# Mobile Device Use, Reuse, and Disposal

Save to myBoK

*by Laurie Southerton, CHP, CHSS*

The healthcare industry increasingly communicates via technology. Mobile devices are becoming prevalent in many organizations to the point where many staff find it difficult to work without them.

The HIPAA privacy and security rules require the private and secure handling of patient information that increasingly resides on mobile devices. As such, organizations are responsible for the secure use, reuse, and disposal of mobile devices such as notebooks, tablet PCs, PDAs, and smartphones.

## HIPAA Privacy and Security Rules

The HIPAA privacy rule mandates that healthcare organizations keep protected health information (PHI) private. This pertains to all transmitted and maintained health information that identifies an individual or that could reasonably be used to identify an individual, including name, address, phone number, Social Security number, e-mail address, license plate number, prescription numbers, and medical record numbers.

The HIPAA security rule protects all forms of electronic PHI through controls maintained as administrative, physical, and technical safeguards. Mobile device security is primarily addressed under technical safeguards such as access control, person or entity authorization, audit control, and transmission security or encryption.

## Designed to Preserve Data

To address the use, reuse, and disposal of mobile devices, one must first understand what is stored in the various components of a typical mobile device.

A mobile device is a computer with an operating system, applications, and storage areas. Just as with all complex modern computing systems, mobile devices are designed to preserve, rather than shed, data. For instance, in nearly all mobile computing devices the subscriber identity module (SIM), a smart card, securely stores the mobile phone unique subscriber information or the international mobile subscriber identity.

This information includes subscription information, all saved and dialed telephone numbers, phone preferences, text messages (including deleted messages), the network state information including the current location area identity, and information concerning countries visited by the user.

The phone has internal memory in the form of an onboard flash memory from which deleted items can be retrieved. Almost all data written to a computing hard drive or other type of digital storage remain there until overwritten. Deleted items are not erased from the device; deletion merely removes the pointer to the data. As such, a typical hard drive is littered with remnants of information that can be retrieved with widely available tools and techniques.

Information stored on a mobile phone can include the phone identity, some text messages and multimedia messages, location information, wordlist database, audio recordings, phone settings (language, date, time, tone, volume), camera images, computer files, logged incoming calls and dialed numbers, executable programs, calendar events and tasks, general packet radio services, Wireless application protocol, and Internet settings and the cache from these activities. As new calls and messages are stored in phone memory and on the SIM, new calls and messages overwrite deleted material that may have been stored but not yet overwritten.

Many times the phone has a flash memory card used to extend storage capacity. This is considered a file system and can be used to store multimedia messaging service messages that may include images, audio, video, and rich text. However, phone

system items are not stored on flash memory.

Privacy issues surface when the potential exists for renovating all the information amassed in the various components of a typical mobile device and using it with malicious intent.

## Mobile Device Technical Controls

All healthcare organizations that authorize the use of mobile devices should have sound security policies in place that restrict personnel from using personal mobile devices. Ideally, each issued or authorized mobile device has a standard image installed that cannot be altered by the individual user.

The image must:

- Support applications that allow only properly authenticated individuals to access the device and its information
- Allow for audit control through logging activities
- Encrypt the data and information transmitted

Change management policies and procedures are IT safeguards that limit error and prevent unauthorized changes to computer systems and disruptions to the organization's IT assets. Change management policy and the resulting change management control system contain specific procedures that define analysis, application, and review of changes to the IT infrastructure.

These policies should maintain current standards for mobile devices. If the security policy is implemented and enforced, device reuse and disposal become a natural extension. Privacy for the information stored in the various components of a typical mobile device must be considered per the required and addressable HIPAA technical controls.

### Access Control and Authentication

Access control addresses the levels of privileges granted to system resources. Authentication is based upon verifying the unique identity of a user through something the user knows, has, or is (such as a password, token, or retinal scan).

HIPAA requires that controls restrict PHI access to properly authenticated, authorized individuals only and only when required by a business need. The determination of who has access to what information is a function of organizational policy, and the organization's rules of access should be tailored to fit its particular situation.

The requirement supports emergency access control. As such, the security policy must support a solution for authorized users who have forgotten or lost an authentication mechanism such as a password or keycard. One consideration is implementing a secure form of two-factor authentication, which requires at least two authentication forms, such as a password and a keycard.

This differs from traditional password authentication, which requires only one authentication factor in order to gain access to a system. Auditing and logging software used in conjunction with devices such as token authenticators provides this type of automatic logging.

### Audit Control

A mechanism must exist to record and review mobile device activity so that individuals can be held accountable for their actions. The logging activity must be such that activities can be traced to the device and the user.

### Transmission Control

Technical security measures must protect against intrusion or unauthorized access when data and information are being transmitted. Data and information transmitted and stored in an encrypted form are much less likely to be exploited. To comply with HIPAA, strong encryption such as 256-bit symmetric encryption must be implemented.

## Use, Reuse, and Disposal

With implemented change management policies and procedures in place, the IT department should maintain a current standard image for each issued mobile device, know to whom each device has been issued, and regularly review audit logs and report anomalies.

If the device is to be reissued to an individual with identical access rights, the current SIM card can be removed from the device and destroyed and a new SIM card issued. There may be no reason to reimage the device. If flash cards are authorized, the contents of the flash drive should reflect the access parameters and may not need to be erased.

Still, the HIPAA privacy rule provides that the organization must reasonably safeguard PHI to prevent intentional or unintentional use or disclosure that is in violation of the privacy rule. With the amount of inadvertent PHI that may be viewed, the organization is best served by removing, destroying, and reissuing a new SIM card and erasing and reimaging the device as well as the flash drive when applicable.

If the device is to be reissued to an individual with different access rights, the SIM card must be removed and destroyed, and the device must be erased and reimaged with the current standard image. A flash card must be erased, overwritten, or totally destroyed.

If the device is to be disposed, the SIM card and flash memory (if applicable) must be removed from the device and destroyed. In order to positively ensure destruction of the mobile device, the device must be dissembled. The memory chip(s) or the hard drive must then be desoldered or physically removed, smashed, or otherwise destroyed.

Threats against the security and privacy of PHI are real. Personal information is a commodity that is readily bought and sold. Unfortunately, criminals go so far as to hack into hospital databases in order to obtain the Social Security numbers of newborns.

The development of forms, policies, and procedures is required to establish the compliance framework for the HIPAA privacy and security rules and provide a baseline for security. Although this article provides an overview, it is recommended that healthcare organizations consult with HIPAA professionals and legal counsel on the development of policies and agreements required by HIPAA.

## References

Ali Pabrai, Uday O. *HIPAA Certification: Professional 2nd Edition*. Boston: Thomson Learning, 2003.

Ali Pabrai, Uday O. *HIPAA Certification Security Specialist 2nd Edition*. Boston: Thomson Learning, 2003.

Chadwick, David W. “An X.509 Role-based Privilege Management Infrastructure.” Available online at www.permis.org/files/article1_chadwick.pdf.

IAnywhere Solutions. “Best Practices for Mobile Application Architectures.” May 2006. Available online at www.ianywheresolutions.com.

Le Bodic, Gwenael. *Mobile Messaging Technologies and Services: SMS, EMS and MMS*. West Sussex, England: John Wiley & Sons, 2003.

“RSA ACE/Server.” Available online at www.securehq.com/images/rsa/AS51_DS_1103.pdf.

Willassen, Svein Y. “Evidence in Mobile Phone Systems.” (Synthesized version of the paper “Forensic Analysis of Mobile Phone Internal Memory,” presented at the Conference of Digital Forensics in Orlando, FL, 2005.)

Wilson, Tim. “Stolen Data’s Black Market.” September 7, 2006. Available online at www.darkreading.com/document.asp?doc_id=103198.

***Laurie Southerton*** *(laurie.southerton@gmail.com) is a private consultant for security analysis.*

---

**Article citation**:
Southerton, Laurie. "Mobile Device Use, Reuse, and Disposal" *Journal of AHIMA* 78, no.6 (June 2007): 68-70.