MOBILE DEVICES such as laptops and smartphones have become an increasing threat to the security of protected health information (PHI). Back in October, AHMC Healthcare Inc., based in Alhambra, California, reported the theft of two unencrypted laptops containing the PHI of approximately 729,000 patients. Reports of stolen laptops and other mobile devices containing PHI have not been uncommon in recent years. In fact, most breaches of PHI reported to the U.S. Department of Health and Human Services (HHS) are related to the theft or loss of mobile devices.

These types of reports are also not surprising given the rise in the use of mobile device technologies in the health care industry. Two recent studies have shown that health care professionals are increasingly using mobile devices such as smartphones and tablets for clinical purposes. A survey published in August 2013 by the Deloitte Center for Health Solutions found that more than 40% of physicians in the United States use mobile phones to access patient records, write prescriptions, and communicate with other health care professionals. BYOD Insights 2013, a survey conducted by a group of Cisco partner firms, points out that 88.6% of American workers in the health care industry use their personal smartphones for work purposes. Arguably the most troubling finding of the BYOD Insights 2013 study is that even the most basic protocols have not been adopted to ensure the security of these mobile devices. For example, nearly 60% of respondents in the health care industry reported that their smartphones are not password-protected, and more than half of respondents accessed unsecured or unknown Wi-Fi networks with their smartphones.

HIPAA Requirements for Securing Personal Health Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, the Privacy and Security Rules, as amended by The Health Information Technology for Economic and Clinical Health (HITECH) Act and the recent HIPAA Omnibus Final Rule, specify requirements for securing PHI. The HIPAA Security Rule specifically requires covered entities and their business associates to conduct periodic risk analyses of the potential risks and vulnerabilities to electronic PHI maintained on all their systems, including mobile devices, and to then adopt policies and procedures for addressing the threats and vulnerabilities.

“Failing to comply with HIPAA security requirements could result in civil penalties of up to $50,000 per violation and a maximum penalty of $1.5 million for all violations of an identical provision during a calendar year.”

Failing to comply with these security requirements could result in civil penalties of up to $50,000 per violation and a maximum penalty of $1.5 million for all violations of an identical provision during a calendar year. In at least two cases reported by HHS, the loss or theft of mobile devices resulted in settlements of over one million dollars.

Take the Necessary Steps to Secure Your Mobile Devices

In light of significant penalties under HIPAA for failing to adequately secure the confidentiality and integrity of electronic
PHI on mobile devices, health care organizations and their business associates should strongly consider the risks to mobile device security and adopt formal policies and procedures that adequately address these risks. The following minimum security measures should be considered carefully by any organization that wants to maintain data security over the mobile devices used by its workforce:

• Adopt access control policies that require authentication to access mobile devices, including use of complex passwords with a combination of letters and numbers. Some devices (such as Apple’s iPhone 5S) now offer biometric authentication measures to further secure mobile data from unauthorized access.

• Install or enable encryption on all mobile devices that store or access patient data or other sensitive information. Encryption is particularly important given that lost or stolen encrypted devices do not generally give rise to breach reporting requirements under HIPAA or most state breach reporting laws. Many newer mobile device models now offer full device encryption as a built-in option. This option should be enabled before the health care professional uses the device to access sensitive data.

• In addition to enabling encryption for data on the device, users must also be concerned about encryption for data that is transmitted via the device. Virtual Private Network (VPN) technology should be implemented before sending or receiving protected data via a mobile device. When a VPN is established between the device and a corporate network, all data transmitted between the two is encrypted to protect against interception by an unauthorized third party.

• Finally, SMS text messaging from mobile devices is inherently insecure. Unless text messaging of electronic PHI is expressly prohibited by organization policy, a secure HIPAA-compliant text messaging system should be implemented on all mobile devices with access to this sensitive data. A number of software solutions are available for securing text messaging in accordance with the requirements of the HIPAA Security Rule for electronic PHI.

• Enable or install firewalls to block unauthorized access. Some mobile operating systems have built-in firewalls that users can enable.

• Enable or install mobile security software to protect against viruses, malware, spyware and other malicious applications. A wide range of applications offer different levels of protection. Some features often found in security software applications include the ability to remotely wipe a device (in case of loss or theft); a remote alarm feature; and tracking capability via the device’s GPS system. It is important to keep mobile security software up-to-date.

• Disable or uninstall file-sharing software that can be used to access sensitive information or infect mobile devices with computer viruses or malware.

• Forensically wipe all stored health information before a mobile device is discarded or given to another user.

• Adopt a mobile device management (MDM) system that enforces security measures for all devices that connect to the organization’s network. A typical MDM system will register all mobile devices that seek to access data on the organization’s network; restrict access to non-compliant devices; manage security updates and access rights for user devices; roll-out approved applications; and provide IT administrators the ability to remotely wipe a device if it is lost or an employee is terminated.

Securing Mobile Devices—More Than Just Good Practice

Health care organizations and their business associates should remember that securing mobile devices that access or maintain electronic PHI is not just good practice, but is the law. The security measures described above are just a few that a health care organization should consider when adopting policies and procedures to protect PHI and other sensitive information on mobile devices. The Office of the National Coordinator for Health Information Technology (ONC), the federal organization within HHS charged with coordinating efforts to implement and use health information technology, provides additional advice on securing mobile devices on its website at www.healthIT.gov. Additionally, the National Institute of Standards and Technology (NIST) has published Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST Special Publication 800-124), which is intended to help organizations centrally manage and secure mobile devices. The publication can be found on the NIST website at www.nist.gov. The help you need to secure mobile devices is widely available, so take advantage of it!

Kevin Page, JD, is an associate at Waller Lansden, Dortch, and Davis, LLP, Nashville, Tenn., focusing on health care litigation; Phillips Hampton is founder and president of LogicForce Consulting, LLC, also in Nashville.