Internet Security: What Health Information Managers Should Know

by Dale W. Miller

As experts in the authorized release and protection of patient information, health information managers are continually faced with new challenges as their organizations implement computer-based patient record systems, participate in health information networks, and embrace other new technologies. Not the least of these challenges is security related to the use of the Internet.

Extensive Internet coverage in the industry and public media adds to the difficulty of determining which security issues should be given priority. Sometimes it seems that the Internet and Internet security are getting more press coverage than nearly any other single topic-including the Olympics and political elections. Separating the hype from reality and making reasonable decisions can be extremely frustrating and time consuming. But, unless you are within a few months of retirement or planning to move to another planet, the Internet cannot be ignored.

The level of concern about Internet security depends on how the organization is using the Internet and how the organization connects to it. Even if the organization has not connected its network to the Internet or has not yet officially begun to use it, it is highly likely that there is unofficial use already occurring at the organization's facilities. Some staff members who are not being provided Internet access via the organization's systems and networks may be using the Internet at work by dialing up service providers under their own subscriptions. Even though these staff members may be paying for these services, the fact that they are gaining access to the Internet on the organization's premises, and possibly with the organization's computers, may put the organization at risk.

Internet Security Risks

The major categories of information security risks related to Internet access are:

- Unauthorized access to the organization's computer systems and networks
- Unauthorized disclosure of confidential patient information or the organization's proprietary and confidential information
- The introduction of computer viruses and other computer contaminants into the organization's computer systems and networks

Although these are not exactly information security risks, poor judgment in the use of the Internet can also result in sexual harassment claims, adverse publicity for the organization, and the loss of many hours of productive time.

If the organization has already implemented a well-designed, comprehensive information security program, most of the policies, training, and controls will be in place to address Internet information security risks. Only minor enhancements in the program may be necessary. Because the Internet is changing so rapidly, however, constant vigilance is necessary to ensure that the information security measures the organization has implemented provide sufficient protection. The infrastructure provided by an organization-wide information security program ensures and facilitates that constant attention.

If the organization has not yet established an information security program, the decision must be made whether to address Internet security issues by implementing an organization-wide program or to deal with only the Internet issues and implement a complete program at a later date, perhaps in preparation for a Joint Commission on Accreditation of Healthcare Organi-zations survey or in response to a lawsuit.

Implementing Internet Security Measures

A starting point for addressing Internet security is to determine how the Internet is being used. Usage can be divided roughly into three categories.

Using the Internet as an Information Resource or Online Library
An example of this would be browsing the World Wide Web to access the vast amount of information available, such as visiting AHIMA's Web site to review professional development opportunities, or visiting the US Congress Web site to review proposed healthcare confidentiality legislation.

Using the Internet as a Communication Vehicle
Sending and receiving e-mail, participating in mailing lists or discussion groups, and making information available to the public on the World Wide Web are examples of the Internet's use as a communication vehicle.

Using the Internet as an Extension of the Organization's Network
Examples of this would be linking your computer systems to another organization's computer systems to participate in a joint research project, provide remote access for staff members, transfer files to other organizations, or conduct business transactions.

The second step in addressing Internet security is to determine how the Internet connection is actually made. In general, a dial-up connection from a personal computer solely for browsing the World Wide Web creates far less risk than a high-speed connection to the organization's networked computer systems. Dial-up connections are slower, however, and offer less functionality. Connections that allow access to the organization's systems from outside the organization create the greatest risk.

Managing Internet connections is not a do-it-yourself project that can be handled by most departments in the organization. The information systems department should be formally assigned the responsibility of establishing and maintaining the organization's links to the Internet. Organizational policy should prohibit the establishment of other connections to the Internet from the organization's computers. The policy should also prohibit dialing into the Internet from personally owned computers while those computers are on the organization's premises, if those computers are also connected to the organization's network at the same time.

The organization's connections to the Internet should be protected by a firewall. A firewall is the computer hardware, software, and network equipment used to control the link to the Internet. It is more appropriate to think of a firewall as a concept rather than a specific piece of equipment or a specific set of filters screening the information passing through the network connection. The functions and controls enforced by the firewall should be in accordance with the organization's information security policy. The information systems department should monitor the firewall and continually update its functions as new threats are discovered.

