Privacy and Security Advantages of EHRs

Save to myBoK

by Dale W. Miller

During the late 1980s and early 1990s, the healthcare industry first began to consider implementing what was then referred to as computer-based health records. Concerns were raised about whether these electronic records could be made as secure as the paper records then being used at most organizations.

The results of a 1993 healthcare information privacy survey conducted for Equifax by Louis Harris and Associates and Alan Westin, PhD, at Columbia University indicated strong public support for healthcare reform—including increased use of electronic records. However, 80 percent of the respondents voiced concern about threats to personal privacy, and 71 percent believed computers must be sharply restricted if privacy is to be preserved.

In the 12 years since this study was completed there have been significant advances in information processing and communication technology, as well as in methods for protecting information. In spite of these advances, the transition to fully electronic health records (EHRs) has not yet happened. Despite the vast expansion of electronic commerce, routine e-mail use, the implementation of electronic records in other industries, the increased use of electronic banking and stock trading, and significant advances in security technology for computer systems and networks, security concerns about health records of more than a decade ago still linger.

Recent Security Breaches: Cause for Concern?

During the first six months of 2005, a series of high-profile security violations increased public awareness of the dangers of confidential information falling into the wrong hands. Computer tapes containing millions of consumer financial records were lost, access to personal information was routinely sold to unauthorized persons, and malicious software was installed by intruders to capture the credit card information of 40 million customers. These and other events leading to the unauthorized disclosure of private consumer financial records created the potential for widespread identity theft.

These security breaches were the lead stories on newscasts and occupied national headlines. As expected, reports of these events do not instill confidence in the public that EHRs will be secure—especially at a time when health information exchange initiatives are being proposed to link millions of records. This is in spite of the fact that information security professionals have been advocating that the conversion to EHRs offers the opportunity to protect patient privacy to a greater degree than is possible with paper records and that the HIPAA privacy and security rules mandating protection are in effect.

Our reaction to these security breaches may be compared in some ways to the manner in which we react to airline crashes. At the time we are focusing on these individual tragic events, we tend to forget that air travel is much safer than any other form of travel. While we are appalled when we learn about serious security breaches, it is important to keep in mind that EHRs can be made more secure than paper records and that the organizations where the breaches occurred failed to use generally accepted good security practices and in some cases did not even implement the security measures required by their contracts.

Now that the healthcare industry is working much more actively toward implementing EHRs on a broader scale, it may be worth revisiting the issue of whether electronic records are more or less secure than paper records by reviewing some of the ways EHRs can be made more secure than paper records.

Eliminate the Middleman

A big advantage in the use of EHRs is that it is much easier to provide direct access for the end user to the specific information needed without a middleman to format, retrieve, or otherwise prepare the information for use. The person who simply files, copies, retrieves, or delivers confidential paper records for use by another person gains access to this information and must be trusted not to disclose the information.

Searches for specific information in a large number of electronic records can be performed easily by the person who needs the information without disclosing confidential information to others, whereas a person has to look at all paper records to perform a search function. For example, trying to locate the paper records of all patients who received a specific drug will result in incidental disclosure of confidential information as staff members look at the records for every patient. The staff members will discover confidential information not related to the request and not necessary for them to know.

Transmitting records electronically eliminates the need for messengers to transport paper documents between departments or facilities and eliminates the possibility that the documents will be lost or that the documents will be read by the messenger.

Centralized printing and delivery of paper reports increases the opportunity of someone not involved in a patient's care to read and possibly disclose or misuse the information. The use of EHRs eliminates much of the risk involved in the disposal of paper records. Persons shredding or recycling paper records will have access to the confidential information.

Role-based Access

Role-based access is the principle of granting an individual access to only the information necessary to perform his or her responsibilities. Although role-based access requires changing traditional thinking about granting access and presenting information, access to confidential information can be controlled to a much greater degree of granularity with electronic records. Information can be much more easily segmented for a specific use directly related to the role of the person needing the information, as opposed to paper records where the person needing only a few items of information has access to all of the information included on the page or in the folder.

New EHR applications can be developed to protect patient privacy by presenting only the specific data objects needed, combinations of data objects for specific purposes, or only the data related to a specific episode. This is in contrast to the current practice of displaying broad categories of information, such as all billing information.

Greater Accountability

EHRs make it possible to enforce much greater accountability for the creation and access of information. EHR systems have the capability to maintain a record of who entered or viewed information and when and, in some cases, where the access occurred. These log records can then be audited to investigate possible incidents of unauthorized access and disclosure. The knowledge that access to the information is being recorded may deter some people from attempting to gain access to confidential information.

It is extremely difficult and expensive to maintain a similar record of access to paper records. Unless closely monitored, a person using a paper record can alter, remove, or destroy pages from the record. Digital signatures and encryption can be used with EHRs to attribute the entry of information to specific persons, vouch for the authenticity of the information, and prevent modification of the information.

Eliminate Faxes

Faxing paper records presents a variety of security risks. A fax can be sent to the wrong location, read by anyone at the receiving location, and stored or disposed of insecurely. Unless the fax is machine generated, the information in the fax is also disclosed to the person preparing and sending the fax.

Many faxes can be eliminated if caregivers and others who need the information are able to gain access to the information electronically when and where they need it, rather than requesting that the information be sent to them in a fax.

Ability to Encrypt Information

One argument against electronic records is the relative ease with which millions of patient records stored on a disk or reel of tape can be lost or stolen. In contrast, it is difficult to steal truckloads of paper records from an HIM department. While most would agree that this is true and acknowledge that millions of financial records on tape have recently been lost or stolen, the information stored in electronic format can be encrypted to prevent access if it is lost or stolen. Paper records being transported or warehoused can be read, copied, and disclosed if they are lost or stolen.

Paper records in a lost or stolen briefcase are vulnerable to disclosure, while information on a laptop and PDA in a briefcase can be protected with encryption. Sensitive information can also be encrypted for electronic transmission or storage to prevent unauthorized access.

Support for a Mobile Work Force

The anecdote of the car dealer who called the hospital to ask if it would like the folders of medical records in the trunk of the car just traded in by a physician illustrates some of the risks in permitting paper records to be taken from secure locations to support health professionals working outside of hospitals or clinics.

EHRs make it possible for work to be done securely in any location without the need for making additional copies and carrying paper records. Paper records can be left in an airport, coffee shop, bus, or at the wrong patient's home.

More Secure Communication

As EHRs are implemented, it is possible to use more automated messages to communicate with both patients and caregivers. For example, appointment reminders and some test results can be sent to patients automatically as text messages to their personal mobile phones or as e-mail messages to their private accounts rather than as postcards or as calls from a receptionist who does not have a need to know the information.

The healthcare industry has become accustomed to the methods and practices for protecting paper records that have evolved over the years and the level of privacy and security those practices provide. The industry now has the opportunity to improve the protection of patient privacy and the security of information as it moves to EHRs. But that improvement in protection will only occur if the implementers and users of EHRs recognize this opportunity and use effective security methods and technology to protect the information.

Dale W. Miller *(dwmiller@irongateinc.com) is director of client services at Irongate, Inc., in San Rafael, CA.*

Article citation:
Miller, Dale W. "The Privacy and Security Advantages of EHRs." *Journal of AHIMA* 76, no.8 (September 2005): 62-63,68.