

CyberSurgeon

What doctors should know about e-mail confidentiality issues

by Karen Sandrick, Chicago, IL

Electronic mail is an extremely helpful tool for surgeons to use in communicating with their colleagues and their patients. E-mail eliminates the aggravation of telephone-page-beeper tag and can provide a convenient record of consultation notes or patient care instructions. It can also be an effective way of communicating information that patients may find too complicated to remember after the doctor-patient encounter—specific test results and their meaning, medication dosing details, postoperative follow-up care, and names and addresses of other caregivers or social service agencies. E-mail can be linked with formal consumer or professional Web sites or search engines to supplement education and communication, and the information in e-mail messages can be made a permanent part of the patient's electronic or paper medical record with a click of the mouse.

But e-mail is not the ideal way of transmitting sensitive patient information. For one thing, it may not be nearly as immediate as most of us think, nor is it completely confidential. By its very nature, e-mail appears to offer an instantaneous connection between sender and recipient, but in actuality, an e-mail message may sit in an individual's queue of new mail for days or even weeks. Nor is e-mail completely private. Members of a physician's office staff may be able to open e-mail messages to route or triage them. E-mail messages may pop up on a terminal screen that can be seen by patients or health care professionals who happen to be in the office. Moreover, unless an e-mail communication system has a secure firewall and uses encryption software, a message could conceivably be accessed by an unauthorized individual over the open Internet, or it could be monitored by an Internet service provider.

As David Krusch, MD, FACS, explains, "When an e-mail message travels over the public Internet, it is relayed through multiple servers at multiple

institutions in a completely unpredictable way. As it is relayed, parts of the message may be broken up. One part may get to its destination along a particular route; another part may go through a separate route. Although the parts of an e-mail message can be difficult to reassemble, generally speaking, someone *can* capture any or all of the message and read it."

E-mail also may not always come from a legitimate source or reach its intended targets. "There is no true way for anyone to authenticate the identity of the sender or the recipient of e-mail. Senders can make an e-mail message look like it came from someone else, and authors don't know with 100 percent certainty who actually receives an e-mail," adds Dr. Krusch, a general surgeon at the University of Rochester, NY, Medical Center, who serves as Chair of the ACS Informatics Committee and the committee's representative to the ACS Communications Committee.

What's needed, Dr. Krusch says, are methods for ensuring the authenticity of the senders and recipients of electronic communication; encryption and decoding on both ends of the communication; and overall guidelines for handling electronic communication in the health care setting. "Without that, electronic communication is totally insecure," he says.

Electronic vs. paper and telecommunications

Standard methods of communication—letters, faxes, telephone conversations—are far more secure than e-mail. "A paper letter is secure unless someone steams it open. As long as you know who has access to the destination fax machine, a fax is secure. A telephone connection is a private circuit, so even though a telephone call goes over public telephone infrastructure, every conversation is allocated a little piece of bandwidth on the phone company's lines. Other people can't get in on a telephone conversation without physically breaking

Guidelines for electronic communications with patients

A task force on guidelines for the use of clinic and patient electronic mail, established by the American Medical Informatics Association (AMIA), released a series of recommendations in 1998. In addition to guidelines on medicolegal and administrative considerations, the AMIA task force published several general tenets for communicating with patients via e-mail. The full set of guidelines was published in the January/February 1998 issue of the *Journal of the American Medical Informatics Association* (vol. 5, no. 1, pp. 104-110) and it can be accessed on the AMIA Web site (www.amia.org). The following excerpt is reprinted with permission from Hanley & Belfus, Inc., Philadelphia, PA, publishers of the journal:

- Establish a turnaround time for messages. Do not send e-mail for urgent matters.
- Inform patients about privacy issues. Patients should know who, besides the addressee, processes messages during regular business hours as well as when the addressee is on vacation or ill. Patients also should know that their e-mail messages will be included as part of their medical records.
- Establish the types of transactions (prescription

refills, appointment scheduling, and so on) that are handled by electronic communication and the sensitivity of the subject matter (HIV, mental health, and so on) that may be communicated via e-mail.

- Instruct patients to describe the category of the transaction in the subject line of their messages for filtering purposes: “prescription,” “appointment,” “medical advice,” or “billing question.”
- Request that patients put their name and patient identification number in the body of the message.
- Configure the automatic reply to acknowledge receipt of messages.
- Print all messages, with replies and confirmation of receipt, and place in the patient’s paper chart.
- Send a new message to inform the patient of the completion of a request.
- Request that patients use the autoreply feature to acknowledge they have read the provider’s message.
- Maintain a mailing list of patients, but do not send group mailings where recipients are visible to each other. Use the blind copy feature in software.
- Avoid anger, sarcasm, harsh criticism, and libelous references to third parties in messages.

into those telephone lines by means of a wiretap,” Dr. Krusch explains.

