Selecting a HIPAA-Compliant Cloud: Avoid the 7 Deadly Sins

HIPAA is not prescriptive or precise, but organizations must be

Like companies in every other industry, healthcare organizations are eager to exploit the cloud and its numerous benefits to efforts such as connected health and cost containment. According to a recent survey by 451 Research, the percentage of all IT workloads deployed to the cloud will soar from 40 percent today to more than 57 percent in two years.[1]

In healthcare, however, moving to the cloud carries unique challenges. In a recent survey, the average cost per record hacked or stolen in a cyberattack was $158.[2] But in healthcare, the cost per record breached was $355 – the highest of any vertical market. This wide disparity is due to the stringent and punitive healthcare regulatory environment, and in particular to the imprecise requirements of the Health Insurance Portability and Accountability Act or HIPAA.

These competing forces of the demand for cloud and the often vague requirements of HIPAA compliance make tricky work of building and deploying a HIPAA-compliant cloud. Here, however, are the 7 most common mistakes healthcare organizations make when building compliant clouds, and some suggestions for avoiding them.

Produced in partnership with

HIMSS Media

The core rule of HIPAA simply says you will protect the confidentiality, integrity and availability of protected health information from all reasonably anticipated threats.

1. Not comprehending what HIPAA is and is not

Some users will approach the cloud believing there is some checklist they can follow to insure HIPAA compliance. But no such definitive cloud-compliance to-do list exists. The core rule of HIPAA simply says you will protect the confidentiality, integrity and availability of protected health information (PHI) from all reasonably anticipated threats. That's it. If there is a data breach, you must comply with the tenets of the HIPAA Breach Notification rule. In addition, 47 states each have its unique cyber-breach disclosure laws. And some healthcare organizations may also need to comply with certain FDA requirements. Often, it takes a so-called breach coach – specialized lawyer – to fully understand the intricacies of HIPAA and other compliance regulations before making cloud-deployment decisions.

2. Believing your cloud provider is responsible for security

Major public-cloud providers will promise security of their cloud. They and third parties offering cloud services using these public-cloud providers may even state they are "100% HIPAA compliant." That statement is impossible because HIPAA offers no such compliance certification – to anyone. And while these big public-cloud services may offer a secure cloud, they cannot and will not certify that they offer security *within* their cloud. For your cloud applications and all the PHI data that runs within them, you are responsible for security and compliance. Thus, it is vital when establishing a relationship with a cloud provider to develop a clearly written understanding of who is responsible for what when it comes to security and compliance. The public-cloud provider may well offer no antivirus, no logging, no network-level protection or intrusion detection. You often get nothing more than a raw Internet feed to your server, and a firewall separating your server from others. The rest is often up to you, or to a trusted third party.

3. Not grasping the importance of the security risk assessment

HIPAA legislation mandates you must conduct a *proper* security risk assessment (SRA) and fully document it. Without an airtight SRA, an organization is largely defenseless in the event of a breach and corresponding HIPAA-compliance inquiry. And plans for cloud deployment of applications containing PHI only complicate the SRA. In essence, the SRA is an organization's assessment of the risks that its PHI data might confront as it moves from place to place, user to user, or process to process. Done properly, an SRA ranks these risks. Then the SRA must show the protections that were put in place to address the risks. Seen this way, compliance is really an end-product or by-product of your security strategy, including what you plan to do in the cloud where data may not be fully in your control. A trusted third-party security consulting firm is often indispensible when it comes to creating this critical document. It is your insurance policy in the event of a HIPAA-mandated audit.

4. Failing to understand the penalties of non-compliance

In a landmark test of HIPAA compliance four years ago, Blue Cross of Tennessee was hit with a $1.5 million non-compliance fine after a thief grabbed several disk drives containing a million unencrypted medical records. Blue Cross forked out an additional *$17 million* on the investigation, notifications and subsequent damage mitigation. And this says nothing about the hit on the insurer's reputation. The important thing to note here is that if you lose PHI, you can be subjected to multiple layers of associated costs. Fines and fees like those heaped upon Blue Cross of Tennessee offer all the more reason to ensure your moves to the cloud are heavily infused with HIPAA-compliance considerations.

