Codify
BY AAPC

Health Information Compliance Alert

Compliance: Look Out: Watch Out for These HIT Pitfalls, OIG IT Audit Director Advises

Tip: Change your passwords... often.

You're familiar with Medicare audits and even HIPAA audits - but have you ever heard of a health information technology audit? If not, get to know the specifics of how the government performs these and what it's seeking. During a recent OIG podcast, the OIG's IT audit director, Jarvis Rodgers, provided some specifics about the latest trends in health IT and how you can avoid getting into trouble. Read on for highlights.

Health Records Worth More Than Gold to Thieves

Protecting a patient's health records may seem like it's just another government requirement that has no rhyme or reason behind it, but the reality is that health records can be immeasurably valuable for thieves.

"Health records can fetch, sometimes 60 times more than what a stolen credit card can yield on the dark web," Rodgers said. "Whereas credit cards may have a shelf life, if they're compromised, of just a day or two, health records tend to last a lifetime. So I think it's important for folks to really protect their health information, to be aware of who has their health information, and recognize that, if your health information is compromised it could also result in things like someone filing a false tax return on your behalf."

To ensure that this information is under lock and key, the OIG investigates how carefully practices, hospitals, insurers and other entities are protecting those medical records, he adds. Therefore, if you haven't yet performed a healthcare IT risk assessment, now is the time to ensure that all of your patients' protected health information is secure and impenetrable.

Have You Changed Your Default Passwords?

One way the government ensures that patient records are secure is to attempt to access them, much like a hacker would. "Penetration testing is another area that we're extremely proud of," Rodgers said. "We're able to provide chief information officers, and sometimes chief financial officers, with information where we have exploited a particular vulnerability, and we've actually been able to get into a network."

While performing penetration testing, OIG auditors review specific items such as whether the entity changed the out-of-the-box usernames and passwords that the manufacturer created, Rodgers said. If those default usernames and passwords are still in effect, then the system is vulnerable to hackers. Practices that have out-of-the box software in their offices should be sure and check whether they have changed these passwords, and if not, you should do so immediately.

Resource: To read more about the OIG's work on IT audits, visit https://oig.hhs.gov/.