Reasonable Approach to Physical Security (HIPAA on the Job)

Save to myBoK

by Margret Amatayakul, RHIA, FHIMSS

Of all the components of HIPAA, physical security may be the most challenging and costly to address. After all, how do you move walls or create doors in open space? This article will show how physical security can be flexible, scalable, and reasonable for healthcare facilities.

What Is Physical Security?

HIPAA's proposed security rule defines physical safeguards as including assigned security responsibility, media controls, physical access controls, workstation location and use, and security awareness training. Although this may seem to be an eclectic mix of requirements, the best practice ideas and cautionary tales below will demonstrate how these items relate.

Who Will Be Responsible?

Many organizations have not yet designated an information security official, partly because the rule has not been finalized, but also because many are trying to decide to whom that responsibility should be assigned. Candidates include the physical plant's security officer, safety officer, information systems analyst, HIM professional, chief information officer, and many others. In short, there is no one "right" person, and in fact, the right person is likely to vary from organization to organization and even over time within an organization.

As you consider candidates, ask who most people turn to when concerned about security. The answer is probably the facility's current security officer. Security officers are highly trained in security awareness and gathering evidence, which makes them excellent in identifying potential incidents and their causes and avoiding future incidents. Security personnel are also upgrading their training in electronic security systems, including thwarting computer hackers and managing physical barriers to wireless data transmission.

Regardless of the choice for information security official, he or she should not work in a vacuum. A team of individuals with a variety of knowledge and skills should work together with the information security official as point person.

A Closer Look at Media Controls

The HIPAA requirements for **managing media controls** include access controls, accountability, back-up, storage, and disposal.

Access controls on media can refer to many things. The proposed security rule does not provide much detail, but many have interpreted this to include protecting fax transmissions, verifying who has print and local save capability on computers, and determining who has access to file rooms, data centers, back-up tape vaults, and even portable devices (such as personal computers and personal digital assistants).1 Many facilities are removing floppy, CD, and even hard drives from workstations. When acquiring new workstations, facilities are buying "thin clients" for most users, which are essentially stripped-down workstations that serve as "dumb terminals."

Accountability is defined by HIPAA as the "property that ensures that the actions of an entity can be traced uniquely to that entity." In its purest form, accountability would require biometric identification for physical access. Today, however, entities can improve signage to provide greater awareness of confidentiality needs, adopt sign-in sheets for visitors to non-public areas, escort visitors, supervise maintenance personnel, keep logs of when locks are changed, and use swipe cards to track personnel entrance and exit.

The physical security section also highlights the need for **safeguarding back-ups.** The healthcare industry has never considered backing up its paper-based medical records, although some portions are stored in electronic form and copies of some documents that are routinely distributed to physician offices may not be accessible in the event of a disaster. Extra environmental precautions are required by the Joint Commission on Accreditation of Healthcare Organizations and other licensing and accrediting agencies, although satellite file areas and warehouses for older records do not always get the same attention. It is not uncommon for these file areas to be used for numerous other storage and functional needs, including housing utility meters accessible directly by workers and storage for everything from old beds to food.

Back-up details for electronic information should be spelled out in a back-up plan (referenced in the administrative section of the security rule). These plans should identify what is backed up (i.e., protected health information [PHI], the application software, other information), the frequency of the back-up process, on what media the back-ups are stored, how they are tested, and where they are stored.

PHI, obviously, should be backed up. In small offices or for departmental systems, however, it is important to ensure that any components of the operating system that change as data are processed are also backed up. A copy of the application software may be available through the vendor, but not if the software has been customized by the provider.

It is prudent to back up PHI at least daily and essential applications should have redundant or mirrored systems that perform continuous back-up. A frequent error is the lack of routine back-up system testing. Error-check programs can ensure the integrity of the back-up, but full restoration testing should also be performed. Finally, it is not uncommon to find that back-ups for stand-alone systems are often stored right beside the system itself. While this is adequate when the goal is only to protect against system failure, the systems can be easily lost or stolen and do not, therefore, safeguard confidentiality.

In addition to storing back-ups, all PHI storage is included in the physical security requirement. Healthcare facilities are cautioned that the weakest link in securing health information is often not in the file area, data center, or even warehouse, but in storage of shadow records, stand-alone servers, individual databases, copies, preliminary reports, drafts, worksheets, and other documents that are not a part of the official medical record but still contain health information.

Safe disposal is also a critical step in the physical security process. Many organizations have begun using a shredder service. This is a good practice, but only if everyone follows the shredding program faithfully. There may be confusion about the containers for PHI and for recycling.

Because most paper discarded in a healthcare facility contains individually identifiable health information, it may be easier to simply focus on shredding everything but Styrofoam, cans, and bottles. Check with the shredding service vendor to determine what other materials can be shredded, such as labels, IV bags, and plastic medicine vials. (Incineration, in which steam from the process is recycled, is an alternative to shredding.)

Finally, all steps in the shredding process need to be protected. Overflowing shred boxes, unsecured shred bins, and bags of material waiting to be shredded need as much security as the shredding itself.

