</i>
Devices Given to Patients	iPod Touches	Smart phones Scale	Smart phones	Smart phones Sensors (e.g. pedometers) CyTek report card	Sensors Laptops
Information Flow	ODLs are sent from iPod Touch to TheCarrot.com through app on device. The Carrot.com generates reports, which patients view through app on device.	ODLS are sent from smart phone to HealthVault through FitBaby app on phone. Patients access reports through app on smart phone.	ODLs are sent from smart phones to the RTI server. Clinicians view reports/dashboards through a portal or EHR. Patients may also view reports through dashboard on smart phones.	ODLs are sent from smart phones to Google Health and project servers. Clinicians view reports/dashboards through a portal or EHR.	ODLS are sent from laptops to HealthVault. Reports will be generated, which clinicians and patients may view on their laptops.
Use of SMS?	Yes. Clinicians send SMS messages to patients.	No.	Not planned at this time.	Possible.	No

General Applicability of HIPAA to Grantees' Projects



Key HIPAA Security Rule Principles

Few Bright Line Requirements

Establishes categories of safeguards to secure electronic protected health information (“E PHI”). Provides Covered Entities (“CEs”) with discretion to determine which safeguards to employ in each category.

Scalable

Level of safeguards can vary with size and resources of CE. Small physician practices do not have to adopt the same types of safeguards as a large hospital system or insurer.

Required vs. Addressable Standards

Standards include those that are “required” and those that are “addressable.” Addressable standards do not have to be implemented if, through a risk analysis, a CE determines that a standard is not feasible and adopts alternative safeguards to the extent practical.

The Importance of Risk Analysis

- Conducting a risk analysis is the first step in identifying and implementing appropriate safeguards.
- Risk analyses inform which technology (and other) solutions a CE should adopt, when they should be adopted, and whether and which alternative safeguards should be implemented instead.
- The risk analysis implementation specification (Section 164.308(a)(1)(ii)(A)) requires CEs to:

“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”

Key Security Rule Requirements Relevant to Use of Mobile Devices

Standards	Citation	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(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	(A)
		Encryption	(A)

Standard 1: Access Control

■ Standard

-> Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in the “Administrative Safeguards” section of the Security Regulations.

■ Implementation Specifications

->
 1. *Unique User Identification.* [Required] Assign a unique name and/or number for identifying and tracking user identity.
 2. *Emergency Access Procedure.* [Required] Establish (and implement as needed) procedures for obtaining necessary EPHI during and emergency.
 3. *Automatic Logoff.* [Addressable] Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
 4. *Encryption and Decryption.* [Addressable] Implement a mechanism to encrypt and decrypt EPHI.

Standard 2: Audit Controls

■ Standard

-> Implement hardware, software, and/or procedural mechanisms that record and examine activity information systems that contain or use EPHI.

■ Implementation Specifications

-> None. The CE's risk assessment and risk analysis can help determine how intensive the entity's audit control function should be.

Standard 3: Integrity

■ Standard

-> Implement policies and procedures to protect the integrity of EPHI and assure it is not improperly altered or destroyed.

■ Implementation Specifications

-> *Mechanism to Authenticate EPHI.* [Addressable]
Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.
-

Standard 4: Person or Entity Authentication

- **Standard**

-> Implement procedures to verify that persons or entities seeking access to EPHI are who they claim to be.

- **Implementation Specifications**

-> None. Personal authentication can be achieved through a variety of mechanisms, including passwords, tokens, biometric identification, and others.

Standard 5: Transmission Security

- **Standard**

-> Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

- **Implementation Specifications**

1. *Integrity Controls.* [Addressable] Implement data integrity measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.
2. *Encryption.* [Addressable] Implement a mechanism to encrypt EPHI whenever deemed appropriate.

Special Risks Presented by Mobile Devices¹

■ Loss, Theft or Disposal

■ Risk level: high

- Because of their small size, mobile devices can be lost or misplaced. They are also an easy target for theft. If proper measures are not in place and activated, gaining access can be straightforward, potentially exposing sensitive data that resides on the device or is accessible from it.

■ Unauthorized Access

■ Risk level: high

- According to the National Institute of Standards and Technology (“NIST”), most cell phone users seldom employ security mechanisms built into a device, and if employing them, often apply settings that can be easily determined or bypassed (e.g. passwords).
- HHS cites data storage and transmission as potential risk areas as well.

