Business White Paper

Secure HIPAA Compliant Cloud Computing

Step-by-step guide for achieving HIPAA compliance and safeguarding your PHI in a cloud computing environment

ClearDATA
SECURE • HEALTHCARE • CLOUD

Step-by-Step Guide for Choosing a HIPAA Compliant Cloud Computing Provider

Table of Contents

Page 2
The Dilemma
for Healthcare Providers

Page 3
The Cloud: Streamlining
Compliance Requirements

P4 Step one: Inventory your PHI
P5 Step two: Protect your self with a strong BAA
P6 Step three: Focus on information security
P7 Step four: Conduct advanced due diligence
P8 Step five: Protect your mobile data

Page 9
Conclusion

Healthcare in the United States has quickly undergone a significant transformation. With the implementation of the HITECH Act of 2009, by the end of 2012 most office-based doctors – 72 percent – were using electronic medical records (EMRs), up from 48 percent in 2009. The Affordable Care Act, passed in March 2010, added another incentive for the market to adopt new technology by encouraging the creation of Accountable Care Organizations – coordinated care teams that share knowledge in order to provide the highest-quality treatment to patients.

Now, tasked with choosing the best way to store and back up electronic protected health information, or PHI, many healthcare technology companies and providers are looking at cloud computing. The technology has made the traditional onsite data-hosting model cost-prohibitive and obsolete by offering rapid server deployment, near instant scalability and greater redundancy than ever before. While the benefits are clear, there are security and compliance requirements unique to the healthcare industry that must be considered when adopting cloud technology.

The Dilemma for Healthcare Providers

As providers adopt EMR and other digital technologies, they are faced with immediate questions and decisions such as where to host the data – at their facility, at a traditional data center, or with a public or private cloud-hosting provider. Regardless of the location, they must comply with the stringent rules for safeguarding PHI as outlined in the HIPAA Privacy and Security Rules and HITECH Act.

This new compliance reality sets in when members of the management team are forced to become experts in the privacy and technical security of patient data. PHI must be safeguarded

throughout the entire "data lifecycle," which encompasses all phases of its use from creation/capture through to destruction (see Figure 1).

Figure 1
Protecteced Health Information (PHI) Data Lifecycle

As healthcare organizations migrate to new technology and seek to safeguard their patient data at each step of the lifecycle, they are faced with daunting topics such as encryption management, vulnerability monitoring and alerting, intrusion detection and prevention, audit logging and log management, patch management, connectivity, remote access, and disaster recovery.

They hear security terms like multifactor authentication, blended connectivity and transparent data encryption. They wonder how all of this technology relates to daily workflow procedures and protocols. They seek to understand how to comply with HIPAA requirements while trying to balance patient care and running a healthcare organization.

If they consider hosting their data in-house, managers often are shocked when presented with the extremely high cost of expertise, redundancy and the physical infrastructure necessary to meet basic redundant performance such as cooling, physical security and connectivity to the Internet.

The Cloud:
Streamlining Compliance Requirements

There is, however, good news. Healthcare organizations struggling to navigate new techno-compliance waters have found that cloud computing can make their lives easier. Savvy healthcare IT leaders are adopting cloud technology as a way to secure PHI, modernize their infrastructre, host their clinical applications, and support big data initiatives, all while reducing their IT costs. The key to reaping

the benefits of cloud computing while ensuring HIPAA and HITECH compliance is to move forward in a cautious, intelligent manner.

Step one: Inventory your PHI

HIPAA security standards require healthcare organizations to safeguard their PHI. They apply exclusively to patient data and do not specify where data must be stored and safeguarded, only that the safeguards are effective and operational.

PHI Inventory Questionnaire

Question #	Summary of survey question
1	Primary purpose of application or database
2	Type of data (e.g., clinical care, financial/billing, research, operational, other)
3	Reporting to external parties? (Yes/No) If Yes, name agency
4	Interfaces with other systems? (Yes/No). If yes, list systems. Include interface diagram, if available
5	Physical location of system/database (e.g., data center, dept. server, shared drive, vendor, etc.)
6	Age of data (< 1 month, …, > 5 years)
7	Is application/system/database supported by central IT dept? (Yes/No) If No, who supports?
8	Vendor for system. Include version/release number, date of installation, date of last upgrade
9	Does vendor have access? (Yes, No)
10	BA Agreement in place? (Yes/No)
11	Policies and procedures for access to system/database
12	Data recovery strategies. Business continuity planning. Disaster recovery plan
13	Interface to medical device. (Yes/No)
14	Will system/application/database be replaced in next 2 years?
15	Rate criticality of data to departmental

Figure 2 - PHI Inventory Questionnaire

This requires a comprehensive inventory of your PHI. Knowing what type of data you have, where it is stored, how it is being used (Figure 2) and how it is being safeguarded is the critical first step to ensuring HIPAA compliance.

Once complete, identify which data is governed by HIPAA security standards. This is important for determing whether the data you are moving to the cloud requires a HIPAA compliant provider. Most cloud computing providers are not compliant which will place your organization at serious risk.