How to Control Physical Access

Physical access controls refer to having appropriate safeguards wherever PHI may be used or stored. **Locked doors** are an obvious solution. Most healthcare facilities have very open campuses in which multiple external doors are locked only at night. Some facilities are looking to the hotel industry or other more security-conscious businesses as models for maintaining employee entrances, guard services, camera monitoring of entrances, and more.

Internal doors also require scrutiny. Evaluate the HIM department's proximity to a photocopier, fax, public areas, or even other departments. Security can be compromised by a back door to a file room or space shared with another department.

In one facility, the HIM department shared space with a social services department that reported to a different executive and had very different policies for allowing visitors. Such visitors included family members and friends of staff and posed a vulnerability for the HIM department.

Or, recall the case in a Florida hospital in which an HIM staff member's child changed HIV test results that were mailed to patients and one patient who received an altered result attempted suicide.

Other areas to watch are entrances with the physicians' dictation area, unlocked file cabinets of old explanation of benefits forms in the reception area of the billing office, shadow records stored near an elevator and out of a staff member's line of sight, or any other potential physical access vulnerabilities.

Sometimes we may be so familiar with the current physical plan that it is difficult to recognize that greater physical access controls are needed. One way to see the forest for the trees is to tour the facility while checking each door for public access, standard lock, and secure lock requirements.

Although **termination procedures** are included in the security rule's administrative requirements, facilities should keep in mind that voluntary terminations are not always "friendly," and that such employees who know about lax security practices pose a threat. Conduct a physical inventory of doors to determine how frequently locks are changed and confirm that they are always changed whenever an employee leaves.

HIPAA's View of Workstation Use and Location

Workstations should be positioned away from public view or screened so that casual observers cannot view the contents displayed on a monitor. **Workstation location** could also be interpreted in light of the privacy rule's requirements for confidential communications and include any location where "work" takes place and working papers are in public view, such as sign-in sheets, schedules, white boards, chart racks and chart boxes, and even locations where shift reports or rounds are conducted. Reexamining workstation location may lead to installing staff elevators where patients can be transported away from visitors and protection such as walls or partitions between examining rooms or bed rooms.

The privacy rule's guidelines have provided information that recognizes that reasonable approaches to such work location issues need to be taken. A hospital cannot be expected to convert to all private rooms. Communications should not be impeded by requiring rounds to be held in a conference room away from access by nursing personnel. But **awareness of one's surroundings** should be considered when PHI is used or disclosed in the course of treatment, payment, and operations.

Some good sources to consider as models for all areas of the healthcare facility include the added protections afforded psychiatric services, and more recently, obstetric and newborn areas. Attention to safeguarding information affects not only the confidentiality of health information but patient care as well. For example, a pediatrician conducting rounds stopped in front of a preteen patient's room. The pediatrician had not finished discussing the previous patient's case and proceeded to describe the gravity of the illness and some alternative surgical approaches. Because the door to the preteen patient's room was ajar, the entire conversation was overheard, personalized, and caused the young patient to become very distraught. The situation could have been avoided first by completing the discussion away from the different patient and, second, by simply closing the door.

Workstation use refers to procedures for functions associated with one's workstation. The proposed security rule uses the example of instructing users to always log off a workstation when leaving it unattended. While this is important and should be done any time the user will be away for an extended period of time or a different user will be using the workstation, the busy environment of most healthcare facilities may make this difficult to achieve. Instead, it may be appropriate to implement automatic log off (also required under HIPAA) set to a relatively short period of time.

Some other functions to consider include the access workstations afford to the network, back office applications, and the Internet. If employees have Internet access, proper use of the Internet should be included in the instructions for proper workstation use. **Create a policy** on introducing foreign software on a workstation, downloading executable files, uploading documents/creating attachments, and which Internet sites may be banned if there are no site or keyword filters at the firewall. One of the purposes of awareness training and a role for the information security official may be to randomly check computers for downloaded screensavers as a clue that employees may be using the Internet improperly.

Training: Make It Creative

Finally, physical security is very much about being aware of one's surroundings. Who can overhear conversations about PHI? Who can see identifying data? What information is accessible to those without clearance?

Security awareness training needs to be simple, random, targeted, and varied. It should fit the culture of the organization and the needs of current security issues. Signage reminding employees that "the walls have ears" may be ineffective if not varied over time. In fact, most organizations find such signs unsightly and prohibit them. More subtle, but equally powerful, opportunities exist. Creativity is required in building a security campaign that is effective and efficient.

For more information on security and privacy education and training, see "HIPAA on the Job: What's Your HIPAA ETA?" in the January 2002 *Journal of AHIMA* (vol. 73, no. 1) or online at www.ahima.org.

Note

1. AHIMA's practice brief, "Facsimile Transmission of Health Information (Updated)" is an excellent resource for creating a fax protection policy. It can be found in the June 2001 *Journal of AHIMA* (vol. 72, no. 6) or online in the FORE Library: HIM Body of Knowledge.

Margret Amatayakul *(margret cpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "A Reasonable Approach to Physical Security (HIPAA on the Job series)." *Journal of AHIMA* 73, no.4 (2002): 16A-C.