Protecting the Wave of the Future: Establishing Security for the Electronic Health Record

by Jonathan Barmettler, CISSP, MCSE, CCNA Jeffrey C. Bauer, PhD

The electronic health record is accessible, portable, and invisible. So how do you protect the EHR in the real world?

The digital revolution is finally gaining momentum in health information management. Over the past few years, three well-publicized reports by the Institute of Medicine have focused national attention on the need to improve quality and reduce costs by replacing paper medical records with electronic information systems. Over the past few months, the White House and Congressional leaders have introduced major initiatives to get healthcare off the paper trail.

If a new federal push for electronic records is not enough to initiate serious security preparations within healthcare organizations, an old federal law will be. HIPAA's security rule is scheduled to become effective in April 2005. Even if the rule is delayed or modified (not uncommon in HIPAA-related matters), the imperative to protect health data from "reasonably anticipated" threats and impermissible uses will not go away. Organization leaders, HIM professionals, and IT specialists must work together to develop compliance strategies. This article provides a conceptual framework for anticipating problems and preparing effective solutions for the unique security challenges of the electronic record.

An Approach to Digital Security

The automation of financial information during the past 20 years is instructive for the healthcare industry. The way we handle money has changed dramatically, and financial institutions have had to develop new ways to ensure the security of our funds and financial data. Health systems are just beginning to experience a comparable transformation. Telemedicine, for example, is analogous to using an ATM. Interactions that previously required face-to-face encounters can now occur asynchronously (i.e., not in real time) in a wide range of locations. Similarly, e-mail communication between patients, providers, and payers is comparable to online banking. In both instances, new technologies have enhanced exchange relationships—changing the way information is created, stored, and used and requiring new approaches to information security.

Unlike financial information's relatively short shelf life, medical data can be relevant, meaningful, and even life-saving for a lifetime. Consequently, forward-looking organizations must address challenges of protecting digital information and make it readily available to medical practitioners for years to come. These challenges are different in paper and electronic environments. A conceptual model with four dimensions provides a useful way to approach security in the electronic environment:

- Latency (visibility)
- Ubiquity
- Retrievability
- Accessibility

Latency

One of the most obvious differences between digital and paper records is latency, or visibility. Paper records are fully self-contained. Everything is present for the eye to see. Conversely, electronic records exist in hidden form. They are not immediately apparent. Digital information is, literally, invisible.

Digital data are also much more compact in both physical format and information content, so large volumes of digital information can be carried easily and unobtrusively from place to place. (See sidebar, "File Cabinet on a Keychain," below.) For example, today's USB key fobs can hold up to two file drawers of scanned documents. One CD can hold more data than a four-drawer file cabinet, and a single-side DVD can contain more data than eight file cabinets. All can fit in a shirt or coat pocket. The potential for security risks is readily apparent.

New digital disk drive units have even more capacity. Laptop and USB drives are now available in 20 to 60 GB configurations; internal desktop systems can have more than 160 GB of disk capacity in off-the-shelf configurations. These drives can store complete patient databases. Like CDs and DVDs, they are removable and transportable. Digital information can "walk out the door" in ways that were impossible when equivalent paper records were stored in file cabinets.

Medical facilities have formal policies and industrial-strength shredders for disposal of paper documents containing patient information. An analogous set of approaches should be adopted for digital media, including:

- Providing bins for destruction of digital media (e.g., diskettes, CDs, DVDs) or ensured support for destruction of digital media placed in the same bins as paper
- Configuring desktop and other workstation systems to limit access to USB ports to users with appropriate administrative rights
- Having procedures to wipe or destroy all disk drives in laptops and desktops before these machines are discarded or returned on lease
- Requiring all users to lock up digital media as they would paper files with the same information
- Training all users to shred or properly destroy digital media no longer usable

File Cabinet on a Keychain

Comparing Storage of Paper and Digital Files

File cabinets of paper records can now be swallowed up on digital storage devices as small as a CD-ROM or a flash drive or memory stick that hangs from a keychain or fits in a shirt pocket. The increased mobility of electronic data poses an obvious threat to security.

Files Created Digitally	**Storage Requirement (KB per Page)**
Text files	2
Microsoft Office files	5
PDF files, text only	10
PDF files, simple line art	50
PDF files, mostly images	1,000

Scanned Files	**Storage Requirement**
(8.5" X 11" page, 1 bit per pixel, black & white, CCITT G4/A4 and compressed)	
1 scanned page	50KB
1 box or file drawer (2 linear feet of files, loose enough for active filing)	125MB
1 file cabinet (4 drawers) (10,000 pages on average)	500MB

Source: Archive Builders. "Measuring Scanned Documents, Born-Digital Documents, & Digital Storage." Available online at www.archivebuilders.com/whitepapers/22009p.pdf.

