3M

Privacy Filters

Mobile Technology in Healthcare:
Risks, Consequences and Remedies

By Kate Borten, CISSP, CISM

The use of mobile technology products – particularly smartphones and tablets – is taking the healthcare field by storm. The convenience of having a handheld device in your pocket or bag that allows you to work while waiting for a meeting, boarding a plane, or sitting at a soccer game is irresistible to a growing number of busy healthcare professionals.

The Health Care Blog[1] references a current Manhattan Research study showing that 30% of surveyed physicians already own iPads, even though the devices were only released in 2010. While this trend is exciting for the future of the healthcare industry, it could also have potential consequences for the confidential information to which doctors are privy. Current mobile technology users present expanded risks to the security and privacy of information assets – including Protected Health Information (PHI) – that are accessed, viewed, stored or cached on mobile devices.

Risks

A number of factors contribute to the security and privacy risks associated with mobile devices. In addition to their high adoption rate, smartphones and tablets are less secure than desktops and laptops, due in part to users' lack of security risk awareness and to inconsistent or unavailable security features.

Vulnerabilities such as weak or missing policies, procedures, workforce training, and monitoring increase this level of risk.

In order to properly examine mobile risks and to look for solutions, these threats have been broken down into the following three areas:

- Breach of data when at rest on a mobile device.
- Breach of data during transmission to/from a mobile device.
- Breach of an organization's private network and information assets via a mobile device.

Breaches occur through a variety of pathways. Mobile devices are most susceptible through the following threats:

- **Mobile Malware:** Malware targeting mobile devices is a growing threat as cybercriminals see opportunities for profit and disruption. The main malware carrier is mobile applications that can be infected with malicious code. A May 2011 report from Juniper Networks[3] states, "[E]nterprise and consumer mobile devices are exposed to a record number of security threats, including a 400 percent increase in Android malware, as well as highly targeted Wi-Fi attacks" over the past year.
- **Lack of Visual Privacy:** Confidential data can be exposed when users fail to prevent others from viewing display screens. Device portability means that unless a user is working in isolation, disclosure of PHI and other confidential information to unauthorized people is likely to occur frequently. As HIPAA's Security Rule makes clear, physical access to a device containing PHI or giving access to PHI must be carefully

HIPAA's Security Rule requires covered entities and their business associates to protect workstations and their surroundings [45 CFR 164.310(b) and 164.310(c)]. The term workstation applies to user computing devices from desktops to portables including laptops, tablets, cell phones, pagers, and smartphones. Regulations also apply to media storing electronic PHI such as portable CDs, memory sticks, and MP3 players. The security protections must follow the ePHI wherever the mobile devices and media are, and regardless of whether the organization or the workforce member owns the device.

Findings from recent Ponemon Institute Smartphone Survey by AVG[2]

- **57%** of surveyed smartphone users said that security is not important as a smartphone feature
- **Fewer than half** of surveyed users have keypad locks or passwords on their smartphones
- **Only 29%** have considered installing antivirus protection
- **65%** of the respondents agreed with the statement: "I worry more about the security of my desktop or laptop computer than my smartphone."
- **55%** of respondents acknowledged that using smartphones for both personal and business uses puts confidential business data at risk

controlled. When it comes to physical access to mobile or portable devices and media, organizations need to employ "security on steroids," and fully educate their staff on the consequences.

- **Consumerization of Devices**: Complicating matters even more is the fact that employees and other workforce members often use their own smartphone or tablet for work purposes. This makes it even more difficult for organizations to impose security requirements, while the resulting co-mingling of personal and business data increases the risk of privacy breaches. Even if the organization has purchased the device for an employee, most users acknowledge they also use the device for personal reasons.
- **Varying Operating Systems**: Unlike desktop and laptop computers, where it is largely a UNIX/Linux versus Microsoft world, mobile devices run on many different operating systems. Apple's iOS, RIM, and Android are among the best-known systems, but there are more than a dozen other platforms on smartphones today. This lack of standardization makes it difficult for organizations to set standard security controls, making it harder to properly protect data on the device.
- **Vulnerable Connections**: Even if the healthcare organization provides an encrypted VPN, users may not bother with a secure connection or may use a public hotspot when using the device for personal reasons, which can expose confidential business data on the device.
- **Loss and Theft of a Device**: Loss and theft of mobile devices is a very serious problem. Of the HIPAA Privacy and Security Breaches posted on the U.S. Department of Health and Human Services' website, loss and theft of portable devices and media has resulted in the largest number of comprised records since reporting began in 2009.

