EARNEY & COMPANY L.L.P.

Physician Advisory Update: Get a Qualified & Independent Lens on Cybersecurity & HIPAA …In *and* Out of the Cloud.

Robert Duggan, CPA, CIA, CHC, CISA, CISSP

Regardless of how your practice utilizes the cloud for EHR hosting or your computing network infrastructure, there are critical elements which must be assessed and monitored on an ongoing basis to avoid system compromise or breach and limit the damage if an event occurs. A few key things to remember:

- Ransomware and breach are serious ongoing care delivery / business interruption risks for practices of all sizes, regardless of IT infrastructure and where the EHR is hosted.
- A cloud based EHR does not completely insulate a Physician practice from these threats. A network interruption from a ransomware attack can still paralyze operations and result in a reportable breach due to stored EPHI in reports residing on local machines (or other storage practices).
- Cloud-based EHR application data storage locations are known ransomware / cyberattack targets.

Attacks on Cloud Technology Providers grew by 630% in the first 4 months of 2020 alone (McAfee). The percentage of malware delivered using cloud apps topped 61% in 2020, and Cloud apps are now the target of 36% of all phishing campaigns according to netskope.

More recently, the attacks on Aprima EHR's storage provider MedNetworx led to weeks of outages for Providers using the Aprima EHR (HealthcareITNews).

A Coastal Carolina Surgery provider has recently endured the 2nd largest Carolinas Provider breach in 3 years and is now subject to class action lawsuits, penalties, and extensive breach remediation costs.

85% of Carolina Healthcare Provider *HIPAA reportable breaches* from November 2019 through August 2021 were Hacking / IT Incident related per review of the OCR website.

As of July 31, 2021, *reported* information security breaches to the NCDoJ are trending to nearly double 2020's 1644 cases, 85% of which were related to hacking and phishing. Based on our discussions with the NC DoJ, these numbers are *only a fraction of actual breaches*; many are not reported due to legal liability and reputation concerns. Failure to report a breach can lead to extensive civil and criminal liability at the state and federal levels. Failure to report is discovered by privacy complaints to NCDoJ (State) and OCR (HIPAA Complaints). The best thing to do is to take reasonable steps now to ensure security and privacy.

The good news is that risks from these potential exposures can be mitigated with reasonable steps:

Physician's Cybersecurity & HIPAA Advisory: Key Elements (details next page)

____Perform a Diligent Information Security / Cybersecurity Risk Assessment Annually Using a Reputable and Qualified Cybersecurity and Compliance Professional

____Perform a Vendor Security Review including review of SOC 2 & Business Associate Agreements

____Independently Assess & Secure Monitored Networks and Endpoints

____Perform Frequent Cybersecurity Awareness Training and Simulated Spear Phishing for Maintaining Employee Awareness & Acuity

____Ensure Robust & *Secure* Data Backup and Recovery Processes in Place

____Ensure Effective Cybersecurity Insurance is in Place and *Secured* *(what do I mean by that? Read on…)*

1. Perform a diligent information security / cybersecurity and privacy risk assessment annually. Use a reputable & technically qualified cybersecurity and healthcare compliance personnel *independent* of your IT Provider to help ensure success and breach avoidance, as well as help your practice ensure quick information recovery and lower cost in the event a breach occurs.

   Ensure best practice cybersecurity controls and monitoring is in place. It is contrary to reason that your IT provider would be able to provide an objective assessment of their own controls for your HIPAA security risk assessment. Similarly, using a HIPAA compliance group to assess may leave you with a checklist-based approach performed by a semi-retired clinician or healthcare administrator that does not sufficiently address cybersecurity risk.

   Using an experienced and certified professional with cybersecurity, healthcare technology, and compliance background will help you ensure your cybersecurity controls protect the networks and patient data, and that your patient privacy effort is compliant.

2. Perform a vendor security review including review of SOC 2 & Business Associate Agreements. It is critical to review security audit reports and agreements for key vendors processing EPHI. Failure to document the understanding of vendor security controls and "justifiable reliance" could result in being held liable in the event of a vendor breach of your patient records.