¹The risks listed here were identified either by NIST in its 2008 “Guidelines for Cell Phone and PDA Security” Special Publication 800-124 or the U.S. Department of Health and Human Services in its 2006 HIPAA Security Guidance for Mobile Devices 12/18/2006.

Special Risks Presented by Mobile Devices²

■ Malware (Viruses)

■ Risk level: low

- Mobile malware can infect a mobile device when a user downloads a virus disguised as a game or security patch etc. Malware can also be appended to email, text and other instant messages available on cell phones. Malware can intercept or access information on the mobile device, collect and send information out of the device and/or, destroy stored information, among various other behaviors.
- According to NIST, malware outbreaks on mobile devices have been mild when compared to malware incidents on laptops.

■ Cloning

■ Risk level: low

- If certain unique identifiers built into a cell phone are reprogrammed into a second cell phone, a clone is created that can masquerade as the original.
- According to NIST, cloning is not as prevalent among digital networks as it was when cell phones relied on analog networks. Today, encryption prevents most device identifiers from being recovered and used to clone a device.

²Id.

Mobile Device Security Risk: Lessons Learned from HHS Breach Notification Reports³

- Majority of reported breaches involve loss or theft of paper records, portable medium (CD or tape) or laptops.
- Few reported breaches involve hacking or other external technical penetration.
- Out of 214 total breach reports, only 23 involved “portable electronic devices” (other than laptops) and all of those were loss or thefts.

Breaches affecting 500 or more individuals are reported by HHS at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>

³HHS breach reports accessed on December 27, 2010.

.....

Initial Best Practice Suggestions for Grantee Review and Discussion

.....



**Overarching Questions for Grantees: Do These Suggestions
Sound Feasible? Necessary? Sufficient?**

Implementing Appropriate Security Practices

- Analyzing security practices when patients are using mobile devices raises issues not contemplated under the Security Rule.
- When conducting a risk analysis to determine which strategies to use to protect EPHI communicated to/from a patient using a mobile device, health care providers should consider the following factors:
 - The complexity and cost of the security measure (e.g. downloading and installing a third-party encryption program).
 - The ability of the patient to perform the task.
 - The effect the security measure will have on the efficient delivery of clinical care (e.g. the effect of locking a device or application with a password on the patient's willingness to report ODLs).
 - The probability and criticality of potential risks to EPHI.

Question for Grantees: Are There Other Factors We Should Include? 19

Best Practice Recommendations: Road Test

■ Transmission Security

- HIPAA Standard: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

■ **Background:**

- Mobile devices can send data in various ways, such as:
 - Internet protocols (e.g. those used by many of the unique software applications grantees have developed under their projects)
 - Email (which uses traditional Internet protocols)
 - Voice (e.g. traditional telephone)
 - Text (“SMS/MMS”) messaging
- Most of these channels are secure without the patient having to take any additional steps...except for text messages...

Spotlight on Text Messages



Where Are Text Messages Located?

When “at rest” on a smart phone, data is generally stored in the computer inside the smart phone (often called “on-board memory”) or on a memory card that is inside of the phone but can be removed.

Some data can also be stored on what is called a SIM card, which ties a smart phone to a user’s phone number and can also be removed.

Data at rest can also be stored offsite on a wireless carrier’s server.

Data can be “in transit” to another smart phone or elsewhere.

Spotlight on Text Messages: Encrypting Data at Rest

- Many smart phones include built-in encryption capabilities for data at rest. For example, through the Blackberry Enterprise Server, Blackberry enables “enterprises” to set the security policies for its employees’ phones.
 - Patients who have smart phones that are not provided by their employer or 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...OR...clinicians providing the smart phones could take responsibility for enabling encryption options for them.
- Many smart phones 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 smart phone.
 - The price of these applications varies, and the difficulty of installation/use can be high.

Spotlight on Text Messages: 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 smart phone (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 smart phones for the purposes of protecting ODLs or other information they communicate to their health care providers through their smart phones.

Best Practice Recommendations: Road Test

■ Securing Text Messages

- Providers that give patients smart phones should investigate whether they can preset the smart phones' built-in encryption tools for data at rest.
- Providers should also investigate the availability, effectiveness, and price of third party encryption tools that encrypt data as it is being transmitted to and from smart phones.
- If implementation of encryption tools is not feasible, providers should engage in alternative protection behaviors:
 - Limit EPHI transmitted via unencrypted channels (e.g. carefully word communiqués with patients);
 - Direct patients to obtain detailed information through a web portal or other secure means.
- Providers should also offer education/training to patients on the risks of transmitting EPHI to clinicians through text messages.