But the Internet doesn’t use switching technology like the public telephone service; it utilizes broadcast technology, which means packets of information are thrust into cyberspace for just about anyone to read. “Other people don’t routinely get our e-mail messages because their systems filter out the messages. However, it’s very easy to write software programs to bypass those filters and grab e-mail,” he points out.

Large institutions such as hospitals, health care systems, and professional associations build internal electronic communication networks that are relatively well protected. Intranets also offer directories that validate or authenticate the identity of the individuals who send and those who receive e-mail messages. “When physicians are com-

municating with physicians within their own private network, they can be relatively confident about who they are communicating with and that no one else can read their messages,” Dr. Krusch says.

Still, secure, authenticated, encrypted information that is communicated via an institutional Intranet is not protected from legal discovery, so it can be used in a legal proceeding, according to Dr. Krusch. And unlike letters, faxes, or consultation notes, which are well recognized as legal patient care documents, e-mail messages tend to be informal in their wording. E-mail users also tend to be somewhat cavalier about sending copies of messages. “We probably click on ‘send’ before we do a significant content review of our e-mail. When we get e-mail from other people, we’re also often guilty of clicking on ‘reply to all’ or ‘forward’ without sifting through the previous chain of e-mail notes

and trail of responses. We don't exercise the same degree of discretion or use the same amount of filtering with e-mail that we do with other types of communication. We're casual, and when we're dealing with patient-identifiable data that can be legally discoverable, casual is not acceptable," he says.

Protocols for e-mail communication

Physicians at the University of Rochester have been exploring criteria that will ensure secure, authenticated, and confidential electronic communication. A proposal made by Dr. Krusch would create an electronic communication system that does not depend on e-mail. According to this proposal, an office practice or hospital would create a secure Web site just like those of commercial companies, such as Eddie Bauer or Harry and David. Like these commercial Web sites, the practice or hospital Web site would obtain a certificate from a company called a certificate authority that attests to the site's authenticity. A certificate not only would validate the identity of the holders of the Web site, it also would allow information to be encrypted.

Once a secure Web site was created, a physician would give to each of his or her patients information needed to be able to log on to the site. "When a patient schedules an appointment or visits the office or has an outpatient appointment or operative procedure, the physician would give the patient a business card that contains a user name and password as well as the electronic address or URL for the Web site. When patients go to the Web site, they would be asked to log in with the user name and password they were given by the health care provider," he says.

A secure Web site would provide a measure of reassurance for both parties to an electronic conversation. Patients would be assured that they are linking directly with their physicians because access to an authenticated Web site is restricted. Physicians would be assured that they are communicating with patients or the individuals their patients trust to share a user name and password. "Because the user name and password would be maintained in a database controlled by the provider, we would have security and authentication right there," he says.

Dr. Krusch also suggests that a Web-based electronic communication system replace free-form

text e-mail-like messages with codified entries and prominently display warnings and disclaimers to indicate what needs to be done in an emergency. "Instead of randomly typing in free text, which is too unstructured to be useful to either party, patients would get to choose from predetermined lists: they want to renew a prescription or schedule an appointment because they have certain symptoms. And smack at the top of the page on the Web site in blinking red letters, they would see the statement 'If this is anything other than a routine matter, please call this number.'" Such precautions are needed, Dr. Krusch believes, to clarify the level of urgency and the nature of the electronic communication. Patients need to be reminded that electronic communication is not the appropriate way to call for medical help but a simplified way to make certain types of limited requests.

Finally, Dr. Krusch advises creating guidelines for processing electronic communication in the private office, clinic, or hospital setting that should include the manner in which messages are triaged, protected, identified, categorized, and answered (see the "Guidelines for electronic communication with patients," p. 34, which have been adapted from the American Medical Informatics Association). "Many electronic communications do not have to go directly to the provider; they can be sent to someone who assesses the type of request, fulfills the request, or realizes that a situation has an increased level of urgency and must be evaluated by a physician," he explains. Consequently, patients need to know not only who reads electronic communication but also when they can expect a response and what happens to their correspondence.

The overall objective of setting criteria for electronic communication is to protect patient-sensitive data. Says Dr. Krusch: "My philosophy, today in the year 2000, is that until everyone is using signed, encrypted, and secure communication systems, we probably ought not to communicate patient information via e-mail. We need to be prudent in our use of electronic communication, whether it is between doctors or between doctors and patients. We need to think about guidelines for setting up a totally new mechanism for communication." □

Karen Sandrick is a freelance medical writer in Chicago, IL.