Newsletter

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

Your Organization May Urgently Need a HIPAA Risk Assessment

The United States government puts strong security and privacy requirements on personal health data. These requirements come from the HIPAA act and its revisions in the HITECH act. Any covered entity that loses data due to non-compliance can face hefty fines, sometimes in the millions of dollars.

Most people think of HIPAA as applying to hospitals and doctors' offices, but they apply to a broad range of organizations that handle protected health information (PHI). An organization that falls into this category needs a risk assessment to discover any weaknesses in its procedures. Compliance takes some effort, but it's much cheaper than being hit with penalties.

The HIPAA categories

There are three categories of organizations that need to comply with the privacy and security rules:

- Health plans
- Health care providers
- Health care clearinghouses

Each of them includes entities that are not limited to direct providers of medical care.

Health plans include any business that pays medical care costs, with a few exceptions. Insurance companies that provide health insurance are the main category. Employer-run health plans are included, if they have fifty or more participants, though workmen's compensation is not considered a "health plan." All plan providers need to safeguard the privacy of the patients; they keep data on and maintain an acceptable level of security.

Health care providers constitute a broader category than the name might suggest. Anyone who sends electronic data in connection with claims, referrals, and eligibility inquiries may be considered a health care provider, even if they never examine or treat a patient. This includes medical offices that handle only the business aspects of health care. Services such as dental and eye care fall under this category.

Health care clearinghouses are a broad category that falls under HIPAA's security and privacy rules. It includes any organization that does data conversions on PHI. Examples which the government cites include "billing services, repricing companies, community health management information systems, and value-added networks and switches."

Continued on inside

Upcoming Events

Webinar: What is Lean Six Sigma?
August 15, 2019

Lunch & Learn: Is Cloud Computing Right for Your Buisness?
September 19, 2019

Cyber Security Panel Discussion
October 10, 2019

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

Continued...

They are not generally subject to the full set of privacy rules, but they need to know what is required and make sure they comply.

Business associates

Businesses that are not directly covered by HIPAA still have to keep it in mind if they process PHI on behalf of covered entities. They are called business associates, and the covered entity has to make them accept a contract that ensures compliance. These contracts will typically reference the privacy and security rules. Anyone who regularly acts as a HIPAA business associate should have a full set of compliance procedures in place.

The benefits of risk assessment

Most HIPAA breaches are not the result of targeted online attacks, but carelessness and accidents. Typical scenarios include not disposing of printouts properly and losing laptops or phones that contain unencrypted PHI. Even the possibility that the information has fallen into unauthorized hands requires reporting and remediation.

The best way to find out how well prepared you are is to run a risk assessment. An assessment from Total Computer Solutions will identify areas that need improvement and let you reduce your risk of an expensive breach.

It is not the loss of data as such, but a pattern of neglect, that brings on the really big fines. The way to avoid even the appearance of negligence is to have a well-documented set of policies and procedures. They need to specify how information is protected and what steps will be taken if a breach may have occurred.

An impressive-looking plan could have gaps in it. The best way to find them is an independent assessment. If your organization falls under the HIPAA privacy and security rules, contact Total Computer Solutions to set up a risk assessment and make sure your procedures are up to par.

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. 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.

Digital Newsletter

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

Meet Our Team: John Reece

We are excited to announce our newest Technical Intern, John Reece. John currently attends ECPI, where he is working on his B.S. in Cyber Security. He is happily married and works at UPS. During football season you can catch him watching all of the Steelers games.

FREE Guide: 3 IT Problems that May Be Costing You Money

IT is the backbone of corporate productivity. Internal email servers store confidential information about your company and clients', data loss prevention systems ensure corporate saboteurs struggle to steal your information, and internal communications keep your teams flowing freely toward achieving their combined goals.

When the system breaks, however, teams are not working together, hackers can steal your data, and your competition can close the gap more quickly. The following three issues may be signs of larger concerns within your network. We have included some potential causes of each and how they may impact your revenue.

Get your FREE copy today!
Visit tcsusa.com/resources/e-books/

Follow us on social media!

totalcomputersolutions

168 Thatcher Road
Greensboro, NC 27409

In this Issue:

webinar

Webinar: What is Lean Six Sigma?

Join us for our upcoming lunch & learn!

Date: Thursday, August 15, 2019
Time: 11 a.m. ET
Cost: Free
Presenter: Zack Guthrie, President, The Guthrie Group
Registration: Visit tcsusa.com/calendar/ or call us at 336.804.8449

The Guthrie Group, Inc

Key Takeaways:

- Understand the basics of Lean and Six Sigma
- Identify eight different types of waste
- Understand the importance of standardization
- Learn about management styles and the mechanics of change