Is the Cloud Safe?

By

It seems that another cyber attack is in the news every week. Cyber criminals are trying to acquire personal information at an alarming rate, and the healthcare industry is a particular target. Patients' protected health information (PHI) often contains birthdates and social security numbers, and is in high demand by identity thieves. Many practices are utilizing cloud-based Electronic Health Records (EHR) and relying on the security provided by the vendor to protect their records. Unfortunately, cyber criminals continually work to crack the most sophisticated security, and PHI may be vulnerable if the vendor has a security breach.

Here are some real-life examples from SVMIC files:

- A practice was informed by a practice management software vendor that the vendor had sustained a ransomware attack. The practice could not use the software for about a week, causing a significant disruption of service.
- The IT Manager and HIPAA Security Officer at a medical practice were informed by its pharmaceutical software vendor that it had been attacked with ransomware. The practice discovered that they did not have a Business Associate Agreement.
- A medical practice was notified by their EHR vendor via a letter that the practice's EHR program "experienced unauthorized access to certain accounts on a specific group of data servers."
- A practice's medical records were frozen for 5 days. The practice uses a cloud-based service through a software vendor that had been subjected to a ransomware attack.
- A medical practice maintained all EHR on a cloud-based system. The vendor shut down access to their system due to a ransomware attack. The practice had no access to its EHR. The vendor advised that no PHI was compromised, but the practice was concerned about possible HIPAA breach and reporting obligations.

Utilizing a cloud services provider (CSP) for an EHR system does not relieve a medical practice from Health Insurance Portability and Accountability (HIPAA) compliance requirements and does not necessarily protect the medical practice if the vendor experiences a cybersecurity breach. A healthcare provider transmitting PHI electronically is considered a "covered entity" under HIPAA guidelines and is required to comply with the applicable provisions of the HIPAA rules. A practice's business associates are also required to be compliant with HIPAA regulations.

According to the Health and Human Services (HHS) website, the HIPAA Privacy, Security,

and Breach Notification Rules establish guidelines for *PHI* when "created, received, maintained, or transmitted by a HIPAA-covered entity or business associate." HHS defines a "*business associate"* as "an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI."

Choosing the right cloud based EHR vendor is an important step in helping to keep electronic protected health information (ePHI) safe. In an article titled "10 Things to Look for in a Cloud Data Backup Service" the author, Sara Angeles, indicates there are several questions to ask when looking for a cloud-based vendor. In addition to regulatory compliance, learn how frequently the vendor backs up data. The more frequent, the better, especially when trying to recreate lost data. Find out where the information is stored – locally, off-site or both, and if the data is encrypted while being stored and while being sent to and from the server. Access to your medical records is critical; ask what measures the vendor takes to protect their servers as well as asking for their disaster recovery plan. The practice should be able to access the records offline if necessary in the event of a crisis, whether electronic or a natural disaster.

The HHS website recommends a Service Level Agreement (SLA) be used when a medical practice utilizes a CSP to create, receive, maintain, or transmit ePHI in order to process and/or store that ePHI. HHS indicates that an SLA "is commonly used to address more specific business expectations between the CSP and its customer, which also may be relevant to HIPAA compliance." HHS recommends that the SLAs contain provisions that address HIPAA concerns such as:

- System availability and reliability;
- Back-up and data recovery (e.g., as necessary to be able to respond to a ransomware attack or other emergency situation);
- Manner in which data will be returned to the customer after service use termination;
- Security responsibility; and
- Use, retention and disclosure limitations

The medical practice should ensure that the terms of the SLA do not prevent the entity from accessing its ePHI. You can find more information regarding guidelines and compliance at the Health and Human Services website.

Cyber criminals will not stop trying to access personal information, no matter where it is stored. Choosing a vendor that is compliant with regulations, employs security measures such as encryption and frequent backups, and provides an alternative access to records are ways to secure your patients' records when working with a cloud-based EHR vendor.

Your medical professional liability policy with SVMIC includes $50,000 of cybersecurity coverage to assist in mitigating the damages associated with a security breach. Through our partnership with NAS, higher limits are available for purchase at discounted premiums. The cost for additional coverage is based upon the limits chosen, group size and other

factors. SVMIC and NAS have jointly implemented a web resource to offer cyber-specific support and risk management to policyholders. The website will offer an extensive collection of training material, sample policies, various risk management tools, and access to webinars on timely topics. Expected to be available before the end of 2017, the new resource will be accessed on the SVMIC Cybersecurity Resource page.