Portable Computer Security (2003 update)

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

Editor's note: The following information supplants information contained in the practice brief "Portable Computer Security" published in the October 2000 Journal of AHIMA.

Background

Portable computers can be efficient and effective in documenting patient care and treatment, particularly when healthcare professionals move between nursing units, healthcare facilities, or patient homes. Not only can they save users time, portable computers can facilitate the collection of more complete and accurate information. Unlike networked desktop computers, however, portable computers are easily stolen and thus pose increased risks to the security of patient health information.

Legal and Regulatory Requirements

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that health information be protected against threats to security, integrity, and unauthorized use.

The final privacy standards (45 CFR, Parts 160 and 164) were set forth to protect the privacy of individually identifiable health information maintained or transmitted electronically in connection with certain administrative and financial transactions.

The final security rule (45 CFR Parts 160, 162, and 164) covers electronic protected health information (ePHI), which is the electronic subset of protected health information (PHI) addressed in the privacy rule.

Section 164.306 of the security rule covers some general rules for all covered entities, including general requirements and crossover requirements with the privacy standards. Specifically, this section covers four things that must be done under the security rule:

- ensure the confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits
- protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- protect against any reasonably anticipated uses or disclosures of such information that are not permitted under the privacy subpart
- ensure compliance with the security subpart by the entity's work force

This section describes implementation specifications for each of the security standards as either "required" or "addressable." If a standard is required, covered entities must implement the implementation specification. If a standard is addressable, the covered entity must assess whether the implementation specification is reasonable in their environment and document the results of their assessment. If it is found to be reasonable and appropriate, the covered entity must implement. (It is permissible to implement an alternative measure that is determined to be more reasonable and appropriate.) If the assessment does not conclude the implementation specification to be reasonable or appropriate, then the covered entity does is not required to implement.

Several references in 164.310 are made specifically to workstations. This section requires a covered entity to "implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI." It further requires that the entity "implement physical safeguard for all workstations that access ePHI to restrict access to authorized users" and requires the implementation of "policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility and the movement of these items within the facility."

- disposal (required): the entity must "implement policies and procedures to address the final disposition of ePHI and/or the hardware or electronic media on which it is stored"
- media re-use (required): likewise, the entity must "implement procedures for removal of ePHI from electronic media before the media are made available for re-use"
- accountability (addressable): the entity must "maintain a record of the movements of hardware and electronic media and any person responsible therefore"
- data backup and storage (addressable): the entity must "create a retrievable, exact copy of ePHI, when needed, before movement of equipment"

Covered entities must account for the fact that many workstations are small and easy to move. As a result, they may be used almost anywhere; for instance, many employees work from home. As with the privacy rule, an entity will have to consider the security questions surrounding such practices.[1]

Section 164.312 says that a covered entity must "implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the "administrative safeguards" section (164.308). To do this, a covered entity must initiate four implementation specifications:

- unique user identification (required): the entity must "assign a unique name and/or number for identifying and tracking user identity"
- emergency access procedure (required): an entity must "establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency"
- automatic logoff (addressable): the entity must "implement electronic procedures that terminate an electronic session after a predetermined time of inactivity"
- encryption and decryption (addressable): the entity must "implement a mechanism to encrypt and decrypt ePHI" as needed

While the requirements that mention encryption in this section and elsewhere are short, a longer discussion in the preamble also contains important information. HHS is not suggesting encryption always must be done, but each aspect of ePHI should be reviewed to determine if encryption makes sense. Decision makers should take into account that encryption is rapidly changing.[2]

The Medicare Conditions of Participation for healthcare facilities also address information security with the following requirements:

- hospitals: "The hospital must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records."[3]
- home health agencies: "Clinical record information is safeguarded against loss or unauthorized use."[4]
- state and long-term care: "The resident has the right to personal privacy and confidentiality of his or her personal and clinical records."[5]
- comprehensive outpatient rehabilitation facilities: "The facility must safeguard clinical record information against loss, destruction, or unauthorized use."[6]
- critical access hospitals: "The facility maintains the confidentiality of record information against loss, destruction, or unauthorized use."[7]
- outpatient physical therapy services furnished by physical therapists in independent practice: "Clinical record information is recognized as confidential and is safeguarded against loss, destruction, or unauthorized use."[8]

The Privacy Act of 1974 mandates that federal information systems must protect the confidentiality of individually identifiable data. Section 5 U.S.C. 552a (e) (10) of the act is very clear: federal systems must "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[9]

The Code of Federal Regulations relative to Alcohol and Drug Abuse, 42 CFR, Chapter I, Part 2, Section 2.1, states that records of the identity, diagnosis, prognosis, or treatment of any patient that are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall be confidential and disclosed only for the purposes and under the circumstances expressly authorized.

In addition, individual states may have laws or regulations that require health information to be protected against threats to security, integrity, and unauthorized use.

Accreditation Standards

The Joint Commission on Accreditation of Healthcare Organizations' hospital, ambulatory care, and long-term care standard IM.2 reads "Confidentiality, security, and integrity of data and information are maintained."

