IntelePeer®
The Cloud Communications Company

WHITEPAPER

HIPAA in the Future: What it Means to You

Peltier/CH Consulting Group

Technology advancements in healthcare pose unique challenges and opportunities for providers. With the rapidly evolving healthcare landscape, both providers and vendors are scrambling to understand the full impact new technology has on HIPAA Compliance. For the purposes of this paper we will be focusing on the HIPAA Technical Safeguards, how current and future technology is challenging HIPAA regulations, and how to protect your organization as you move into the future.

The Rules You Need to Focus on

HIPAA Compliance casts a wide net. The 400+ page document leaves plenty of gray area for healthcare providers to go astray. But there are few areas of particular concern that require attention.

Privacy Rule: The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.) PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual.

Security Rule: Deals specifically with Electronic Protected Health Information (EPHI). It defines three types of security safeguards required for compliance: administrative, physical, and technical.

Administrative Safeguards – policies and procedures designed to clearly show how the entity will comply with the act

Physical Safeguards – controlling physical access to protect against inappropriate access to protected data

Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

CHConsulting*Group*
Expert Guidance • Proven Results

WHAT IS HIPAA?

Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. The Federal Law sets a national standard to protect medical records and other personal health information.

In addition it:

☑ Provides the ability to transfer and continue health insurance coverage for millions of Americans when they change or lose their jobs

☑ Requires healthcare organizations to implement secure electronic access to health data and to remain in compliance with privacy regulations set by HHS

☑ Reduces healthcare fraud and abuse

How Technology is Challenging HIPAA

The impact of mobile devices and applications in the healthcare field is growing with both consumers and professionals. The market is being flooded with the newest applications that handle everything from tracking health statistics, real time interaction between providers and patients, to remotely accessing patient records.

With the sudden boom of these strategies come challenges. Technology is evolving faster than regulations can keep up. One of the biggest hurdles is creating healthcare applications that remain HIPAA compliant. Now with cloud technology and Software as a Service (SaaS) making its way onto the playing field, the rewards have increased.

Remaining HIPAA Compliant

In a recent survey, providers listed external threats to data as the most difficult aspect of remaining HIPAA compliant. In recent cyber-attacks, hospital databases have been breached by ransomware. In these instances, healthcare providers had to pay a ransom to get control of their data. These attacks were helped by employees opening a malware email that put a virus in place to encrypt data. Firewalls only protect so much, but marrying a strong firewall with solid employee IT practices help protect your data and your patients.

> **External threats to data are the most difficult aspect of remaining HIPAA compliant.**

In early 2016, the Office for Civil Rights (OCR) will launch Phase II of its audit program measuring compliance with HIPAA's privacy, security and breach notification requirements by covered entities and business associates. This is the next phase for the OCR audits, designed to expand out to higher risk areas, such as healthcare partners. This move shows that the OCR understands that technology is playing a significant role in HIPAA Compliance. As providers move into cloud technology and Customer Care Groups increase in size and scope, expect the OCR to focus its efforts in these areas.

Preparing for these audits, both as a partner and a provider, will minimize the risk of pricey violations.

Violations – What It Costs to Fail

Think IT security, audits, training and software upgrades for HIPAA compliance is costly? Consider the cost of violations. Not only do violations come with a hefty price tag, but organizations damage their reputation and patient trust. The cost of losing customers may be more expensive than paid fines due to a violation. Investments in network security, internal audits, and software upgrades could deem to be more cost effective. *But it's not always an entire technical system that is at fault. Often times, with HIPAA violations, it's a staff member or a process.*

In 2015, St. Elizabeth's Medical Center was ordered to pay $218,400 for HIPAA violations through an agreement with the Department of Health and Human Services' Office for Civil Rights (OCR).*

In 2012, the OCR received a complaint alleging that the Brighton, Massachusetts-based health center did not analyze the risks of an Internet-based document sharing app, which stored protected health information for almost 500 individuals, according to an announcement from OCR.

