CREATING BALANCE BETWEEN CLINICIAN NEEDS AND CYBER SECURITY POLICIES

Marissa Maldonado, IT Systems Project Manager| Coker Group

One of the original benefits of the healthcare industry's migration to Electronic Health Records (EHRs) was to more easily share Protected Health Information (PHI) in order to better serve the patient. Unfortunately opportunistic groups of cybercriminals have discovered profitable margins when they become part of the information supply chain. Cyber security breaches are increasing in frequency at an epidemic rate. It is no longer thought of as an "if it happens" scenario but "when it happens" scenario. As cyber security policies become more complex in order to protect PHI how does a practice promote a culture of compliance without the policies disrupting the quality of care?

Similar to any culture shift within a practice, you first need to develop a strategy on how to identify existing IT security exposures and weaknesses. Seek out third party cyber security experts who will utilize tools on your network to evaluate how secure your network is from the outside and the inside. These assessments are known as white hat or ethical hacking practices. A few of the key components include network penetration testing, HIPAA security audits, social engineering testing, and email phishing attacks. Based on the analysis of these results you will be able to create firm network risk assessments and the steps to address vulnerabilities.

The second phase involves creating a living framework of cyber security policies and procedures for your practice. What is your policy if your environment falls victim to ransomware? Do you pay the ransom or restore from backups? When are you legally liable to report security breaches? Do you have cyber security insurance? What exactly does your insurance protect you from if there is a data breach? What is your "acceptable use" policy for end users? What is your password rotation policy? How do you ensure sessions on systems are deauthenticated once the clinician walks away from the workstation? How are you enforcing these policies?

When all is said and done, reports are analyzed, new cyber security policies and procedure handbooks are signed by staff how do we ensure we maintain a balance between the quality of care and security compliance? A 30 second security disruption 40 times a day 5 days a week starts to add up for a practitioner. How do you prevent the creative workarounds which offsets the culture of security compliance? For example, it's an all too common occurrence to find post it notes around practices with passwords into systems or different users using the same login for a workstation to prevent the hassle of signing in and out. The possibilities are endless in which clinicians and staff design creative workarounds because they see cyber security as a hindrance in providing fast quality care.

In order to create the balance between clinician needs and cyber security policies we must create a culture of compliance from within the practice. We need to ensure firewalls are current, computers are actively patched, passwords are rotated, backups are reliable, servers are maintained, and wireless networks are secure. These components for a secure and compliant network are obvious and important. Equally important but often overlooked is the continuous education of every end user who is actively in your system. Think of the cyber security policies and procedures like a home security system. You can lock your doors, install cameras and motion detectors, have an active security monitoring system, and perhaps even a guard dog to protect your home. But how do you protect yourself from the person who walks up to your door and knocks on it and is let in by your unsuspecting daughter? The majority of ransomware attacks on networks come from email attachments and links that find a way past firewalls and entice users to execute the malicious code. Each user must understand that in order to provide quality of care to the patient we must also be vigilant in protecting the information we have on our patients. By creating the balance between the users and their cyber security policy and procedures, the measures to protect the network will be seen as an enhancement not a deterrent to providing quality care.

To learn more about Cyber Security, Network Risk Assessments, Cyber Security Cultural Training, or Managed IT and Security Services, please contact Marissa Maldonado, IT Systems Project Manager at mmaldonado@cokergroup.com by calling 678-832-2021.