

## Update your e-mail policy now to keep up with usage

*(Editor's note: This is the second in a series of articles about the risks of using e-mail in health care. Next month's issue will include the third in this series.)*

Chances are good that you have a policy on the proper use of e-mail within your organization and when communicating with patients, but it probably is time for an update to keep pace with rapid advances in technology and the way people use e-mail.

That's the advice from risk managers who say a good e-mail policy may keep you out of serious trouble. Although e-mail is becoming more prevalent, health care practitioners need to be cautious about communicating in this fashion, says **LoriAnn Rickard, JD**, president of Rickard & Associates, a law practice that specializes in health care. She formerly was in-house corporate counsel for St. John Health System, a member of Ascension Health. The content can be a problem, but the Health Insurance Portability and Accountability Act (HIPAA) requires you safeguard the electronic transmission of any protected patient information, she says. That can be difficult without extensive safeguards such as encryption of messages. E-mail tends to be more casual and causes individuals to make quick statements that may be used later for a purpose that the health care professional may not have intended," Rickard says.

"Not only the substance of the e-mail must be considered, but also the transmission over the Internet must be protected. Policies must be in place to govern the submission of health care information in and protect its content from being corrupted and/or intercepted," she adds.

### Attachments more common now

Attachments to e-mails present a particular threat, Rickard points out. As doctors become used to communicating by e-mail, and as more documents are available in an electronic format, they get in the habit of attaching a patient's chart or test results when e-mailing a colleague for a consult, for example. If that attached document is not protected, it can present a serious privacy breach. Rickard cautions that risk managers from the baby boom era, such as herself, can easily underestimate how much e-mail is used in health care now.

Older professionals may be adopting e-mail at a rapid pace, but for their younger counterparts, e-mail is the default method of communication, she notes. "They don't even think about using the telephone first," Rickard says. "If they want to contact someone, they just automatically look for the e-mail address and fire off a message."

### Easy to overlook e-mail risk

Even as health care embraces various technologies, the hazards of e-mail can get lost in the shuffle, she says. Unlike electronic records, for instance, there is no particular vendor associated with it, no one whose contract requires they alert you to the risks and install safeguards.

"With e-mail, it's a doctor who installs AOL on his home computer and starts whipping off an e-mail to somebody, and you don't even know what's going on," Rickard adds. She recounts talking with a young physician who routinely sent an e-mail to the referring physician after seeing a patient — on AOL, with no special precautions to protect the information. When Rickard expressed concern, "He looked at me like I had two heads. It was just second nature to him, and it never occurred to him that e-mail would be a problem."

For that reason, strict policies are necessary and they must be communicated effectively to physicians and staff. Rickard says risk managers should review their e-mail policies at least on a yearly basis and a quarterly basis would be even



better. “The policy you wrote five years ago is not good enough. It’s outdated now,” she adds. “You also need to be familiar with your policies and all the potential risks from e-mail so that if you’re sitting in a meeting and someone suggests using e-mail in a new way, a bell goes off in your head to tell you that your policy needs to be updated.”

### **Avoid forwarding copies of old mail**

Rickard offers these rules to include when updating your e-mail policy:

- If the topic requires a letter or phone call, don’t convey the information by e-mail. When the information is that important or sensitive, don’t risk an e-mail message even if you follow up with a phone call or snail mail.
- Never use the “reply-to-all” function. It is too easy to send the message to unintended recipients that way.
- Do not include past e-mails in your reply. E-mail systems should be set up in a way that the reply function does not automatically copy the first e-mail into the reply. That function, common and useful in some settings, can result in a string of old messages that include confidential information forwarded to someone who shouldn’t receive it.
- Assume anything you send by e-mail will be read by a plaintiff’s attorneys. “If you don’t want to stand on your desk and scream what you said to the public, I don’t think e-mail is the appropriate forum, unless you take a lot of precautions like encryption,” Rickard says. “But even then, assume it will be dug up by plaintiff’s attorneys.” Rickard says she is “flabbergasted at how many risk managers say this has never occurred to them as being a serious issue.” She says the risks are not just theoretical. Rickard has seen cases in her own practice in which confidential patient information was misdirected, with terrible results. Relatives have seen e-mail that disclosed a person’s HIV status, which the

patient had kept private, she notes. The patient and family always react with great anger, she warns. “When I met with the family, it was very difficult.

How do you explain that? In both instances I have seen like that, you really didn’t have much excuse for something like that happening. It just shouldn’t, and you don’t want to have to explain afterward why you didn’t take the right precautions,” Rickard adds. ■