Question for Grantees: Does this sound feasible to you?

Best Practice Recommendations: Road Test

- **Person/Entity Authentication and Access**
 - HIPAA Standard: Implement procedures to verify that persons or entities seeking access to EPHI are who they claim to be.
 - HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in the “Administrative Safeguards” section of the Security Regulations.
- Providers should offer education/training to patients with whom they communicate via mobile device on things like use of passwords and proper device handling.
- Providers should also encourage patients to sign a statement indicating they understand the heightened risks if they do not:⁴
 - Protect their mobile devices with passwords;
 - Enable their device’s automatic logoff function after a specified amount of time;
 - Refrain from sharing their device with friends and family.

Question for Grantees: Does this sound feasible to you?

⁴Project HealthDesign grantees need not retroactively have participating patients sign such a statement.

Best Practice Recommendations: Road Test

▪ Audit Controls

- HIPAA Standard: Implement policies and procedures to protect the integrity of EPHI and assure it is not improperly altered or destroyed.
- *Not Applicable/Providers need not take any additional action.*
 - As with the other Security Rule standards, the audit control requirement does not apply to devices controlled by patients.
 - From a best practice perspective, there is no need for a patient to log and audit his own use of his/her mobile device as it is generally only the patient who will have access to the device.

▪ Integrity

- HIPAA Standard: Implement policies and procedures to protect the integrity of EPHI and assure it is not improperly altered or destroyed.
- *Not Applicable/Providers need not take any additional action.*
 - As with the other Security Rule standards, the audit control requirement does not apply to devices controlled by patients.
 - From a best practice perspective, there is no need for a patient to take steps to ensure the integrity of the EPHI they store and/or transmit through their mobile devices as risk of alteration or destruction is low.

Question for Grantees: Does this sound feasible to you?

Next Steps

- Determine whether the webinar approach is a good one for collecting grantees' feedback on cross-cutting policy issue obstacles.
 - **Question for Grantees: Does the webinar approach work for you? Is there an alternative approach you would prefer?**
- Remaining cross-cutting policy issue obstacles to be addressed:
 - Uncertainty about health care providers' liability when incorporating ODLs into clinical practice and communicating with patients electronically
 - Uncertain policy environment regarding an individual's use of internet-based tools to share health information

Appendix

Citations: Mobile Device Use Estimates

- “Physicians in 2012: The Outlook for On Demand, Mobile and Social Digital Media.” Accessed on 12/29/2010. Released October 2009.
http://www.manhattanresearch.com/newsroom/Press_Releases/physician-smart_phones-2012.aspx
- “2008 Identity Management Trends in Healthcare Survey Research Brief” Imprivata, Inc. Accessed on 12/29/2010. Released 2008.
http://www.imprivata.com/custom/confirmation/resource/research/2008_id_mgmt_trends_health_care.pdf
- McKinsey Mobile Health Care Survey 2009. McKinsey & Co. Accessed on 12/29/2010.
http://www.mckinsey.it/idee/practice_news/global-mobile-healthcare-opportunity.view
- “Mobile Health Market Report 2010-2015” Research2guidance. Accessed 12/29/2010.
<http://www.research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/>
- “Bigger than DTC? The Promise of Mobile Health.” Euro RSCG Life 4D. Survey conducted September 2010.

HIPAA Security Rule Overview

“Ensure the *confidentiality, integrity, and availability of all electronic protected health information* the covered entity creates, receives, maintains or transmits.”

→ “**Integrity** means the property that data or information have not been altered or destroyed in an unauthorized manner.”

→ “**Availability** means the property that data or information is accessible and useable upon demand by an authorized person.”

→ “**Confidentiality** means the property that data or information is not made available or disclosed to unauthorized persons or processes.”

§164.304 and 164.306(a)(1)

30

HIPAA Security Rule Overview Cont'd

A covered entity must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to electronic Protected Health Information.

Covered Entities means:

- (1) A health plan
- (2) A health care clearinghouse
- (3) A health care provider who transmits any health information in electronic form

Electronic Protected Health Information (EPHI) means:

individually identifiable health information ... that is (i) Transmitted by electronic media; or (ii) Maintained in electronic media