Securing Portable Devices

Save to myBoK

by **Angela K. Dinh** , MHA, RHIA

Reports of data breaches involving portable devices last year ran the gamut from oversight to theft: a college of medicine professor gave away a personal computer containing protected health information, including photos of his patients, to friends; a flash drive containing Social Security numbers was lost; a laptop that contained limited health information of 100,000 patients was stolen from a hospital employee's car.[1] The need for securing portable devices is not new. However, many legal and regulatory requirements have been in effect for years, even before the electronic boom began.

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data.[2] The final HIPAA privacy rule provides protection for all patient health information regardless of medium. And the final HIPAA security rule ensures protection of all electronic protected health information in transit and at rest.

Beyond legislation there are also requirements from regulating bodies. From Medicare (Conditions of Participation) to the Joint Commission, regulating bodies require that the confidentiality, integrity, and security of protected health information (PHI) be maintained.

According to the Centers for Medicare and Medicaid Services, physical device and media control is still among the top five most commonly violated security provisions.[3] This article identifies risks and provides key security tips for the protection and management of portable devices.

Identifying Risks

A key component to securing portable devices and the sensitive information they may possess or transmit is identifying and analyzing potential threats and risks within the portable environment. Associated risks can exist in multiple schemes (i.e., a theft versus a virus versus a hacker) and thus be easily overlooked. Core risks to evaluate in the use of portable devices include:

- **Physical security.** One of the major risks of any portable device is the device itself. Devices can be damaged, lost, or stolen. Information contained within the device may be irretrievable and irreplaceable.
- **Internal security.** Malware and spyware can be detrimental to a device, its operating system, and the data stored within it. Viruses, worms, and other malware can target mobile devices, causing them to crash and lose information. E-mail viruses are just as malicious to portable devices as they are to standard desktop computers.
- **Loss of data or exposure of sensitive information.** Data loss and exposed sensitive information can cost time and money. Organizations should consider the costs of replacing the devices and their security measures as well as any actions taken on behalf of the victims involved. Exposure of sensitive data can lead to identity theft and medical identity theft, which is one of the fastest growing white collar crimes in the US and affects millions of Americans each year.[4]

Applying Protection

Once a portable device leaves the security of the organization, its safety lies with the user and the security mechanisms implemented within its system. There is not much that can be done to control the environment, but there are ways to control the devices. And while no method is 100 percent effective, multiple methods used together can significantly reduce risks.

- **Inventory.** Before anything goes anywhere, there should be a complete documented list of what portable devices belong to the organization and have permission to access the network or contain electronic PHI. Each device should be tagged with an identity marker (e.g., number) used to track the device.
- **Policies and procedures** must identify and document the responsibilities of staff related to portable devices. Organizations should adopt protocols for incidence response and define consequences. They also should identify who

has permission to use and remove portable devices from the premises. Policies and procedures should be updated and maintained on a regular basis to ensure effectiveness.

- **Training.** All staff permitted to use portable devices should be trained on expectations and liabilities. Each employee should understand clearly the organization's policies.
- **Check-in/check-out process.** Each device should be signed in and out by the user so the location of the device is documented at all times. Even if a device belongs to a specific employee for the duration of employment, the device should be considered checked out to that individual. Before check out, the device should be backed up as a safety precaution. Upon check-in, it should be backed up again, scanned for malware and inspected to ensure that it is in the same condition as it was when it left the facility. For those devices checked out to an individual for the duration of employment, the device should be routinely backed up and maintained for updates, malware scans, and other work for optimal safety and function of the device.
- **Encryption.** There are many types of encryption available in the industry. Organizations should research all alternatives to find the best encryption software for their portable devices. Some may find application-layered encryption or file encryption to be enough. However, organizations should encrypt the entire device with a second method. Using a supplemental method enhances security.
- **Authentication.** Only the intended user should be able to access the device. Authentication such as a password is crucial. Passwords should be hard to guess and include numbers, letters, and symbols. Multifactor authentication increases security. Including the use of a password with a fingerprint or swipe key (or all three) will provide added protection to the device.
- **Anti-virus software and firewalls.** Like desktops, portable devices require protection against viruses and spyware. Anti-virus and anti-spyware software is a necessity. Firewalls preventing unauthorized access should also be used as well.
- **Data use and storage.** Organizations may take the added precaution of restricting storage of sensitive information to the network. Users off-site access the network through a secure connection rather than working with the data on the device itself. In the event a device is lost, stolen, or damaged, no sensitive information is disclosed to the wrong party.

From laptops to smartphones, CDs to flash drives, anything that can store PHI or connect to the organization's network should share the same security measures and be subject to the same policies and procedures. A policy plan for portable devices is a unique imperative, and it must be treated as such for the safety of all electronic PHI.

Organizations must clearly document these policies and procedures. Staff must be trained and educated on their responsibilities, and accountability must be clear. All devices must be equipped with proper security measures. Security is not the responsibility or achievement of one person or department, but it is the collaboration of many.

Notes

1. Privacy Rights Clearinghouse. "A Chronology of Data Breaches." Available online at www. privacyrights.org.
2. Quinsey, Carol Ann. "Portable Computer Security." Updated June 2003. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.
3. Centers for Medicare and Medicaid Services. "CMS Enforcement Statistics Report." September 2008. Available online at www.cms.hhs.gov/Enforcement/Downloads/EnforcementData0908.pdf.
4. AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79, no. 7 (July 2008): 63–69.

Angela K. Dinh (angela.dinh@ahima.org) is a professional practice resources manager at AHIMA.

Article citation:
Dinh, Angela K.. "Securing Portable Devices" *Journal of AHIMA* 80, no.1 (January 2009): 56-57.

Driving the Power of Knowledge