Ubiquity

Unlike original paper records that can be in only one place at a time, electronic records can exist in many places simultaneously. Digital technologies give medical records an unprecedented omnipresence, so HIM professionals, IT specialists, and clinicians must work together to maximize the benefits and minimize the risks as migration from paper to disk makes data available anywhere, any time.

Paper-based problems of shadow records and splinter data (i.e., individual practitioners' observations that are not part of the approved record, such as rounding notes on 3" x 5" cards) do not automatically disappear with digital conversion. Electronic information is superior because many people can use it at the same time, but special care must be given to ensure that all relevant information is integrated. Database coordination is essential, reinforced by HIPAA's focus on defining the primary dataset and documenting the flow of information. Securing protected healthcare information (PHI) also involves integrating and securing research databases and other files that contain related patient data. The full benefits of the electronic health record (EHR) will not be realized if it does not contain all relevant data.

The proliferation of form factors (e.g., work stations, laptops, PDAs) promotes ubiquity by allowing caregivers to use data almost anywhere. Unfortunately, theft and loss of devices also make information available to unauthorized persons. The problem is exacerbated by the storage capacity of miniscule data platforms. (See "Leaving the Database Behind," below.) Hundreds of confidential patient records can be stored on a cell phone or PDA, for example. A person who steals or finds the device could access the onboard data without entering the online network.

Best practices of backup, security, and positive control are even more important in this expanding infosphere. Ubiquity compels HIM and IT professionals to update policies and procedures in responsive ways, including:

- Maintaining a complete and current inventory of all repositories of patient information by content, location, device, and size
- Tracking and synchronizing decentralized patient information for integration into the record set, as necessary
- Developing policies for ownership of both devices and data, with meaningful and enforceable penalties for noncompliance
- Defining clear requirements for positive possession (e.g., "I can see it, I locked it up, I have it in my hand") of all equipment and data media that contain PHI
- Mandating durable labels with the authorized user's name and address so that lost equipment can be returned
- Using robust security and encryption systems on laptops and PDAs where PHI resides, with controls for compliance
- Maintaining appropriate software and hardware security when portable devices are operated in wireless environments

Leaving the Database Behind

The Increased Potential for Losing Data

Data's increased mobility puts it at risk not only of being stolen but of just plain being left behind.

"At McCarran Airport, 1,200 cell phones, 1,500 sets of keys, and more than 300 laptops were turned in last year alone."
Source: McCarthy, Alyson. "The Honesty Test." KLAS Channel 8 Special Report. Available online at www.stuffbak.com/video/klas.mpg.

"More than 10 mobile devices are lost or stolen in the world every minute. The majority are never returned to their owners."
Source: Impivaara, Matias. "Go Mobile, Stay Secure." *F-Secure Newsletter*, January 2002. Available online at http://f-secure.fr/news/newsletter/protected/archives/prot-1-2002/juttu1396.htm.

"At least 400 laptops belonging to federal law enforcement agencies including the FBI, the Drug Enforcement Administration, and the US Marshals Service have been misplaced, lost, or stolen, a recent audit by the Justice Department's Inspector General has determined."
Source: Kane, Margaret. "Senator Decries Rising Tide of Lost Laptops." CNET News.com, August 16, 2002. news.com.com/Senator+decries+rising+tide+of+lost+laptops/2100-1029_3-950155.html.

"A division of GMAC Financial Services has been quietly informing about 200,000 of its customers that their personal data may have been compromised because of the theft of two laptop computers from an employee's car at a regional office near Atlanta."
Source: McDougall, Paul. "Laptop Theft Puts Customer Data At Risk." *Information Week*, March 29, 2004. www.informationweek.com/story/showArticle.jhtml?articleID=18402885.

Retrievability

Although electronic medical information can be expanded from virtual invisibility on a microchip to thousands of user interfaces in real time, it has no value if it cannot be located when needed. HIM and IT professionals must ensure that required information can be found, formatted, and delivered to authorized requesters in a timely and effective manner. Like paper records, electronic records must be indexed and they must be protected from fire, flood, and theft. However, electronic information requires special protections beyond those normally associated with retrieval of information from paper records.

For example, electronic information must be protected from electronic threats like viruses, worms, and other hacking intrusions. Electronic records systems also require hardware and software to function; both need to be constantly updated and frequently replaced. Maintenance and upgrade costs must be budgeted for all system components, along with earmarked funds to train existing personnel or hire IT staff knowledgeable in new technologies.

Disaster recovery and business continuity planning also have special dimensions in the virtual world. Hardware, software, and buildings can be replaced, but electronic data are often irreplaceable. Information managers and systems operations staff must participate actively and proactively in functions that protect information, backing up data according to strict protocols that support restoring all necessary data to rebuild a system. A recovery process generally requires a series of backup data libraries, with reliable storage at a site distant from the location of normal operations.

