Health Information Compliance Alert

Security Compliance: CORK PHI LEAKS IN STAFF E-MAIL WITH THESE KEY TACTICS

Use these strategies to keep your compliance plan strong without breaking the bank

When you allow your staffers to send and receive e-mails, 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 ANY IDENTIFYING INFORMATION

Your first step to avoid a privacy or security breach is to coach your employees never to 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 PHI for business purposes, you can't always strip patient information from your message. "You should only send PHI via e-mail if it's absolutely necessary," concurs attorney **Debbie Larios** of Miller & Martin in Nashville, TN.

Example: If you allow your billing staff to send PHI to potential payers, teach those workers to send only the information necessary. Instead of asking, 'I'm going to treat John Smith for AIDS. Is he covered by your insurance plan?' you should simply ask, 'Is John Smith covered by your insurance plan?' (Bonus: Check out the sample chart Identifying Information for more information on deidentification).

LET YOUR PATIENTS LEAD THE PROCESS

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 to contact 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 tell 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 only respond to e-mails your patients send. Follow your normal procedures for initiating contact - whether that's by phone or regular mail, he says.

SCRAMBLE & ATTACH FILES

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 that 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.

PIGGY BACK YOUR PAYERS' SYSTEMS

Don't assume your payers haven't established an encryption method you can benefit from, experts caution. Payers are increasingly opening secure payment channels that you can use in place of your own system. Good idea: Before you write off e-mailed PHI for payment purposes, task your staff with polling area payers. Then make a list of those with whom you can work to send secure e-mails, he counsels.

FILTER YOUR PATIENTS' INFORMATION

You could also "set up a filter at your firewall that will 'bounce back' outgoing e-mails that contain PHI," King recommends. That filter could then send an alert message to the administrator or other designated official warning him that a staff e-mail containing PHI was detected. That warning can be used to kickoff security retraining, he suggests.

Plan of action: Start this process by training your tech staff to make a list of each patient's Medicaid number, Social Security number and any other sensitive data. Use the list to help your system recognize those keystrokes as PHI and not let that information through, King says.

THE BOTTOM LINE

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

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

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