Newsletter

Celebrating 29 years serving Central, N.C.! *March 2019*

Why HIPAA Should Not Deter You From Storing Your PHI in the Cloud

Cloud-based Software-as-a-Service (SaaS) systems deliver high-value, cost-effective information services in the healthcare industry. However, many healthcare providers are not sure about how to leverage cloud computing technology while complying with HIPAA regulations for the privacy and security of protected health information (PHI). Perhaps, an understanding of and confidence in the ability of cloud healthcare solutions to satisfy industry standards and laws will see more hospitals trust the technology with the storage of sensitive patient information.

What are the Main Cloud Security & HIPAA Compliance Issues in Healthcare?

HIPAA privacy and security rules regulate PHI handling and storage, and noncompliance exposes healthcare providers to hefty fines. So, before moving their databases to the cloud, hospital chief information officers (CIOs) want security guarantees that unauthorized third parties may not access, copy, or steal patient names, Social Security numbers, medical files, financial information, and other personal data.

The Perks That Come With Storing PHI in the Cloud

Once healthcare establishments address cloud security and HIPAA compliance concerns satisfactorily, they may start enjoying the benefits of storing PHI in the cloud (some may include additional fees), such as:

- Quick data access: Hosting healthcare records in the cloud makes it quick to access them, which translates to high usability. For example, a hospital may have several cloud-hosted servers in various strategic locations close to where most of its customers are. Locating a data center close to its users helps minimize latency and improve application performance, increasing the clinical value of the stored healthcare information.
- Cost-Effectiveness: Cloud computing eliminates the need for healthcare providers to build and maintain expensive data centers and applications. Lower IT investment costs may then translate to more days cash on hand, which is great for a hospital's liquidity.
- Safe backup/disaster recovery options: The cloud is ideal for implementing disaster recovery and business continuity options.

Continued on inside

Upcoming Events

Incident Response Planning Lunch & Learn presented by TCDI
March 7, 2019

Is Cloud Computing Right for Your Business? Webinar
April 4, 2019

Cyber Security Panel Discussion
April 11, 2019

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

Continued...

- Healthcare providers can have redundant IT systems hosted in the cloud for their quick deployment in case of primary data center failure. Such redundancies are very critical to the continuity of hospital operations. Likewise, cloud-based disaster recovery measures prevent the permanent loss of PHI in the event of fire destruction, malicious/accidental deletion, or theft.

How to Secure PHI in the Cloud as Per HIPAA Privacy and Security Rules

1. Anyone who handles sensitive patient data in a healthcare organization must be aware of HIPAA rules for data information protection. Also, all personnel and parties involved in the creation, receipt, transmission, or maintenance of electronic PHI should undergo formal training to meet compliance standards. IT professionals in healthcare establishments should figure out their legal responsibilities as well as the obligations of their SaaS providers as per HIPAA rules. A secure cloud-based system for storing patient information should address the following:

- Encryption of data during transmission as well as storage
- Data ownership
- Portability of data
- Integration of information systems through APIs and open interfaces
- Protection of structured and unstructured data

2. It is also critical to conduct a compliance assessment to reveal any loopholes in native data protection strategies. How likely is it for a user to accidentally delete patient data? What is the possibility of data loss due to application integration mishaps? How safe are the hospital records from malicious insider-actions or hacking? Addressing these concerns is critical to HIPAA compliance.

3. Likewise, a healthcare organization storing sensitive patient information in the cloud should have an HIPAA-compliant backup system. Be sure to test your SaaS data protection solution to ensure it can facilitate quick and accurate data recovery. The system should support automated and on-demand backups to inspire more confidence in its ability to prevent the permanent loss of critical patient data.

Compliance with HIPAA rules in the provision of healthcare services is achievable, and it need not deter hospitals from moving their patient data to the cloud. Contact us to learn more about secure PHI cloud storage solutions!

5 Easy Ways to Make Your Client's Personal Data More Secure

Data security should be a top priority for any agency. These firms handle high-value personally identifiable information (PII), such as birthdates, social security numbers, and even health records. Should a hacker steal the data, they might use it to commit identity fraud. Therefore, as a provider, you want to secure your data in compliance with the law, and to maintain customer trust.

