Part B Insider (Multispecialty) Coding Alert

PRIVACY: Watch out-- Patient E-mails Could Be Your Privacy Weak Spot

Treat your patient's health e-mails like other medical records

You work like crazy to protect your patients' privacy--and then they go sending their personal health information via insecure e-mail. What can you do?

E-mail is a major challenge to physician offices. Patients want to be able to ask their doctors questions via e-mail and let doctors know about new symptoms or problems. And your Medical coding and billing company and other business partners also want to e-mail you about pressing issues.

The question is: Are you violating the Health Insurance Portability and Accountability Act every time you deal with e-mails? Here's what the experts advise.

1. First of all, relax. The HIPAA regulations don't require that e-mail be encrypted, because the **Department of Health & Human Services** recognized that it would be too difficult for the average doctor's office to secure e-mail. "Patients wouldn't be able to communicate with their doctors any more," says **Robert Markette**, an attorney with **Gilliland Markette & Milligan**.

"The security rule doesn't give any specific standards," explains Markette. Instead, it just tells you to take reasonable steps to protect patient information--and then leaves it up to you to decide what's reasonable.

The decision whether to encrypt all your e-mail depends on the size and complexity of your organization, adds attorney **Robyn Ellis** with **Gentry Locke Rakes & Moore** in Roanoke, VA.

2. Set some rules for your business partners. Let your billing office know that you don't want to send or receive private patient information via e-mail. If it's urgent, the biller can fax the info, says Markette.

You should write into your contracts with your billing company that it cannot send patient health information (PHI) via unencrypted e-mail, urges Ellis. Oftentimes, billing organizations have a form agreement they want you to sign, and it doesn't mention e-mail encryption. You should have your attorney add a clause to those contracts about protecting e-mail, she urges.

3. Be aware of the risks. You can't stop people from using e-mail, but you should be aware that e-mails can be intercepted by hackers or other "bad guys," says Markette. Sending Social Security Numbers or credit card numbers via email is definitely a bad idea.

Warn Your Patients

If you have a Web site, use it to caution patients about the risks of sending health information via e-mail--especially if the site allows them to send an e-mail, says Ellis. The warning should tell patients they should either send information in encrypted form, or be aware of the risk that someone will intercept it.

4. Protect the e-mails once you've received them. Once you've received an email, it's in your system, and you can protect it, says Markette. That means having a firewall on your computers and requiring a username and password to get into the computer that contains the e-mail. Every time a computer turns on its screensaver, it should require a password to "wake up."

5. Preserve any e-mails that deal with a patient's treatments. You may or may not have to print out a copy of a patient e-mail, depending on what your state's law says about medical records, says Markette. But if the e-mail results in a prescription change or other treatment change, then there should be some record in the patient's chart.

Virginia law doesn't require you to keep a hard copy of e-mails, but you do have to keep any important e-mails in a form that can't be altered, says Ellis. You could store the e-mails on CD-ROMs or microfilms that can't be rewritten.

The bottom line: If state law would consider an e-mail part of the medical record, then you need to keep it for as long as you keep other medical records, usually six or seven years, says Markette. "It's probably not a bad idea to print it off and put it in the file."