Safeguards for Remote Access

by the AHIMA Privacy and Security Practice Council

Working from home has become a common practice as organizations try to maximize the number of productive work hours in a day. A plethora of new portable devices and Web-based technology enables this option by providing off-site access to work-based applications and facilitating the transport of large amounts of data with a minimum of resources. An entire master patient index can be stored on a flash drive no bigger than a pack of gum.

HIPAA privacy and security rules do not prohibit remote access, but they do require that organizations implement appropriate safeguards to ensure the privacy and security of protected health information (PHI).

Reasons for Remote Access

When healthcare staff work remotely, it often includes the PHI of patients or health plan members. This is usually driven by a combination of factors, including:

- The clinical imperative for instant access to PHI
- The need to automate the traditional physician practice of tracking current patients on 3x5" index cards
- The need to address insufficient manpower to handle critical functions, including coding and transcription, by offering flexible options
- A desire for flexible work arrangements to enhance recruitment efforts, job satisfaction, and staff retention and to address needs of working parents
- Expansion of health systems over widespread geography
- Multiple-site research projects
- The disappearance of international borders and the emergence of an international academic research community
- The new emphasis on the portable patient health record
- Availability of new technology that facilitates wireless dictation and billing[1]
- The competitive cost of off-shore labor

Whereas in earlier times the number and types of work force members who worked remotely were limited, the variety of roles that access PHI remotely now runs the gamut and includes administrators, billers, coders and validators, consultants, IT staff, providers, physicians, data analysts, researchers, transcriptionists, and vendors.

The Expanding Technology World

Formerly, documentation taken off-site was limited to that easily copied via photocopy machines, carbon and NCR paper, microfiche, et cetera. New technology has increased the options and expanded the range of material requiring protection. Safeguards are necessary for virtually every type of medium, data, and image created in the healthcare environment, including:

1. Ancillary test results
2. Clinical and research databases
3. Dictated reports
4. Financial data
5. Organizational data
6. Medical records
7. Picture archiving and communication systems
8. Pathology slides
9. Proprietary information
10. Research data

The format of the data and the media on which they are stored is evolving and can be as varied as the data. As the technology evolves, even greater access will undoubtedly follow suit. Technologies include iPods, local area networks, wide area networks, local hard drives, laptops, Palm Pilots, Blackberries, thumb drives, smart phones, scanned images, virtual networks, and voice over technology, which could conceivably include automated messages containing personal health information left on a patient's answering machine.

Safeguarding New Technology

Because of these new and developing remote work options and applications, HIPAA requires that organizations must develop mechanisms for addressing new risks.[2] Such risks include:

- Theft of unencrypted portable devices
- Increase in identity theft
- Poor security practices at home that might lead to inappropriate access by family members (e.g., failure to log out, improper disposition of confidential waste, unauthorized printing and saving of PHI)
- Unauthorized downloading of electronic PHI
- Inadequate virus protection
- Data corruption
- System hacking
- Disasters at remote sites

While it is impossible to eradicate all risks, some control can be attained by taking prudent precautions and establishing safeguards. Technological and administrative (operational) solutions are available, but each is attended by various degrees of risk or annoyance.[3,4]

Technological safeguards that are independent of policies and procedures are preferable. To be most effective, they should either be supported by the organization from the moment of installation or be a prerequisite to granting permission for remote access. They may include:

- Establishing a virtual network with controlled access developed to the organization's specifications. This approach is best because the work product never leaves the site. A small risk exists for unauthorized screen scraping (when a computer program extracts data from the display output of another program) and creative data downloads. There are added set-up and maintenance costs with this option.
- Maintenance of encryption, password management, virus protection, and patch updates on portable and home devices. These activities protect the application, the device, the network, and the data. However, such safeguards are cumbersome to operate and interfere with the user's work, thus encouraging work-arounds. Cutting-edge technology with safeguards invisible to the user may reduce work-arounds but increase cost.[5]

In the absence of technological safeguards, compliance may be achieved through administrative safeguards. They include policies, procedures, and work force education, training, and awareness. Examples include:

- Requiring specialized remote access user agreements delineating obligation to adhere to administrative, technical, and physical safeguards designed to protect the privacy and security of electronic PHI.
- Prohibiting taking work off-site. Work product that does not leave the premises is protected by whatever security features are installed on-site and in a well-functioning, controllable environment. However, emergencies must be handled by on-site staff or await reinforcements. Unplanned events ranging from an employee's minor illness to a disaster of major proportions can bring part or all of an operation to a grinding halt.
- Restricting off-site work to a controlled virtual network.
- Granting permission to work off-site at the organization's request and need only. With such a policy the organization owns the hardware and bears the responsibility to support such safeguards as password and content management protections, antivirus software, and spyware detection. It saves the cost of on-site office space, while enabling secure, controlled access from home. The downside is the cost of servicing both the hardware and software and the inability to monitor unsupervised work. Such permission should be restricted to self-motivated and independent workers and work types that can be objectively monitored both for quality and output.

- Requiring anyone who takes work off-site on his or her own initiative to assume responsibility for its security and maintain virus protection, patch updates, dispose of confidential waste, and log out. If remote access is for user convenience, strict policies must be developed and enforced including requiring adequate security in the off-site environment.

Whether the solution selected is technological, administrative, or a combination, a comprehensive audit plan is vital. It could be a high-tech, automated solution that can track the presence and adequacy of all safeguards on each device with a built-in alarm system. It could also be a well-designed manual review ensuring use of encryption and passwords on each device and ensuring that permissions granting remote access rights are reviewed and renewed on a predetermined basis. Regardless of choice, the method must be able to monitor or track quality and quantity of work and compliance with organizational security policies.

Healthcare organizations operate in an ever-changing environment that encourages and sometimes demands that staff work remotely. Unfortunately, organizations are exposed to a criminal element that has learned the value of both hardware and the data that reside on it.

Theft may be driven by the cash value of the hardware or may be part of a complex scheme orchestrated by organized crime to co-opt large numbers of patient identities. The target could be Social Security numbers, insurance IDs, insurance information, or any other data with market value. Regardless of the actual target, it is incumbent upon healthcare organizations to develop safeguards for data allowed off-site, whether these safeguards are technological or administrative in nature.

Notes

1. Cross, MargartAnn. “PDAs Chase Workflow Improvements.” *Health Data Management*, May 2006: 61–62.
2. Centers for Medicare and Medicaid Services. “HIPAA Security Guidance.” Available online at www.cms.hhs.gov/SecurityStandard.
3. Ibid.
4. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 164.306(a).
5. McDougall, Paul. “Scrambling Data Is Easier than Stopping Its Theft.” *Information Week*, September 19, 2006: 27.

*Lead authors: **Aviva Halpert**, MA, RHIA, CHP, CHS, is chief HIPAA officer at Mount Sinai Medical Center (aviva.halpert@mountsinai.org). **Nancy Davis**, MS, RHIA, is director of privacy at Ministry Health Care and cochair of the AHIMA 2007 Privacy and Security Practice Council. **Chrisann Lemery**, MS, RHIA, of WEA Trust Insurance is cochair of the Privacy and Security Practice Council. **Beth Hjort**, RHIA, CHPS, is professional practice manager at AHIMA.*

Article citation:
AHIMA Privacy and Security Practice Council. "Safeguards for Remote Access" *Journal of AHIMA* 78, no.7 (July 2007): 68-70.