Health Information Compliance Alert

Remote Work Compliance: Bolster Your VPN Security With This Insight

Tip: Make password management a priority.

Whether your organization has been part of the pandemic-inspired, remote-work renaissance or you're considering allowing your employees to work remotely now, they'll need to be able to access important information to cross items off their to-do lists.

"As more users work remotely and need to connect to the internal network and systems, virtual private networks (VPNs) make this possible by providing secure connectivity," says **Funso Richard, CISA, CISM, CDPSE, CCSFP**, information security officer, Ensemble Health Partners, in Cincinnati, Ohio. VPNs are incredibly important to establishing a secure external connection from an employee's device to a healthcare organization's internal network and data.

However, like many technologies, VPNs have their own vulnerabilities, which include:

- **VPN misconfiguration:** A misconfigured VPN can allow an unauthorized connection to an organization's internal resources, which can cause a data breach or ransomware infection.
- **Missing patches:** Promptly applying software and security patches to your VPN when the patches are available helps safeguard against threat actors attempting to exploit vulnerabilities.
- **Endpoint connections:** VPNs do help protect the network, but the protection doesn't apply to the endpoint connecting to a healthcare internal system through the VPN. In other words, the VPN protection ends at the user's laptop, tablet, or other devices. Healthcare organizations should enforce security controls on any device (endpoint) that will connect to the internal network through the VPN.

Create Complex Passwords to Safeguard Your Resources

Passwords are an essential piece of the puzzle to keeping access to protected health information (PHI) and user accounts safe from unauthorized access and disclosure. However, too many users are unaware of or are negligent of proper password policies. In fact, "80 percent of data breaches in 2021 occurred because of weak or reused passwords," Richard says. "The stronger a password is, the better protection it affords," he adds. A user's password should be complex and lengthy, which makes it harder for a hacker to figure it out.

Tips for creating a secure password include:

- **Do:** Make your password a minimum of 12 characters with capitals, lowercase, numbers, and special characters.
- **Do not:** Use eight characters or less, dictionary words, trending paraphrases, pet names, or other easily guessable terms.

There are several factors that encompass stellar password creation and management. A strong password is an excellent step in protecting your healthcare organization's data, but multifactor authentication (MFA) adds greater security. Used together with the user's password, MFA adds extra layers of protection to the sign-in process, so the user can be securely granted access to internal resources. Depending on the MFA application, the user may need to supply a password or personal identification number (PIN), a badge or smartphone, or biometric verification (fingerprint).

For example, your IT team could configure VPN connectors to request MFA before establishing a connection with internal systems. This will help ensure the correct device is making the connection while also securing the endpoint connection.

Get Everyone on the Same Page

Before your remote staff log in to the VPN, IT staff must ensure not only that remote patient monitoring (RPM) devices are secure before they go home with patients, but also that your workforce understands what's at stake. A solid password policy with MFA should be in place before your employees can work from home. Additionally, protocols should be instituted to bolster compliance and digital vigilance, protecting your organization's internal network and data - and your patients.

"The toolkit of the hackers is fairly sophisticated and constantly changing," cautions **Eddie Hearns, MA, CPMA, CPC**, Approved Instructor, of OLDME CPC LLC. He adds that the ideal strategy for any organization is to establish a strong business continuity plan. In addition to regular backups, strong network security, and cybersecurity policies and procedures for staff to follow, a business continuity plan should include plenty of training to ensure everyone in the organization is aware of a hacker's tricks