IT MANAGEMENT SOLUTIONS
Focus on your business, we focus on your technology

EGUIDE – SERVICE PATIENTS, NOT TECHNOLOGY: ACHIEVING HIPAA COMPLIANCE & HIGH LEVEL DATA SECURITY IN THE CLOUD

Created for Pedro Nunez

Service Patients, Not Technology: Achieving Hipaa Compliance & High Level Data Security In The Cloud

Prioritizing Security & Privacy in Healthcare Sector

Physician offices, hospitals and health insurers take practical steps each day to protect private patient health information (PHI) and comply with HIPAA regulations. Anyone interacting with patients and regularly accessing or discussing confidential medical records is obligated to adhere to certain requirements to uphold privacy and security.

For example, employees must be mindful of what is said aloud pertaining to an individual patient. Doors must be closed when patient conditions, treatments and procedures are discussed in person or over the phone. Staff should never leave voice mails with specifics about patient health conditions or test results. Even simple acts like summoning patients from the waiting room must be carried out with patient discretion in mind.

Failure to do this can result in a reported HIPAA breach that can be accompanied by potentially heavy monetary fines and often-irreparable reputation damage. The industry's need to prioritize the integrity of patient data is even more pronounced in this time of flux within the healthcare sector.

Transitioning to the Electronic Age

Healthcare service providers today are in the process of converting all paper medical records to electronic health records (EHRs) or electronic medical records (EMRs) to meet the meaningful use requirements outlined in the American Recovery and Reinvestment Act of 2009 (ARRA). The ARRA incentivizes the healthcare sector to accelerate the adoption of enterprise-wide electronic medical data by 2015 or face possible penalties.

We are entering a period in our history where volumes of confidential patient health information (PHI) will be stored, shared, and accessed electronically for the very first time ever. There has never been a more critical time for healthcare service providers to ensure that patient rights are protected, confidential information is safeguarded, and this transition from the immovable locked file cabinets to today's electronic-system is completely HIPAA compliant and secure.

How HIPAA Breaches Most Commonly Happen

The U.S. Department of Health's Office of Civil Rights found that there have been 21 million HIPAA security breaches since 2009. These breaches have resulted in an average of 2,769 records being lost or stolen per breach. Among them:

- **48% were stolen medical files**
- **48% were stolen billing and insurance records**
- **20% were stolen prescription details**
- **13% were stolen monthly statements**
- **24% were stolen patient billing/ payment details**
- **19% were stolen payment details**

During this period, 66 percent of the reported large-scale HIPPA violations were due to the physical loss or theft of electronic equipment or storage media such as a laptop or flash drive that held unencrypted PHI.

Another 8 percent of the large-scale HIPAA breach incidents were the result of hacking and cybercrime.

Physical Theft

Based on the above findings alone, one can come to the obvious conclusion that storing such unencrypted data on a physical hard drive or any portable storage media device elevates the risk of an HIPAA breach. Therefore, eliminating the need to store or transfer this data on equipment such as laptops or flash drives should significantly minimize the risk of many of the HIPAA violations reported today.

Cybercrime

Cybercrime is a growing threat within the healthcare sector since the industry has been slow to adopt new technology.

> According to the Identity Theft Resource Center, there were 17 reported financial industry data breaches in 2012 compared to a reported 154 healthcare industry breaches during the same time frame.

The aging technology commonly used by healthcare service providers is rife with software and security flaws making it susceptible to data breaches resulting from hacking and other cyber attacks.

Data thieves view private medical records as a high valued commodity - a gateway to identity theft. Safeguarding this data is challenging. With the shift to electronic records, data thieves have upped their game, finding new ways to gain unauthorized access to patient data by exposing vulnerabilities.

Defending against cybercrime requires constant monitoring for intrusion attempts and security upgrades. In this era where the volume of stored data is increasing, new cyber threats seemingly surface everyday, and there is continuous demand to comply with regulations; healthcare service providers securing their own infrastructure will inevitably become overburdened and more vulnerable to attacks and HIPAA breaches.

The Case for Moving Data to the Cloud

Although many healthcare service providers have shown a reluctance to abandon their in-house IT infrastructure and security measures, on-premise data center attacks are proving to be more prevalent, costly, and difficult to rebound from.

Healthcare providers who have resisted the cloud due to privacy and security concerns could be making a grave mistake. Increasing evidence suggests that the cloud can actually enhance data security. It does this while also freeing up manpower and budget dollars that can be better allocated toward the principle objective of improving patient care.

Decreased Instances of HIPAA Breaches Due to Physical Theft

In a cloud-based infrastructure, only the PHI that the user has accessed via their web browser resides on their computer. All other data is hosted virtually on a secure cloud-based server from a guarded physical storage facility.

Decreased Instances of HIPAA Breaches Due to Hacking

Another advantage of the cloud is that encryption requirements are better enforced, regardless of whether data is in transit or at rest. Even in the event of unauthorized access to data, the encryption key would also have to be obtained or else the data is secure and unreadable to the intruder. While data encryption is also possible when data is physically stored at an on-premises data center, it is much more difficult to facilitate.