By policy, use of the Internet should be limited to patient care or business functions and other purposes as approved by an individual's manager. This makes it the manager's responsibility to deal with an employee who spends too much time browsing Web sites related to a hobby, for example. Currently, just browsing Web sites does not pose a significant amount of risk. As more and more Web sites implement the capabilities of Java (a programming language that automatically transfers small programs to your computer to perform enhanced functions while you are browsing Web sites), the risks of computer viruses or other programs that search for information on your computer and report it back to the Web site without your knowledge will increase.

A valuable feature of the Internet is the ability to send e-mail to other Internet users anywhere in the world. These e-mail messages are very similar to postcards. As a communications facility, the Internet should not be considered to be secure. The messages may be read by many persons and stored on many different systems prior to delivery, and the recipient may make copies and forward the message to any number of people. The message may be delivered in minutes or it may take several days. Communicating with patients via e-mail poses risks to the patient's privacy. In many cases, e-mail messages to patients will be directed to e-mail systems at their place of employment where the message is subject to review by the patient's employer. Many organizations that use e-mail for communication with patients require the patient to request in writing that e-mail be used and to acknowledge the potential for breaches of confidentiality. Policies governing the use of e-mail should be developed and communicated to all users of the Internet in the organization.

Mailing lists provide a special e-mail capability very similar to a discussion group or bulletin board. Internet users subscribe to mailing lists for special interest groups. Sending an e-mail message to the list makes it available to all subscribers. Although this is a valuable source of information, these groups may also be used inadvertently or even intentionally by staff members to disclose proprietary or confidential information. A typical message to a mailing list might be a request for copies of another organization's policies or training material that could be used to develop policies in preparation for a Joint Commission survey. Many organizations do not permit distribution of proprietary materials-materials they have spent thousands of hours and tens of thousands of dollars developing-to potential competitors, although some organizations might not have restrictions on making their policies public. Staff members should be informed about the organization's policy for participating in mailing lists, the type of information subscribers can post, and whether or not they are permitted to provide comments on behalf of the organization. Patient identifiable information should never be posted to these lists in order to illustrate procedures or methods.

If the organization has not established a Web site, it is not uncommon for one or several Internet-savvy employees to take the initiative to create a Web site for the organization. In some cases, inappropriate information has been included in these Web sites. Policies should be established defining the responsibility for the creation of any Web sites and requiring all information for publication on the organization's Web site to be approved by the organization's public relations department.

Access to the organization's systems and network from the Internet should be totally prevented or stringently controlled. Robust system access controls and firewalls are essential to prevent unauthorized access from outside the organization. Remote logins, telnet, remote procedure calls, and other functions that permit accessing the organization's computers from the Internet should be blocked by the firewall.

File transfers, or FTP, should be used with caution. This capability allows files to be transferred from one computer to another via the Internet, often without verifying the identity of the requestor. When FTP is used to transfer files into the organization it is possible to download software in violation of copyright laws or to infect the organization's computers with viruses. File transfers outside the organization include the risk of disclosing confidential patient information or proprietary information.

While the risks associated with the Internet are significant, the benefits of using the Internet properly can be enormous. Health information managers should ensure that their organizations have established formal information security programs with the policies, training, and controls to address Internet usage. They should become users of the Internet to more fully understand the issues and should ensure that all systems and networks storing and processing patient information with links to the Internet are protected with firewalls.

Ten Ways to Prevent Internet-related Security Risks

1. Determine how the Internet is being used.
2. Determine how the Internet connection is made.
3. Permit only the information systems department to establish and maintain Internet links.
4. Implement a firewall.
5. Establish policies limiting Internet uses to approved purposes.
6. Establish policies governing the use of e-mail.
7. Inform patients about the risks of using e-mail to communicate confidential information.
8. Give guidance to employees on what can be shared via mailing lists.
9. Define responsibility for creating any Web sites.
10. Use file transfers with caution.

Dale W. Miller *is director of Consulting Services at Irongate Inc., San Rafael, CA. He may be reached on the Internet at dwmiller@irongateinc.com.*

Article citation:
Miller, Dale W. "Internet Security: What Health Information Managers Need to Know." *Journal of AHIMA* 67, no.8 (1996): 56-58.