HIPAA Compliance and Remote Employees

The health of patients continues to be a priority for everyone in the healthcare industry. This health also extends to patient data and keeping information that could be used to harm patients in the future safe and secure today.

Working with network administrators to create a robust and comprehensive WFH policy will ensure that patient data and organization-related data is safe and employees can focus on giving their patients the best services possible.

Working remotely has become the new normal for many industries, healthcare included. Outside of the first responders, medical practitioners, or specialists in hospitals and healthcare facilities treating patients, there are other departments who provide services to patients. These employees routinely have access to personal health information (PHI), and are working to ensure that any follow up care, additional services, or even simple patient record keeping is updated and protected following the strict HIPAA guidelines.

HIPAA Violations in the Real World

In October of 2020, City of New Haven agreed to pay HIPAA violations up to $200,000 for a failure to terminate network access and credentials of a former employee. The investigation found that an employee was able to log into their account eight days after termination and access patient personal information. It also found that this employee shared their login and password information with an intern who was routinely using it to access patient information.

Also in October 2020, Aetna agreed to may $1 million dollars in HIPAA violations after it was determined that plan-related documents were accessible without login credentials and subsequently made searchable by various internet search engines, affecting 5,002 people.

Other examples of HIPAA violations include stolen devices, social media posts and video commentary, as well as delays in practitioners providing their patients with medical records.

While these instances may seem few and far between, HIPAA violations are at a higher risk of happening now, while more employees are working from home, than ever before.

How to Remain Compliant When Working From Home

Administrators, now more than ever, need to remain vigilant against HIPAA violations and how easily these can happen while so many employees are working from home. Listed below are key considerations that administrators, along with their IT teams, need to make moving forward:

Make VPN Mandatory

Virtual private networks, or VPNs, extend the same protections and policies that employees receive in the office to the home when properly connected. Using VPN connectivity can create a shield around incoming and outgoing traffic from remote devices, keeping all communications encrypted and secure.

Maintain Complete Network Activity Reports

Network administrators should keep an updated list of every employee working from home, devices attributed to them, and the level of network access each person has. This level of detail, paired with network activity reports, can be extremely effective in noticing suspicious activity and closing the loop when employees leave any organization.

Continuous Employee Training

Keeping employees informed about what phishing emails, suspicious links, or other overall cyber security policies are in place will go a long way during this time. As employees continue to adapt, work from home, and serve patients in need, they may often overlook glaring red flags in emails that have malicious intentions. Train employees to notice suspicious activity and report it to the proper channels before it becomes an out of control cyber attack.

Enforce Clean Password Hygiene

With employees working from home and in constant contact with sensitive personal information, keeping passwords secure is paramount. Passwords for home networks should be changed monthly, using strong passwords - combinations of characters, symbols, and numbers that cannot easily be guessed. In addition to updating home network passwords, login credentials, laptop passwords, and other password-specific applications should also be changed monthly to ensure that they do not lapse or can be easily accessed.

Deploy Multi-Factor Authentication

MFA, or sometimes known as two-factor authentication (2FA), can add an additional layer of defense to any login or credentialed-access portal. This additional authentication asks for either a text message, secondary email, or other form of access confirmation, and most times this cannot be faked by hackers. In addition to another layer of authentication, this can also be the first warning that someone is trying to access an account. If you receive an email asking for confirmation or an access code, it could be a signal that someone is trying to access another account of yours without being authorized.

Sources

https://www.hipaajournal.com/hipaa-violation-cases/

https://www.totalhipaa.com/hipaa-compliance-working-remotely/

How Arista Can Help

Arista's Cognitive Unified Edge (CUE) solutions help enable school IT administrators to monitor, protect and control their networks while also providing protection from evolving threats. CUE products provide enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Block students from accessing inappropriate content
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for learning
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Network Security for Healthcare

- Stop viruses and other malware before they can enter the network
- Integrate with existing Active Directory/LDAP to bring preconfigured user context into your organization
- Set up different policies to control Internet access tailored specifically for doctors, administrators and other medical staff
- Identify every user on the network with Captive Portal to allow access to network resources only to those that require it
- Filter web content based on different types of users from medical staff to visiting patients with user policy based web filtering
- Prioritize mission-critical applications that directly affect the level of care provided to patients
- Prevent network slowdowns caused by any individual or group of users and applications

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989