Reduced Investment to Defend Against HIPAA Breaches

If a HIPAA breach does occur, security audits, certifications, and assessments are necessary to defend against civil or criminal prosecution. They demonstrate that the best effort was made to comply with the security requirements of HIPAA and improve your defense. They also come at a significant cost that is more affordable to cloud providers than a healthcare service provider with a private data center.

Leveling the Playing Field with Major Healthcare Institutions

When it comes to the physical and technical safeguards required by the HIPAA Security Rule, most cloud service providers implement physical security measures exceeding those practical for most small-to-medium-sized businesses. Safeguards to ensure data confidentiality and integrity are also implemented - such as advanced authentication, encryption, automated session timeouts and audibility logging – all less likely to be utilized in an on-premise data center environment.

Shared Accountability with Business Associates

A "Business Associate" is defined by HIPAA as any entity outside of your practice or organization who either performs services on your behalf or requires the use or disclosure of public health information to complete tasks they've been contracted to execute.

Until recently, some ambiguous language in the act left it up to interpretation whether or not cloud-service providers were to be classified as business associates. Although most cloud-service providers accepted accountability and signed a business associate agreement, some refused and argued that the act's definition, citing "routine regular access", didn't apply to them since they primarily stored encrypted PHI to which they neither held the key to, nor routinely accessed.

This prompted many skeptics in the industry to doubt if cloud-service providers had the processes and protocols in place to protect PHI and bear their share of accountability in the event of a HIPAA breach in the cloud.

The new HIPAA Omnibus Final Rule has clarified that any cloud data operator who maintains PHI is to be classified as a business associate. This means liability and compliance is extended to cloud data operators with a signed business associate agreement. Cloud operators are accountable, and subject to monetary fines or related fees, for any failure to protect patient data security and privacy if they sign a business associate agreement. Healthcare service providers are advised to refuse to work with anyone who still refuses to sign a business associate agreement.

Proactive Remote Monitoring

Leading cloud-service providers offer an around-the-clock remote monitoring service that maximizes uptime while monitoring each node in the cloud infrastructure, each access point, and the data center platform as a whole. This is an extremely important function that detects and addresses potential issues before they become serious breach incidents. Metrics are collected and alerts are triggered whenever faulty conditions such as a data backup failure or an authorized attempt to access data are detected.

What to Ask Your Cloud-Service Provider

As you can see, as it becomes obvious that the cloud is establishing a foothold in the industry as the data management system of choice for many healthcare service providers, cloud security continues to evolve for the better. However, you must still choose a cloud-service provider wisely and ensure that patient data is secure at all levels of workflow.

We've compiled a list of several things you should ask your cloud-service provider regarding EHRs and PHI data.

1. Who has access to this data and the systems supporting it? - Any cloud-service provider should be able to tell you who has access to the physical storage facility, the hardware, operating systems and data.

2. Is there an audit trail and can unauthorized access to patient data be easily verified? – Is there an auditing mechanism in place tracking all PHI-related system activities, warnings and failures? Any unusual system activity such as suspected unauthorized access should be easily detectable.

3. Is the data password-protected and accessible to only those authorized? – Are users prompted to enter a unique username and password with each log on? Do active logged-in sessions time out after periods of inactivity?

4. Is the data encrypted? Is it only viewable to those with proper authentication or accessing it through an application? – Is SSL-based encryption performed at the application level when healthcare sites and the data center communicate? This ensures end-to-end protection from the service access point to the data center and prevents any unauthorized network provider employee from accessing the data. Data also can't be read while in transit to an end user's viewing software over the Internet.

5. What kinds of backup processes are in place to ensure business continuity? – How often is data backed up and what is the method of backup to reduce data loss? Are copies made on removable media and stored off-site if a disaster impacts the data center? Are the two copies continuously synchronized? What authentication processes are in place to ensure data integrity?

6. How are the threats of viruses and Trojans handled? – Is there anti-virus software running every time files and disks are scanned or accessed? Is the anti-virus software frequently updated with the latest virus signature databases?

7. What Kind of Physical Security Exists at the Data Center? – Is security at the data center manned 24-hours with appropriate identification required and recorded with each visit? Are security cameras, motion detectors or alarms present throughout the facility?

Conclusion

The necessary investment to buy and maintain physical equipment, hardware and software, and supply personnel with the continuous training they need to deliver top-level data security is unaffordable and overtaxes the resources of smaller healthcare entities. Converting to cloud-based services enable practices and companies of any size to achieve industry-leading HIPAA compliant data security while benefiting from a slew of cost-efficient benefits that liberate them from security problems – bringing them back to caring for patients, not patient technology.

If you're interested in a cloud-service provider who follows the administrative simplifications referenced under HIPAA, and can satisfactorily assure the safeguarding of electronic patient health information, contact us today.

For Additional Information Please Contact
Pedro Nunez
pnunez@itmsolutions.us
T: 978-291-8125
F: 9782330580
60 Island St, Lawrence, MA