> *The Common Security Framework is "highly prescriptive and meets the bar for HIPAA risk analysis."*
>
> | Michael Frederick | Vice President of Operations | HITRUST

5. Failing to nail down a comprehensive business associate agreement (BAA)

Prior to 2013, the responsibility for securing PHI fell solely to the healthcare organization. The HIPAA Omnibus Rule changed things to include pretty much any third party that touched PHI data. This followed an investigation that revealed most breaches were happening at the business-associate level, like medical transcribers, third-party billers and others. Thus was born the BAA, the document that needs to spell out very clearly and unambiguously who is responsible for what when it comes to PHI security. As mentioned earlier, big public-cloud companies secure their cloud, but not your application or data necessarily. It is generally believed that in a breach aftermath, investigators will give serious consideration to a clearly written BAA when it comes to assessing potential fault.

6. Not appreciating the importance of HITRUST certification

Recognizing HIPAA's lack of preciseness and prescriptiveness when it comes to compliance, large healthcare organizations created HITRUST specifically to help ease the burden of HIPAA compliance. HITRUST developed a Common Security Framework (CSF) to be used by all organizations working with PHI, including prescriptive controls to ensure compliance. Michael Frederick, vice president of Operations at HITRUST, noted that the CSF is "highly prescriptive and meets the bar for HIPAA risk analysis." And the CSF constructs apply evenly to PHI data within or outside the cloud. Frederick maintains that when it comes to cloud compliance, privacy can take precedence over security. "You just need to be very clear who owns the data and where it resides at all times," he emphasized. "You cannot transfer your risk to cloud providers." Further, he pointed out that there are "numerous cloud providers like Armor that can be very helpful" in ensuring cloud deployments are HIPAA compliant, and many of these providers are HITRUST-certified.

7. Making the wrong choice in a cloud-compliance partner: two case studies

With all that's at stake with HIPAA compliance and with cloud compliance in particular, it just makes good business sense to work with a trusted compliance partner to help avoid potentially costly mistakes. There are many such compliance companies out there. How can you know which is right for your organization?

In the following case studies, two healthcare companies went through this mission-critical process of finding and selecting a cloud compliance partner. In each case, a key exercise was careful, thoughtful consideration of expectations of the partner selected.

Rx Savings Solutions

Founded on the simple principle of helping people find lower-cost alternatives to pricey maintenance medications, Rx Savings grew from concept to reality literally in a matter of weeks. Company founder Dr. Michael Rea soon realized that Rx Savings was going to need a highly secure and compliant cloud solution for accessing and storing protected healthcare information (PHI).

He and his team started their search with a checklist of requirements for a compliance partner and its solution:

- Expertise to ensure Rx Savings would pass HIPAA audits
- Demonstrated quality of service
- Firewalls defined by multiple layers of security
- Ability to scale up or down effortlessly while paying only for the services needed at a given time
- The partner's ability to explain the solution's complexity in terms a non-IT person, like Dr. Rea, could easily grasp
- A solution that is as secure and HIPAA compliant as it is reliable

It took one false start with another company, but Rx Savings eventually settled on a partner that delivered on all requirements. In addition, this partner had a collaborative relationship with HITRUST, and actually served HITRUST as a provider. It was that level of HIPAA-compliance expertise that gave the Rx Savings team full confidence in their final choice of a cloud-compliance partner.

Ortho Kinematics

This Austin-based company revolutionized spinal imaging analysis with a solution allowing doctors to capture videos showing the spine in full motion, enabling far more reliable and effective diagnostics compared with still images. Upon its launch, Ortho Kinematics leaders realized they needed a cloud provider and a solution that would unquestionably meet HIPAA compliance guidelines for its PHI. And like Rx Savings, they had their own checklist of requirements:

- A secure cloud that demonstrably meets if not exceeds HIPAA and FDA security requirements
- A fair and reasonable price
- No long-term contract
- A solution that would reduce the 24-hour run time of a complex video on a workstation to an hour or two

Ortho Kinematics settled on a cloud partner that today is entrusted with all of its patient healthcare information. Bryant Mile, head of IT infrastructure at Ortho Kinematics, went so far as to say, "The partnership has helped design a roadmap for future Ortho Kinematics growth."

Moving forward

The road to a HIPAA compliant cloud is fraught with potholes and wrong turns. The good news is that no organization needs to travel that road alone. Specialists and trusted third parties are at the ready to keep your efforts on task. Remember that the goal is not cloud computing per se, but rather the business value cloud can deliver to the highly dynamic environment that is healthcare today.

References

[1] 451 Research Voice of the Enterprise: Cloud Computing Workloads and Key projects survey of 1100 user organizations.

[2] Ponemon Research (underwritten by IBM) survey Cost of a Data Breach 2016 http://fortune.com/2016/06/15/data-breach-cost-study-ibm/