Consequences

HIPAA's Privacy Rule requires protection from unauthorized access to or disclosure of PHI. The Security Rule requires covered entities and their business associates to implement security controls that protect the confidentiality (most at risk on mobile devices), integrity and availability of PHI. Today, most states have breach notification laws requiring organizations to protect certain personally identifiable data.

Organizations that fail to adequately protect PHI are subject to penalties, cost of notification and remediation, loss of reputation and possible loss of future revenue. According to The Ponemon Institute's March 8, 2011 report, "US Cost of a Data Breach," the average cost per compromised record is $214. The average cost to an organization per event has risen to $7.2 million.

The HITECH Act will only increase these costs. Often a breach is related to HIPAA non-compliance, for which Congress significantly raised the civil monetary penalties. In the future, some portion of these penalties will be shared with affected individuals, which is likely to motivate more patients and their lawyers to file complaints. The Act also requires HHS to perform more compliance reviews of covered entities and their business associates. Further, state attorneys general are now empowered to bring legal action in healthcare privacy and security violations, and some have already done so.

Remedies

Questions to answer before writing a mobile security policy:

- Who should be permitted to use mobile devices for work?
- Should workers be permitted to use their own devices, or should the organization provide the devices? What are the trade-offs? Should workers be permitted to use organization-provided devices for personal use?
- Should only specified devices (such as RIM BlackBerry) be permitted?
- Should workers be permitted to store confidential data on the devices? Should data be backed up to the network?

The first step to reduce an organization's risk surrounding the use of mobile devices is to perform a risk assessment. As described by the National Institute of Standards and Technology and HHS, this involves identifying vulnerabilities and threats, weighing the resulting risks, and then implementing appropriate security controls to reduce risks that are "too big" to accept. HIPAA's Security Rule describes possible controls in three categories: administrative, physical, and technical.

- **Administrative:** A mobile device policy should specify acceptable and unacceptable usage for employees to ensure the device is used only for work purposes, on private networks, and with approved applications, for example. The policy should also require the mobile device user to acknowledge agreement with the policy and commitment to follow it, including using specified security controls such as acceptable passwords and privacy screen protectors to prevent unauthorized view of the display screen.

  Users should then receive training in the security features of their mobile devices. Passwords and keyboard locks should be required. Users should be reminded to prevent others from viewing displays, to clear old data, and to immediately report loss or theft of their device.

- **Physical:** It's important for organizations to not overlook necessary physical protections to ensure confidential data is protected at all times. Physical controls fall mainly into two areas: (1) keeping the device in the user's possession or locking it, and (2) using a privacy screen protector or film to protect visual privacy and stop unauthorized personnel from getting access to PHI and other confidential information.

- **Technical:** Technical controls cover the full range of device protections including user authentication, keyboard lock, anti-malware software, firewall, encryption for data at rest, VPN client, remote "wipe" agent, and possibly a virtual machine to separate business and personal use. Apart from the device, organizations should implement VPNs, firewalls between wired and wireless networks, and consider MAC address filtering. Additionally, organizations should set up their own mobile apps store or identify approved stores.

With the use of mobile technology in healthcare rapidly expanding, so too are the associated risks. As a result, data breaches are becoming more common, with serious consequences for organizations and the individuals they serve.

---

[1] "The Doctor Is In (and Using an iPad)" by Jane Sarasohn-Kahn, The Health Care Blog thehealthcareblog.com

[2] "Smartphone Security" by the Ponemon Institute and sponsored by AVG free-product.blog.avg.com/2011/03/avg-mobile-survey-results.html

[3] "Malicious Mobile Threats Report 2010/2011" by Juniper Networks www.juniper.net/us/en/company/press-center/press-releases/2011/pr_2011_05_10-09_00.html