According to HIPAA Journal, hackers stole or accessed at least 135,060,443 healthcare records (including health plan data) between 2015 and 2018. Your organization can avoid such security breaches by taking the following five steps:

1. Know Where Your Data Is

You need to determine where your data is before you can protect it. Are you sharing your customer data with third-party providers, such as cloud services? Which datasets are you handling and storing on-premise? Next, classify your data based on how sensitive and vulnerable it may be. For example, credit card information and SSNs are high-value targets for hackers, so be sure to track and classify such data accordingly.

2. Review Relevant Personal Data Security Rules

Protect your company from hefty fines for noncompliance with several data security rules. It's in your best interest to study relevant Federal and State laws so you may figure out what they require of your agency. For instance, the Payment Card Industry Data Security Standard (PCI DSS) defines requirements for data security management, processes, protocols, as well as network and software design. Any firm that accepts credit card payments should comply with PCI DSS regulations.

Other critical data compliance mandates include:

- HIPAA/HITECH
- Gramm-Leach-Bliley Act (GLBA)
- State data breach notification requirements

3. Conduct a Thorough Cyber-Risk Assessment

It's imperative that you assess your entire IT footprint for cyber threats, including on-premise and cloud computing risks.

Identify all the network security gaps and vulnerabilities. Be sure to cover the following areas:

- Customer portals: Any interfaces that customers use to interact with your system. These include online and mobile portals.
- Endpoints: How many physical devices connect to your company's network? Identify all end-user hardware because it's a potential target for phishing, spyware, malware, or ransomware attack. The most vulnerable end-point devices are office desktops and mobile devices, such as laptops, tablets, and smartphones.
- Credit card transactions: Hackers target credit card transactional data because it includes high-value PII.
- Vendors: Be sure to investigate the security safeguards that third-parties handling or processing your customers' data have in place. It's your legal responsibility to protect the sensitive personal information you share with software vendors or cloud providers.
- On-premise systems: Hackers may target the management information system, content management system, or other on-premise software that your employees interact with day to day.

4. Train Your Employees

Cybersecurity starts with you. Also, make sure the staff understands the obligations, and they have mastered everything, from password security to data compliance. Usually, agents handle sensitive company and customer data while executing official tasks, including:

- Medical claims processing: The job involves the manipulation of protected personal health information (ePHI).
- Billing and underwriting: These processes involve the collection and maintenance of personally identifiable information, including client name and date of birth. If the customer is a patient, underwriters will capture personal health information.
- Accident/personal injury investigations: Technology helps insurers collect and preserve confidential intelligence on accident or injury situations.

5. Protect the Data

Implement robust cybersecurity measures for your organization's data. These include firewall protection for your company network, intrusion detection and elimination, and endpoint security. Be sure to encrypt all data on both on-premise and offsite servers. In-transit data also requires encryption.

The above are the fundamental steps you need to take to secure your agency's network. However, a comprehensive cybersecurity plan includes specifics that depend on your unique needs. This is where Total Computer Solutions comes in! Engage us right away for a network security assessment toward keeping your business data safe.

Digital Newsletter

If you would like to receive our newsletter digitally, please visit tinyurl.com/ycqvv2r6.

Follow us on social media!

168 Thatcher Road
Greensboro, NC 27409

In this Issue:

Lunch & Learn: Incident Response Planning

Join us for our upcoming lunch & learn!

Date: Thursday, March 7, 2019
Time: 11:45 a.m.- 1:00 p.m.
Cost: Free
Location: Guilford Merchants Association, Greensboro, NC
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449.
Presenter: Tom MacKenzie, CIPP US/E, CIPM,
Vice President, Privacy & Security Compliance

Key Topics for Discussion

- Common Breach Root Causes
- What to Consider in Preparing for Incident Response Planning
- The Anatomy of an Incident Response Plan
- Key Players and Their Responsibilities
- Critical Do's and Don'ts