3. Independently assess & secure the network and endpoints. We are in a different environment now than we were 5 years ago. Campaigns from hostile actors are often utilizing file-less attacks which *do not have detectable signatures*. A firewall and antivirus software are no longer enough to protect your network. Endpoint Detection and Response (EDR) security applications should be deployed to monitor computer and user activity. Even if you are hosting your network in the cloud, it is still important to ensure monitoring and logging of network traffic and that EDR applications are watching local user endpoint behavior 24/7 using deep learning or AI technology.

4. Perform frequent cybersecurity awareness training and simulated spear phishing for maintaining employee awareness and acuity. With the predominance of zero-day and file less attacks, it is critical to ensure that the workforce remains keenly aware of spear phishing attempts and knows not to click on anything coming from outside the practice unless they are familiar with the sender address. We also note the improved effectiveness of external spam / antimalware filters and anti-malware email protection that now scans email link content once when it comes in and again before it allows the user to open the link. This is a crucial feature in the current environment.

This document is intended as a reference tool to assist in understanding and addressing concentrations of cybersecurity risk to your Practice. It is not intended to be used as a comprehensive cybersecurity or HIPAA risk assessment guideline.

5. Ensure robust & *secure* data backup and recovery processes are in place. It is critical to ensure your data is backed up regularly and features point-in-time recoverable & secure instances. Ensure your provider is completely test restoring your backups on a periodic basis.

   Recoverable and secure point- in-time backup instances are crucial in the event of a successful ransomware attack. If the Practice is unable to decrypt the ransomed data, the point-in-time recovery ability can enable the practice to roll-back systems to a date prior to infection (following cyber-forensic log review) for minimal business interruption.

6. Ensure Effective Cybersecurity Insurance is in Place and *Secured.* The rider on your general liability policy for cyber is not enough. You need to ensure your separate cyber insurance policy covers any fines, legal costs, data recovery / ransom payment*, breach remediation costs, and civil liability in the event of a breach. To secure your policy, it is important that you fill out the questionnaire the insurer provides 100% accurately. Failure to do so could result in non-payment of coverage amounts. The idea of not worrying about security and relying on cyber insurance is a myth. If you don't have the stated controls, the policy is unlikely to pay out. These checklists can be exhaustive, and the best way to ensure compliance with them is an independent assessment of your controls. Getting the correct controls in place can also help your premiums; ask your insurance provider.

   We do not advocate the payment of ransoms or over-reliance on cyber insurance, as it perpetrates a $1.5 Trillion-dollar criminal industry, and as mentioned above, the policy will not likely pay out if stated controls were not in place at the time of the breach. Instead, ensure information security controls are in in place which ensure resilience and roll back capability in the event of an attack. Also, most cyber policies do not cover business interruption, and none cover the reputation damage.

In closing, risk-assess your cybersecurity and compliance posture with a qualified cybersecurity and privacy professional annually to understand the design effectiveness of cybersecurity controls in place and ensure reliance on key technology vendors is justified. Be sure you understand who is responsible for each critical element of your security posture and related support agreement terms. Understanding and improving these elements will not only reduce the risk of successful attack or breach, but it will also enable greater resilience and a contained incident response in the event of compromise.

Earney Technology Risk Advisory Services is a Team of 6 highly qualified professionals with over 60 years of combined experience in information security, and we are here to help.

Rob Duggan leads Technology Risk Advisory Services for Earney & Company. Rob has over 20 years of information security audit experience including 7 years serving national healthcare organizations as Internal Audit and Compliance Officer and 10 years of international audit in over 25 countries. Rob is a Certified Public Accountant, Certified Internal Auditor, Certified Information Systems Auditor, Certified Information Systems Security Professional, holds a Certificate in Healthcare Compliance, and is a graduate of NC State University. Rob is a frequent speaker on cybersecurity nationally & within the Wilmington professional community, and serves on the Board of Advisors for UNCW's Center for Cyber Defense Education.

For additional information on Earney Technology Risk Advisory capabilities, please visit us at: Information Security & Privacy | Earney & Company, L.L.P. (earneynet.com)

This document is intended as a reference tool to assist in understanding and addressing concentrations of cybersecurity risk to your Practice. It is not intended to be used as a comprehensive cybersecurity or HIPAA risk assessment guideline.