In summary, security-focused HIM and IT professionals should address key aspects of users' needs to retrieve data from electronic records, including:

- Creating and managing business continuity and disaster recovery plans, with related updating whenever new data systems are installed
- Testing performance of these plans on a regular basis and correcting all detected failures
- Preparing current and future budgets that reflect the real costs of maintaining hardware, operating systems, and software required to access health information
- Providing operational backup systems to copy data to less volatile storage, with appropriate off-site retention of storage media
- Ensuring objective assessment of the security profile of systems that house PHI and correcting vulnerabilities that are found
- Having and enforcing standards for virus protection, intrusion detection, and data integrity

Accessibility

HIPAA's security and privacy regulations focus considerable attention on accessibility. After all, medical information must be kept for a long time, making it more vulnerable to unintended disclosure and damage. While access to paper records is generally controlled by locks, badges, and checkout procedures, electronic information can be accessed from sites that are not under physical surveillance.

In most health facilities, workstations and laptops connected to the network give access to almost all information within that network, including health records. By extension, open ports on unattended laptops or workstations can give anyone access to network data. Steps should be taken to close ports as soon as they are not in use and to authenticate all users when they begin using a port, especially in public locations like reception areas, conference rooms, cafeterias, and libraries.

Procedures must also be developed to regulate valid attachment to the network through user-owned equipment (e.g., a physican's PDA or a vendor's laptop). These "foreign" devices are not usually controlled by the facility and may not,

therefore, comply with antivirus and security specifications. Encryption methods and firewall protocols must also be addressed, particularly with the growth of wireless connectivity and medical staff interest in access to hospital records.

Policy and procedures must also encompass role-based access tied to the user's relationship to the data. Privacy compliance officers and senior managers need to participate in this determination. Restricting access to specific components of an electronic record is increasingly common. The task of matching users to specific information is generally assigned to an access control group. Because health facilities have many temporary employees and high rates of turnover in some departments, accumulated rights can be a large problem (see "Access Control," below).

Authentication—verifying a user's identity—is another challenge that must be addressed formally. Generic log-in procedures have been common in the past, but HIPAA security rules are forcing health systems to implement more robust log-in systems for all workstations and applications.

Clinical managers, HIM professionals, and IT leaders must address the following elements when developing sound policy for access to the EHR and related PHI:

- Evaluating all firewall holes and implementing mechanisms to disallow inappropriate or unapproved access
- Shutting down all unused ports and other connections when the user has ceased to interact with the network
- Authenticating all remote access to the EHR and to PHI at both the network level and the application level
- Installing firewalls or implementing virtual local area networks between the wireless network and other systems (e.g., a VLAN that strictly limits access to designated databases and no others)
- Defining patient care roles and related security profiles for awarding access to specific employee or medical staff groups
- Requiring users to authenticate themselves to all networks and applications
- Establishing criteria to verify that accumulated rights are consistent with each user's current security profile
- Performing audits to identify users placed on termination and deletion lists
- Comparing active users' access rights to their actual needs for data

Electronic data may be invisible, but security can be established by seeing risk in terms of latency, ubiquity, retrievability, and accessibility. With the EHR gaining momentum and the HIPAA security rule soon to take effect, organization leaders, HIM professionals, and IT specialists must anticipate problems and prepare effective solutions to ensure the smooth transition to a secure EHR.

Access Control

Limiting a user's access to specific information in the electronic record is an important security measure. Ongoing management of rights is just as important.

"Most users, over time, accumulate access rights—nothing is ever removed. This usually results in increased information risk. Ideally, users should, as the organization changes and as their roles within the organization change, experience changes in access rights…

"During the termination phase [of employment], organizations should verify that the relationship between the user and the organization is, in fact, dissolving, and disable access accordingly. Often, accounts are disabled for a term, then deleted. Unfortunately, although this sounds simple, it demands process rigor. Our research indicates that, on average, users must be deleted from at least 10 different repositories or directories—because average organizations have 60+ repositories for user information and privilege storage."

Source: King, Chris. "User Access Chaos Needs Life Cycle Management." ZDNet, September 18, 2002. http://techupdate.zdnet.com.

Jonathan Barmettler *(jonathan_barmettler@superiorconsultant.com) is senior systems consultant and* ***Jeffrey C. Bauer*** *(jeff_bauer@superiorconsultant.com) is senior vice president of Superior Consultant Company, Inc., Dearborn,*

MI. M.

Article citation:
Barmettler, Jonathan, and Jeffrey C. Bauer. "Protecting the Wave of the Future: Establishing Security for the Electronic Health Record." *Journal of AHIMA* 75, no.8 (September 2004): 24-28.