Codify
BY AAPC

Health Information Compliance Alert

Security: Use 5 Tips To Ensure Your HIMS System Makes The Security Rule Grade

Your management system is crucial for security rule compliance.

Can your health information management system (HIMS) carry out your security rule compliance? Even if you answered 'Yes,' now is the time to look into an upgrade. Luckily, you don't have to go it alone. Our top security experts tell you what you need -- and what to avoid.

Save Those Pennies

Upgrading your current HIMS to one that can help you efficiently comply with the security rule doesn't have to cost a fortune, says **Dennis Bagley**, manager in the **Technology Consulting & Solutions** practice at Plante & Moran in Southfield, MI. "Five or 10 years ago, you were looking at millions of dollars [for security upgrades]. Things are affordable now," he surmises. And with a strong information management system, "you can expect a huge return on investment," he adds.

Gag Your Gurus

While your IT manager or technical support team needs to facilitate the process, they have to step back and get the clinicians involved, Bagley recommends. "They'll be the ones using the system, so they have to buy into it," he stresses.

This means "the process must be driven by what features and functions those users need on the system," Bagley notes. And because most clinicians don't know what the options are, "you have to educate them," he says.

Find The Fab Five

There are five basic components that all HIMS must have, details **John Parmigiani**, senior VP for Consulting Services at **QuickCompliance** in Avon, CT. Without these key features any HIMS is doomed, he says.

1. Access Controls: "You have to be able to identify users," Parmigiani reminds. Without access controls, your patients' PHI is readily available to unauthorized viewers.

Beyond identification, your HIMS must also allow you to assign privileges. "You have to define roles within the system and indicate specific areas that those roles can access," Bagley clarifies.

2. Authentication: Design your system to demand that all users prove who they are, Bagley advises. There are multiple ways for this to happen, including passwords, personal identification numbers (PINs), biometric technology, digital certificates and tokens.

Important: Most vendor systems are based on single-factor authentication, but your HIMS should rely on multiple-factor authentication, Parmigiani counsels.

Example: Rather than only asking for a password when users attempt to login, your system could ask them for a password and a PIN. This is especially crucial if you expect any users to login to your HIMS from their homes or other remote locations, he explains.

3. Integrity Controls: Any access and authentication capabilities are pointless if you can't determine whether users are creating or modifying your patients' PHI. Your system should have "built-in integrity controls that alert you if data has been altered," whether the change was intentional or not, Parmigiani says.

This feature becomes most important when you begin working with electronic medical records, experts warn. Any modifications or false data that slips onto a health record could cause significant problems in the patient's treatment, Bagley affirms.

4. Audit Controls: These controls should work seamlessly with integrity controls to ensure the security, privacy and accuracy of patient information, Parmigiani explains. By recording and examining all the activity on your HIMS, you can see "who tried to access what and what they did," he tells us.

Remember: Your system's audit controls don't replace those built into your applications, Parmigiani cautions. Use both layers of tracking so that you can see not only who logged in to your applications, but also what that user did once inside.

5. Transmission Security: You have to make sure that your patients' PHI is always secure -- whether it's at rest on your system or in transit across a network. This feature combines integrity and accountability, Parmigiani explains, because it protects patient data from unauthorized viewers and can openly show both who sent it and who received it. Encryption is the most popular and cost-effective method of security data transmission, experts agree.

The Future

Once you have your five basic components in place, you can pick and choose secondary elements like time-outs or privacy screens, Parmigiani says.

Most important: If all practice HIM systems conform to these common denominators, the move to complete electronic records and increased use of health information technology will be painless, Bagley says.

First step: Be an informed buyer, Parmigiani advises. You have to know exactly what you want from a HIMS. Otherwise, you could wind up with a system that meets neither your practice's needs nor the security rule's mandates, Parmigiani warns.