

Health Information Compliance Alert

Protect Your Practice HIT from Invasion

Hint: Don't ignore patches and updates.

When you set up boundaries against cyber attack, you do the triple duty of defending your patients, complying with the HIPAA Security Rule, and protecting your hard-earned cash.

Wake-up call: The WannaCry ransomware attack was aimed at folks who hadn't updated their software and, not keeping up with the latest software patch ended up being a liability.

"Healthcare has traditionally been less sophisticated when it comes to information security ... [but] now is the time to get serious about protecting systems, because lives and institutions are at stake," warns HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, VT.

Consider this: The first step in healthcare security is following trends and engaging certified IT staff who know how to keep your practice in the tech loop. Here are a few pointers that will discourage a ransomware takeover of your servers:

- Update your software when it prompts you to instead of letting it lag behind. Cyber criminals will try to sneak in when your guard or programs are down.
- Back up your files to an external hard drive.
- Take advantage of cloud-based technologies and storage, preferably with a verified third-party vendor with experience in HIPAA security.
- Check logging and monitoring records of your networks often.
- Don't open emails from unknown sources and if you suspect phishing or any other kind of social engineering, alert your IT director immediately.

Tip: The OCR offers a monthly update with its Cybersecurity Newsletter, which highlights what's impacting healthcare's IT each month. The report indicates the biggest monthly cyber challenges the feds are troubleshooting with official assistance and violation reporting guidance.

Resource: To look at May's issue of the OCR Cybersecurity Newsletter about WannaCry, visit <https://www.hhs.gov/sites/default/files/may-2017-ocr-cyber-newsletter.pdf>.