Health Information Compliance Alert

Training Strategies: Train Staff To Protect E-mail Without Encryption -- Here's How

You can secure e-mailed data without breaking the bank.

Once you allow your staffers to send and receive emails, you've got to make sure all information contained in those messages is secure. Encryption may be the safest answer, but it's also the most expensive security option.

Check out these cost-effective solutions.

Omit All Identifying Information

Your first step to avoid a privacy or security breach is to coach your employees to never put patients' identifying information in an e-mail, says **Stephen King,** an information security officer with the **Community Health Network of Connecticut** in Wallingford. But if you're using protected health information (PHI) for business purposes, you can't always strip patient information from your message. "You must set clear guidelines on when to send PHI and make sure to only send what's relevant," concurs attorney **Kirk Nahra** of **Wiley Rein & Fielding** in Washington, DC.

That means if you allow your billing staff to send PHI to potential payers, you must teach those workers to send only the information necessary. Example: "Instead of 'I'm going to treat John Smith for AIDS. Is he covered by your insurance plan?' you should ask simply, 'Is John Smith covered by your insurance plan?'" Nahra offers.

Put Patients In The Driver's Seat

Let your patients decide if they will accept the risk of sending unencrypted PHI, suggests security specialist **Tom Walsh** of Overland Park, KS-based **Tom Walsh Consulting**. When your patients request contacting your facility by e-mail, tell your staffers to "ask them to sign off on an agreement that says, 'I am okay with the risks of sending e-mail,'" Walsh says. And be sure your personnel tells patients wanting to communicate by e-mail that the agreement is valid only until the patient requests that e-mails no longer be sent, he notes.

Remember: This authorization should not be considered a free pass for sending tons of information to the patient, Walsh cautions. Rather, educate your staffers to respond only to e-mails your patients send. Follow your normal procedures for initiating contact -- whether that's by phone or regular mail, he says.

Use A Scrambled Attachment

Establishing an e-mail encryption system is expensive, but you may already have the tools to encrypt a document that can be attached to your e-mail, Walsh notes. Many popular word processing applications, including Microsoft Word, allow you to encrypt your files, he says.

Explain it this way: "Sending the information in the body of the e-mail is like sending a postcard," Walsh explains. On the other hand, "attaching an encrypted document is similar to putting the information inside a sealed envelope," he says.

The drawbacks: Your patients will need a password to decrypt your attachment, Walsh points out.

Strategy: Give patients who want to receive e-mail a password that's good for six months. That way, you can develop a strong password and control when it's changed, he says.

Weigh All Your Options

Don't assume your payers haven't established an encryption method you can benefit from, Nahra says. "Payers in particular are setting up a lot of secure channels," he explains. Good idea: Before you write off emailed PHI for payment purposes, task your staff with polling area payers. Then make a list of those who you can work with to send secure e-mails, he counsels.

You could also "set up a filter at your firewall that will 'bounce back' outgoing e-mails that contain PHI," King recommends.

Plan of action: Train your tech staff to add each patient's Medicaid number, Social Security number and any sensitive data to the list of banned keystrokes. That way, the gateway will recognize that information as PHI and not let it through, King says.

The Bottom Line

The security rule doesn't mandate encryption, but you do have to protect patients' confidential information, King says. And a basic policy outlawing PHI in e-mails isn't enough to keep you out of hot water, he declares.

Many e-mail gaffes are the result of common mistakes, experts advise. Best bet: Teach your staff to doublecheck that each e-mail is addressed to the correct recipient and that your organization's confidentiality disclaimer is prominently displayed.

Next step: Ask your key personnel to list the pros and cons of each security method outside of encryption. Then decide which solution poses the least risk your patients' information, Nahra suggests.