Step two: Protect yourself with a strong BAA

Given the directives in the 2013 HIPAA Omnibus Final Rule and the fact that cloud hosting vendors store, transmit and process PHI, service providers must comply with the same mandates for data protection as the healthcare organization. This requires cloud hosting providers to sign a Business Associate (BA) agreement, which mandates that they:

- Comply with their contracts to secure PHI and control its use and disclosure
- Have appropriate safeguards in place that satisfy the requirements of the HIPAA Privacy and Security Rules
- Report all privacy and security incidents to the healthcare provider
- Hold their agents and subcontractors to the same restrictions and conditions with which they must comply
- Make arrangements to handle patient requests for PHI
- Provide their clients with the necessary information to respond to patient requests to “account for all disclosures”
- Require all of its vendors that may come in contact with PHI to sign BA agreements (hardware maintenance, software and service providers)
- Be able to make their records related to PHI available to their clients in the event of audit
- Return or destroy all PHI when the contract expires or is terminated

Step three: Focus on information security

Many cite security as a concern when moving data to the cloud. However, Lothar Determann, a leading healthcare security expert, points out in "Data Privacy in the Cloud – A dozen myths and facts" in The Privacy Advisor, that cloud computing in itself is not a detriment to security. Data is only as secure as the entity handling the data. "Moving data to the cloud can be a bad thing for data security if the vendor is weak on security and careless," he writes. "It can be a good thing if the vendor brings better technologies to the table and helps the data controller manage access, data retention, and data integrity."

Selecting a cloud computing provider that exclusively services the healthcare market has many benefits. First, they have a depth of understanding on the unique challenges and regulatory complexities faced by healthcare organizations that other providers simply do not. This reduces your risk from inadvertant compliance lapses or a lack of proper protocols to support normal healthcare work flows.

Second, by focusing their time and resources solely on the needs of healthcare organizations, they have become leaders in building highly secure cloud computing infrastructures purpose-built to safeguard PHI against breach and data loss.

Third, their specialized professional and managed services teams offer expertise in encryption management, vulnerability monitoring and alerting, intrusion detection and prevention, audit logging and log management, patch management, connectivity, remote access, and disaster recovery. You can rest easy knowing your infrastructure is well protected.

One of the best ways to overcome concerns about data security in the cloud is to carefully evaluate cloud providers and their approach to management, security and accountability. Compliance with healthcare regulations requires that the healthcare provider maintain visibility into where data is stored throughout its lifecycle and who has access to the data at each stage. Public cloud environments can make tracking data throughout the lifecycle a difficult, if not impossible, task.

Step four: Conduct advanced due diligence

Healthcare cloud consumers should conduct the due diligence necessary to ensure that their PHI is protected. Here are some essential questions healthcare institutions should ask of a potential cloud provider:

- In what industries do you specialize? What is your primary focus? Healthcare is a complex, highly regulated environment, with multiple specialized healthcare applications, legacy hardware and network environments, and various levels of IT management sophistication. Ask whether or not the provider has a general focus, or specializes in a specific segment of the market, such as financial services, healthcare, e-mail, or ERP? Understanding the focus of the cloud provider will help pinpoint core competencies.
- Will you seek to fully understand our data lifecycle? Will the lifecycle be documented and periodically reviewed as new technologies or systems are added?
- Is your workforce required to undergo background checks, as required under a BA agreement?
- As with healthcare providers, does your entire workforce undergo HIPAA and Security Awareness training and adhere to "Minimum Necessary Use" principles?
- Will you take on the entire responsibility to provide security mechanisms, or rely on us to provide do-it-yourself mechanisms? Will the security mechanisms satisfy legal requirements for reasonably safeguarding patient data? This review should consider security controls, such as system activity monitoring and alerting, unique user enforcement, and end-to-end vulnerability management and intrusion detection and prevention.
- How will you address encryption requirements for data in motion and at rest; backup and restore testing; and all other safeguards recognized by either widely accepted security framework, such as NIST or HITRUST's Common Security Framework? Once healthcare institutions conduct deeper due diligence, many find that their service providers are only compliant on the physical layer and require a "shared

responsibility" or do-it-yourself tools and capabilities for the remaining HIPAA compliance. As a result, some service providers require the cloud consumer to have deep cloud security privacy know-how to ensure that data is secured within a policy-driven architecture.

- Have you been independently audited for your security controls? Are you SSAE 16 or SAS70 Type II certified?
- What other services do you offer? Do you offer extensive managed services for healthcare, consulting, and professional services? Do those services complement your cloud and security offerings?
- Where are the physical systems located, and do you own them or tap into additional computer resources to meet spikes in demand? The location of the data is an important consideration. Latency in accessing data could be an issue if the data is located off the main backbone of the Internet. If the data is located in a different country, there could also be regulatory jurisdictional issues and legal uncertainties.
- How available and reliable is your infrastructure? Ensure that the cloud provider is equipped to handle critical application loads. Remember, you will need to have established, "always on" continuity plans.

  What administrative, technical, physical and organizational policies and procedures are in place and designed to safeguard patient data? Are those policies and procedures sufficient to be effective, and are they operational? Determine if they mirror your organization's standards.

Step five: Protect your mobile data

With mobile phone and tablet use growing among medical providers, the newest threat to PHI security is accidental employee error. A recent Health Data Management article warns, "Internal security threats have always been legion, and now that there's a mobile device in every pocket, the situation is downright scary. It's important for companies to be vigilant and monitor data traffic through log analysis and access management, and to keep track of mobile device or external storage media use."

Choose a cloud provider with deep domain expertise in HIPPA compliance that will help healthcare organizations broaden their policies and procedures to include mobile data.

Conclusion

Keeping pace with what seems to be an endless run of federal regulations and oversight that impact the IT side of the healthcare industry is a seemingly impossible task. In the last few years, operating in the healthcare industry has become exponentially more complex. Especially regarding HIPAA Privacy and Security Rules and HITECH Act, healthcare organizations can – understandably – barely keep pace. Working with a cloud service provider that is solely focused on healthcare and has an impeccable record of success in meeting compliance requirements can ease the burden. Choose wisely, and work with a partner that can help provide wise guidance through the maze of options available for meeting new regulations and easing IT and privacy burdens.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

1600 W. Broadway Road, Tempe AZ
(800) 804-6052
www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD