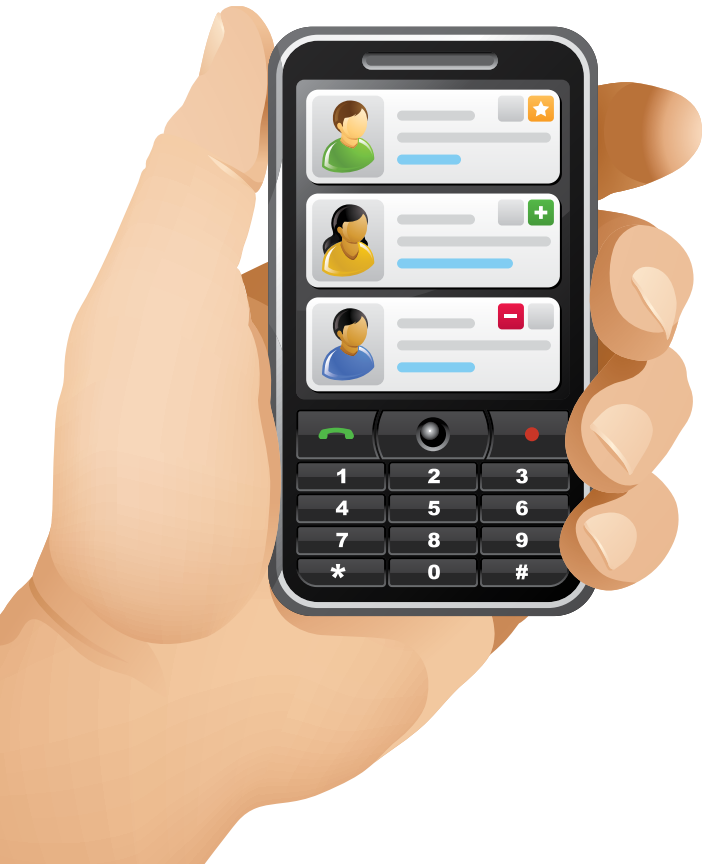
# Mobile Devices and Their Use in Healthcare: Medical Staff Policies and Procedures to Address the Pitfalls of Their Use

*Patrick D. Souter, Esquire*
*Looper Reed & McGraw PC*
*Dallas, TX*

The proliferation of mobile devices in our society has resulted in their use becoming commonplace in most every personal and professional venue. The universe of mobile devices includes such small units as iPhones, Android phones, and Blackberries to larger devices such as iPads, tablets, and notebooks. The healthcare industry is not immune from this phenomenon. It has been stated:

> A new generation of physicians is embracing mobile technology, not only with smartphones, but rapidly with tablet computers as well. A significant group of "Super Mobile" doctors now use both devices, and they are far more likely to use mobile technology in clinical settings to access decision tools, learn about new treatments, look up reference material, and handle patient information.[1]

The use of mobile devices by physicians is not insignificant. More than 80% of physicians own at least one device with approximately 25% utilizing at least two such devices in his or her practice.[2]




With this rapid advancement in communicating in the healthcare industry, it is imperative for healthcare facilities and their medical leadership to recognize not only the efficiencies but the dangers in their use. Healthcare facilities need to work with their medical staff leaders to implement safeguards to protect Protected Health Information (PHI) accessed and transmitted by mobile devices and to instill in those practitioners using mobile devices the necessity to be diligent in complying with such requirements.[3] Hospitals and their medical leaders may no longer have a mindset that policies and procedures for utilizing mobile devices may be established at a later time or when the mobile devices become more prevalent in the industry. Failure to ensure security and privacy under the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[4] along with similar legislation including those relating to confidentiality, may very well result in violations and penalties.[5] A lesson may be learned from the recent $1.5 million settlement reached between the U.S. Department of Health and Human Services Office for Civil Rights and a Massachusetts specialty hospital and its associated professional group resulting from an investigation tied back to a theft of a laptop computer.[6]

## HIPAA Security and Privacy Rules

Unfettered use of mobile devices is causing PHI and its security to become a greater concern for providers. The HIPAA Security Rule requires providers to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI.[7] In addition to the HIPAA Security Rule, the HIPAA Privacy Rule establishes standards for the protection of PHI and other personal information. This protection is done through appropriate safeguards to limit disclosure of PHI.[8] With the ever-increasing use of personal mobile devices for professional purposes, more and more providers are taking pictures, dictating, or sharing information, some of which constitutes PHI, through these devices. In these instances, it is possible to allow unauthorized access or give someone inadvertent access to such protected information.

Hospitals must have written policies in place addressing the privacy of health information and must ensure that unauthorized individuals cannot gain access to patient records.[9] Because the security and privacy concerns emanate from HIPAA, the implementation and enforcement of the policies and procedures should incorporate and further the HIPAA policies and procedures in place.

## How May Disclosure Occur With a Mobile Device?

When a practitioner utilizes a mobile device, it is not unusual that the last thing on their mind is the HIPAA implications of such use. The following are common instances where there may be an improper disclosure of PHI as a result of using a mobile device in developing, accessing, or retaining PHI:

- It is misplaced by the user or lost or stolen where another may have access to such information;

- The device is left unoccupied or viewable where an unauthorized person may have access to PHI;
- An unauthorized individual "hacks" into the device's database or through an unsecured transmission line;
- Transferring or placing information on a mobile device (or even flash drive) that is not encrypted so that the provider may have access to it on a trip or at home; or
- The mobile device is traded in and the memory is not completely deleted or "scrubbed."

It should be noted an unauthorized disclosure does not need to occur to implicate a violation of the HIPAA Security and Privacy Rules. These rules allow for there to be communications between healthcare providers or with patients as long they have established appropriate administrative, physician, and technical safeguards from a security and privacy standpoint to ensure the PHI remains confidential with integrity and security. Failure to do so is a violation itself.

## How to Ensure Protection When Utilizing Mobile Devices

With the different issues surrounding the use of mobile devices in the hospital environment, medical staff policies and procedures must be established to satisfy the HIPAA Security and Privacy Rules and related statutory and regulatory requirements, to protect against security breaches and unauthorized disclosure, and to establish best practices in recording and exchanging PHI. The following are suggested areas for hospitals to review and incorporate into their basic operations, as well as their medical staff policies or procedures:[10]

- It is mandatory that any information rising to the level of PHI be kept in a secured environment meeting the various requirements and safeguards previously mentioned. If PHI is received from another entity or person, there must be policies and procedures in place to establish how it must be immediately designated as PHI and for it to be secured. It is essential that hospitals conduct a thorough analysis of the risks to PHI security and privacy and continue such analysis on an ongoing basis. Additionally, providers should document the methodology chosen to address such risks and update them as necessary to keep up with ever-changing technology.
- Any transmissions of PHI using mobile devices must be through encrypted data transmission. Because most personal devices are not going to be as secure as those of the facility or medical practice, it is advisable to limit the use of personal mobile devices.
- Access by any mobile device must be restricted by password and sufficient other safeguards so the PHI may not be accessed by those who are not authorized to access it. There should be a requirement the passwords be changed on a set time basis


(i.e., every ninety days) and be of a sufficient security level to hinder attempts to obtain the password (i.e., require different types of letters, numbers, and symbols in the passwords). There should also be a policy and procedure on restricting access to passwords and how the passwords are maintained.

- So as to limit the theft or loss of a mobile device, require the mobile device when not in use to be in a locked area such as an office or workstation or in a locked briefcase if the person is off site. One should not leave a mobile device in an automobile or in a location where the device or the information may be viewable or easily stolen. An inventory of mobile devices maintained by the facility or medical practice should be maintained.
- PHI should not be downloaded to an unsecure site or location. It should not be printed off or otherwise obtained in hard copy from the mobile device that is left available in an unsecured area or where one may have access that does not require at a minimum a password to obtain such information or access. Providers need to have reasonable tracking measures in place to monitor and restrict downloading PHI to unsecured devices.
- If possible, limit use of the mobile devices used in the hospital setting for only patient care purposes and do not allow for accessing of databases that are not necessary. Policies and procedures in this regard will limit the likelihood of viruses, malware, and other types of intrusions into the mobile device or database that may compromise security and privacy or assist those who are attempting to "hack" into the system. In addition, it should be required that an antivirus software be maintained, kept up to date, and scheduled to run on a regular basis.

- If there is a breach of the system, a lost mobile device, or a known unauthorized disclosure due to the use of a mobile device, there must be policies and procedures on how it must be reported to the medical leadership, with mandatory action on such breach or disclosure to specific people in a particular format within a set time period.
- Disposal or reuse of mobile devices should be subject to specific standard policies and procedures. The information maintained on mobile devices should be removed and its memory "scrubbed" to ensure that no PHI is still on the device. If the mobile device is to be disposed of it should be done with an appropriate third party that disposes of such devices in a secure method.

Medical staff policies and procedures should address when, where, and how mobile devices should be used in accessing or discussing PHI. One should not openly discuss or obtain PHI on their mobile device when others may hear or see the information. There should also be policies and procedures regarding the access of PHI from a third party's mobile device or from an unsecured area.

In order to ensure that the medical staff understands the importance of patient privacy and the use of mobile devices, it is suggested that the hospital involve its medical leadership in establishing and developing its policies and procedures relating to privacy and confidentiality of medical records, including how mobile devices may or may not be used, as it applies to a particular facility. Although this may be easier in theory than it is in practice, the medical staff may be aware of instances where mobile devices may be used in practicing medicine, how such devices may make practice medicine more efficient and convenient, and how such devices may actually improve the quality of care received by a patient. It is also important to have ongoing education of the medical staff to keep them up to date on the current laws and regulations governing PHI, and the hospital's mobile device policies and procedures so that they clearly understand how mobile devices may be utilized in the workplace.

## Conclusion

The recommendations set forth above are generalized in nature. Specific policies and procedures should be created based upon use, facilities, and other issues that are unique to your organization. The U.S. Department of Health and Human Services has issued guidance on ensuring security when using mobile devices and protection of PHI in the process.[11] In addition to establishing policies and procedures, hospitals must train their medical staffs, as well as employees and contractors, on HIPAA privacy and security as they relate specifically to mobile devices if they are to be used. Adopting a mindset that a provider will develop these protections at a later time, or that a provider is simply "careful" with the use, transfer, and/or downloading of information is not acceptable. Such a choice may lead to inadvertent disclosures of PHI, which in turn is devastating to patients, as well as an assessment of significant financial penalties or sanctions against the facility.

---

1 Mary Modal, Tablets Set to Change Medical Practice, QuantiaMD (June 15, 2011), *available at* www.quantiamd.com/q-qcp/qrc_tablets.pdf.

2 *Id.*

3 According to 45 CFR § 103, "Protected Health Information," or what is commonly referred to as "PHI," is individually identifiable health information that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. *See* www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-103.pdf.

4 The Health Insurance Portability and Accountability Act of 1996, as amended (Public Law 104-191).

5 This includes legislation similar to HIPAA at the state level as well as various federal and state statutes related to confidentiality.

6 U.S. Department of Health and Human Services, Massachusetts provider settles HIPAA case for $1.5 million, Press Release dated September 17, 2012, *available at* www.hhs.gov/news/press/2012pres/09/20120917a.html.

7 45 CFR Part 160 and Subparts A and C of Part 164.

8 45 CFR Part 160 and Subparts A and E of Part 164.

9 42 C.F.R. § 482.24(b)(3), see also The Joint Commission Standards, IM.02.01.01.

10 Although medical staff policies are the focus of this article, the same principles and considerations would be equally applicable to other types of healthcare facilities and to independent professional groups as well.

11 U.S. Department of Health and Human Services, Security Rule Guidance Material, *available at* www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.