Portable Computer Security (2000)

Save to myBoK

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

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, but portable computers can facilitate the collection of more complete and accurate information. The danger of portable computer theft, however, poses increased risks to the security of patient health information when compared to networked desktop computers.

Legal and Regulatory Requirements

The Health Insurance Portability and Accountability Act of 1996 contains requirements that health information be protected against threats to security, integrity, and unauthorized use. A proposed rule (45 CFR, Parts 160-164) published November 3, 1999, proposes standards to protect the privacy of individually identifiable health information maintained or transmitted electronically in connection with certain administrative and financial transactions.

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."[1]
- home health agencies: "Clinical record information is safeguarded against loss or unauthorized use."[2]
- state and long-term care: "The resident has the right to personal privacy and confidentiality of his or her personal and clinical records."[3]
- comprehensive outpatient rehabilitation facilities: "The facility must safeguard clinical record information against loss, destruction, or unauthorized use."[4]
- critical access hospitals: " The facility must safeguard the clinical information against loss, destruction, or unauthorized use."[5]
- 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."[6]

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."[7]

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 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 borrowers, assigned equipment serial numbers, and software
- audit policies, procedures, and assigned equipment and software lists
- 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

In terms of theft awareness and instruction, healthcare facilities should:

- require that employees are 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 near an exterior window or door 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
    - place a portable computer on an airport conveyor belt only when 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
    - lockdown 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 (The anti-theft plaque contains 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.)

Prepared by

Gwen Hughes, RHIA
Professional Practice Division, AHIMA

Notes

1. Medicare Conditions of Participation for Hospitals, 42 CFR Ch. IV, Part 482.24.
2. Medicare Conditions of Participation for Home Health Agencies, 42 CFR Ch. IV, Part 484.48.
3. Medicare Conditions of Participation for States and Long-Term Care Facilities, 42 CFR, Ch. IV, Part 483.10.

4. Medicare Conditions of Participation for Specialized Providers, Code of Federal Regulations, 1998. 42 CFR Ch. IV, Part 485.60.
5. Conditions of Participation for Specialized Providers, Code of Federal Regulations, 1998. 42 CFR Ch. IV, 485.638.
6. Medicare Conditions of Participation for Specialized Services Furnished by Suppliers, 1998. 42 CFR, Ch. IV, Part 486.161.
7. Health Care Financing Administration. "HCFA Internet Security Policy." November 24, 1998. Available at www.hcfa.gov/security/isecplcy.htm.

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. *1999 Comprehensive Accreditation Manual for Ambulatory Care*. Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations, 1998.

Joint Commission on Accreditation of Healthcare Organizations. *Comprehensive Accreditation Manual for Hospitals: The Official Handbook; Refreshed Core Manual.* Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organizations, 1999.

Joint Commission on Accreditation of Healthcare Organizations. 1998-1999 *Comprehensive Accreditation Manual for Long Term Care.* Oakbrook Terrace, IL: Joint Commission on Accreditation of Healthcare Organization, 1998.

Acknowledgments

Jill Callahan Dennis, JD, RHIA
Michelle Dougherty, RHIA
Kelly McLendon, RHIA
Monica Pappas, RHIA
Harry Rhodes, MBA, RHIA
Ralph Whiteaker

Issued October 2000