During its investigation, OCR found that the health center "failed to timely identify and respond to the known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome." In addition, St. Elizabeth's in 2014 submitted notification to OCR that a laptop and USB drive had been breached, putting unsecured protected health information for 595 consumers at risk.

This case study clearly demonstrates the consequences of not paying attention to or investing in a solid HIPAA Compliance protocol.

*http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html

How the Cloud Can Help

There are plenty of reasons to move into the cloud, not in the least the superior security it offers providers. In addition, there is flexibility and multiple locations support (the ability to seamlessly move callers from one location to the next), cost reduction, and robust data analysis, as well as ease of search functionality. A solid data storage plan allows physicians to use multiple metadata fields to quickly search and access records. The benefits far outweigh the risks.

Cloud technology mitigates some of these data breaches, storing data outside of a vulnerable server. As healthcare providers begin to utilize this new technology, choosing the right cloud provider becomes essential in keeping your data secure. Not all cloud providers are the same and in the coming year, they will be subject to the same audits that healthcare providers have been in the past decade.

Large hospital groups in particular face complex issues in data storage, but with cloud storage, data is easily accessible to all physicians, regardless of location. This eliminates costly and timely transportation of records from one facility to the next, not to mention the risks transportation of physical records pose. With information stored in the cloud, providers are able to focus on more important issues, like patient care, training, organization growth, and medical development.

Regardless of whether you are thinking of moving into the cloud, your organization still needs to be protected and compliant.

How to Protect Your Organization

Remaining diligent is the key to successfully securing data. People still remain the top offenders of HIPAA violations, despite growing technology challenges. Audits on processes and compliance should be done quarterly. The old adage "if it ain't broke, don't fix it" does not apply. Compliance isn't something you do and put on a shelf. Every employee and every department, not just IT, is responsible for protecting patient information.

Here are some best practices and things to consider for the every-evolving changes in healthcare.

1. **Update Security Risk Assessments** – as technology advances, so does cyber-attacks. Don't be complacent about your level of security. Quarterly or yearly evaluations are necessary to thwart data breaches.

2. **Vendor Agreements** – keep informed about your partners' security protocols and compliance risks. Make certain all contracts and agreements clearly outline responsibility and controls, as well as compliance practices.

3. **Vendor Selection** – choosing the right provider to partner with makes all the difference in the service you provide. When vetting a contact center partner, look for one that is in the cloud and has solid data management.

4. **IT Security Assessment** – like every area of a company, IT needs to have a quarterly or bi-annual assessment to make certain you are protected from data breaches. Consider hiring professionals who specialize in IT security. The cost may very well pay for itself in avoiding HIPAA violations and loss of customers.

5. **Employee Training** – the number one cause of HIPAA violations in 2015. You can't train your staff enough. Consider the method of training and evaluate the return on investment. It's not enough to put them through a webinar. Employee training must be consistent and constant.

6. **Administrative Practice Review** – people walking out of the office with patient files, laptops being stored in cars, computers left unguarded. Take a hard and fresh look at your administrative practices and challenge your organization to do better. A great rule of thumb: look at your business like an outsider doing an audit.

Being proactive protects your patients and your company. Put a process in place that addresses the best practices and don't get caught trying to fix a data breach or privacy violations after they have occurred. The good news is you don't have to sacrifice technology for security. Cloud providers are leading the industry in winning the battle against cyber-attacks and data breaches, making your transition into the cloud the better option.

Request a demo with IntelePeer
to get an inside look at Atmosphere

CHConsulting*Group*
Expert Guidance • Proven Results

Consulting Group is an extensive network of professionals providing high level consulting services to a diverse range of clients. Our consultants act as an extension of clients' teams to serve as strategy partners, drive growth and provide stability. For more information, visit chconsultinggroup.com, email info@thechcg.com or call 218-286-4004.

Read more about our projects, results, expertise and thoughts at www.chconsultinggroup.com

IntelePeer®
The Cloud Communications Company