Codify
BY AAPC

Health Information Compliance Alert

Security: 3 Proven Tactics Protect Your Transcribed PHI

Use a security questionnaire to iron out your vendor's security rule wrinkles.

If your medical transcription vendor sends completed work to you via e-mail, your security rule compliance could be at stake. Try these field-tested tips to protect your transcribed patient information from Internet hacks.

Question Your Vendor's Standards

You may trust your security rule compliance program to protect patients' PHI, but your vendor's security standards are a different story. First step: Evaluate your transcription company's security efforts.

"We found that several of our vendors didn't have the same security provisions in place that we did," says **Grace Upleger,** HIPAA manager at Vanderbilt University Medical Center in Nashville, TN. Solution: Vanderbilt created a security questionnaire that all transcriptionists must fill out before any work changes hands, she says.

Get started: Kick off your questionnaire development by tracking how the information you'll send to a transcriptionist leaves your organization. For example, do you e-mail it to your vendor? Do you mail it? Do they pick it up? Next: Nail down the best ways your vendor can protect the information in whatever form they receive it. Do this for each step your patients' PHI takes in the transcription process, Upleger suggests.

For guidance on creating a questionnaire that will work for your organization, check out an excerpt of Vanderbilt's vendor security form later in this issue.

Announce Your Terms Up Front

Before you turn your patients' PHI over to a transcription company, you must ensure that the company understands and agrees to your contract based on your terms, Upleger notes. That way, there will be no confusion if the vendor violates the contract.

Here are some of the terms you should define up front:

•-Turnaround time requirements on all document types;

•-Standard document codes;

•-Charge penalties for late or lost documents;

•-Notification requirements for lost documents;

•-Accuracy requirements;

•-Required applications and interfaces;

•-Tracking and auditing requirements;

•-Physical security standards.

How to proceed: Attach an explanation of your terms to your business contract. When your vendors sign and date the contract, they acknowledge that they will abide by your terms -- and that they understand the chain of communication they should follow if there is a problem, stresses **Stephen Priest**, a security consultant with Professor Steve & Associates in Bedford, NH.

Smart: Provide a contact list in your document that notes the names, departments, telephone numbers and e-mail addresses of key staff members in your organization, Priest offers.You could also provide a sample scenario of when the vendor would contact each person. See the box below for an example to help you get started.

Attack Encryption Head On

Encryption is the most debated -- and potentially expensive -- non-required standard in the security rule, but that doesn't mean you should automatically rule it out, especially if you accept transcribed PHI via e-mail, says **Frank Ruelas**, compliance officer for Sacaton, AZ's Gila River Health System.

Your risk assessment will determine whether you should fork over the cash required to scramble your incoming and outgoing e-mail messages, Ruelas points out. If there's a high risk that the messages could be intercepted, not implementing an encryption solution is hard to justify, he says.

But until you can apply a robust encryption method, experts offer these techniques for keeping your e-mailed messages secure:

•-Do not include PHI if you do not have to;

•-Only include the minimum amount of-PHI necessary;

•-If you must send PHI, attach it to your e-mail-as a password-protected file;

•-Let your recipient know when and how you-plan to send the PHI and what the password he-should use;

•-Ask your tech team to set up a notification-system to alert them if an attached file is blocked-at the server level so that you can approve it.

Caveat: Your encryption and alternative e-mail protection methods will only succeed if they are mirrored by your vendors, points out **Mark Eggleston**, HIPAA compliance program manager for Health Partners of Philadelphia.