Health Information Compliance Alert

Toolkit: Pocket This Expert Network Advice

Manage your patch updates wisely.

In healthcare, no matter your size and scope, you are still vulnerable to cyberattacks. And because of the sensitive nature of electronic protected health information (ePHI), organizations big and small must take care to protect their patients and themselves.

Whether your organization is part of a multi-state enterprise or rural physician practice, there are things that management and staff can do to prevent digital mayhem. "There are a lot of fairly inexpensive security controls that can and should be implemented by organizations regardless of how small they are," advises **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah.

1. Hire a Vetted Expert to Manage Your Networks

The HIPAA Security Rule requires covered entities (CEs) to "designate a security official who is responsible for developing and implementing its security policies and procedures," reminds the **HHS Office for Civil Rights** (OCR) summary.

"If you can't afford a full-time person or team dedicated to security controls, consider engaging a managed service provider," Stone says.

2. Protect Your Practice With Encryption

Encryption needs to be part of your multi-layered office security and is a mechanism that obscures information from unauthorized users.

"Encrypt ePHI when stored and during transmission," instructs Stone. "Encryption is not expensive but it can require some expertise to properly apply it. Implement access control so that only authorized individuals can get to ePHI."

Plus: It's a good idea to include encryption in security training and give anecdotal evidence to show staff what can happen when data is not encrypted.

3. Install Firewalls to Shut Out Intruders

A great way to block out unauthorized users is to install a firewall that monitors your network traffic.

More importantly, "configure firewalls so that only people inside the network can access ePHI," Stone maintains.

4. Keep on Top of Patch Management

When you bypass, ignore, or delete software updates, you run the risk of leaving the door open for hackers. Cyber thugs scan for vulnerabilities day and night - moreover, healthcare entities remain a favorite target. Managing bugs, glitches, and patches is crucial and keeps intruders out, safeguarding your patients and your reputation.

"Network server infiltration often happens because of easily preventable means," Stone says.

"One of the most common preventive measures is patching - applying vendor security updates in a timely manner," she counsels. "Security updates are important because they 'patch' known vulnerabilities."

5. Update Your Operating Systems

It is essential that practices not only implement anti-malware solutions, but that they keep track of old products, outdated software, and shoddy devices.

"Vulnerabilities are targeted by malware and exploited by hackers to get into organizations' systems,” says Stone. "In the healthcare industry, I see a lot of devices that have older operating systems that have hit or will soon hit end of life (EOL). EOL is when security patches are no longer being released by the vendor. ”

She continues, "Remember how hard WannaCry hit NHS machines in the UK? It was because they had so many Windows XP machines still in service, which were no longer receiving security updates. But even when organizations have machines that are still fully supported by the vendor, I see a lot of healthcare providers with unpatched machines. This is often due to lack of resources, lack of knowledge, or lack of policies and procedures telling someone in the company they have to patch everything regularly or be held accountable.”