Recommendations

The risks of portable computer and associated information theft can be minimized when healthcare facilities:

- improve access and physical controls
- provide employees with theft awareness instruction
- make small investments in computer accessories

In terms of establishing appropriate controls, healthcare facilities should:

- establish written policies and procedures covering the loan and use of portable computers
- purge user data from returned portable computers prior to assigning the same portable computer to the next user
- require all borrowers to sign a copy of the policy statement or guidelines for portable computers
- avoid maintaining patient health information on portable computers. Instead, store the information on the healthcare facility's network so the information can be backed up and maintained more securely. When network storage is not possible, maintain the patient information on disk(s), storing and transporting the disks separately from the computer carrying case, or encrypt the information to protect it from unauthorized access should the computer be stolen
- require written authorization by the HIM director when portable computers are to be used to collect and/or maintain patient health information
- limit use of the assigned portable computer to the employee
- hold the computer borrower responsible and accountable for the safety and security of the assigned equipment and information
- maintain a current list of portable computer users and borrowers, assigned equipment serial numbers, and software
- audit policies, procedures, and assigned equipment and software lists regularly
- perform loss investigations on all stolen equipment
- secure portable computers, offices, and meeting rooms when equipment is left unattended
- when purchasing portable computers, consider those with local repair facilities to avoid potential theft during shipment to or from the factory when computers are sent for repair
- require the use of strong passwords of at least seven to eight characters, including alphanumeric and special characters
- In terms of theft awareness and instruction, healthcare facilities should:
- require that employees be familiar with the facility's policies and procedures relative to portable computer use prior to being assigned such equipment
- require that employees be familiar with the facility's policies and procedures relative to confidentiality of patient health information
- educate employees about the potential risks caused by computer or information theft or loss
- provide employees with computer and data theft precaution and deterrent information. Examples might include instructions to:
    - avoid using portable computers where they can be easily stolen
    - transport portable computers in a car's trunk rather than on a seat, thereby keeping it hidden
    - carry the computer in something other than a readily identifiable computer carrying case
    - carry disks separately from the case containing the portable computer

- when possible, place a portable computer on an airport conveyor after the preceding individual has cleared the metal detector
- place unattended portable computers in room safes when leaving a hotel room. (Some hotel room safes include an AC adapter so that the computer can be recharged while locked away.)
- lock the room or place the computer in a laptop depository when leaving portable computers in an unattended meeting room. (A laptop depository is a portable safe in which computers can be placed. An alarm will sound if the depository is moved after it is closed.)
- avoid setting a portable computer down in a public place
- avoid accessing patient identifiable health information where it might be seen by individuals without a legitimate need to know

In terms of making investments in computer accessories that will minimize the risk of theft, facilities should:

- provide employees with the best accessories available to protect their portable computers and require use of these devices. Examples include:
    - carrying cases that do not appear to contain computers
    - cables with locks that hook to desks or tables and that once removed do not allow a thief to turn the computer on
    - lock down enclosures, proximity alarms, and software programs that instruct computers to "phone home" to report their location
- install and use appropriate password, security, and encryption programs
- use an anti-theft plaque or etching tool to engrave the company name/ID on all portable computers (Some anti-theft plaques contain a metallic bar code and registration number. If a thief tries to pry off the plaque, the computer casing will be damaged, decreasing the resale value. If the thief succeeds in removing the plaque, the computer will still bear the imprint of the words "stolen property" on its shell.)

Updated by

Carol Ann Quinsey, RHIA

Originally prepared by Gwen Hughes, RHIA

Notes

1. AHIMA's Policy and Government Relations Team. "Final Rule for HIPAA Security Standards," February 2003. Available in the FORE Library: HIM Body of Knowledge at www.ahima.org.

2. Ibid.

3. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for Hospitals." *Code of Federal Regulations*, 1999. 42 CFR Ch. IV, Part 482.24.

4. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for Home Health Agencies." *Code of Federal Regulations*, 42 CFR Ch. IV, Part 484.48.

5. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for States and Long-Term Care Facilities." *Code of Federal Regulations*, 42 CFR, Ch. IV, Part 483.10.

6. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for Specialized Providers." *Code of Federal Regulations*, 1998. 42 CFR Ch. IV, Part 485.60.

7. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for Specialized Providers." *Code of Federal Regulations*, 1998. 42 CFR Ch. IV, Part 485.638.

8. Health Care Financing Administration, Department of Health and Human Services. "Medicare Conditions of Participation for Specialized Services Furnished by Suppliers." *Code of Federal Regulations*, 1998. 42 CFR, Ch. IV, Part 486.161.

9. Health Care Financing Administration. "HCFA Internet Security Policy." November 24, 1998. (www.cms.hhs.gov/it/security/docs/internet_policy.pdf).

References

Briggs, Bill, ed. *Comprehensive Guide to Electronic Health Records*. New York, NY: Faulker and Gray, Inc., 2000.

Joint Commission on Accreditation of Healthcare Organizations. *2002-2003 Comprehensive Accreditation Manual for Ambulatory Care*. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations, 2003.

Joint Commission on Accreditation of Healthcare Organizations. *2003 Comprehensive Accreditation Manual for Hospitals: The Official Handbook*. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations, 2003.

Joint Commission on Accreditation of Healthcare Organizations. *2002-2003 Comprehensive Accreditation Manual for Long Term Care*. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organization, 2003.

"Standards for Privacy of Individually Identifiable Health Information: Final Rule." (45 CFR, Parts 160 and 164) (August 14, 2002). Available at www.hhs.gov/ocr/hipaa/whatsnew.html

"Health Insurance Reform: Security Standards; Final Rule (45 CFR Parts 160, 162, and 164). (February 20, 2003). Available at www.hhs.gov/ocr/hipaa/whatsnew.html

Article citation:
Quinsey, Carol Ann. "Portable Computer Security." (AHIMA Practice Brief, Updated June 2003).