MARCH 2020

ARMOR

WHITE PAPER

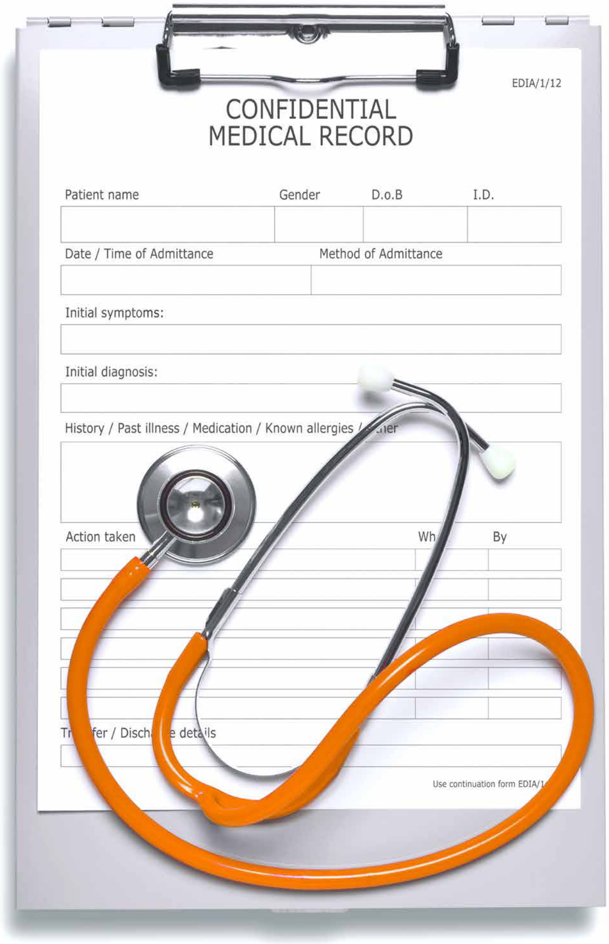
HIPAA-COMPLIANT CLOUD: AVOID THE 7 DEADLY SINS

INTRODUCTION

HIPAA is not prescriptive, but organizations must be compliant. Like companies in every other industry, healthcare organizations are eager to take advantage of the cloud and its numerous benefits, such as connected health and cost containment. According to a recent survey by 451 Research, the percentage of all IT workloads shifted to the cloud will soar from 40 percent today to more than 57 percent in 2 years.

Despite this increase in cloud adoption, the healthcare industry has unique challenges when migrating to the cloud. The industry is highly regulated 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. As part of that regulation, the industry has more stringent penalties for data breach if the company is not compliant. In a recent survey, the average cost per record hacked or stolen in a cyberattack was $158, but in healthcare the cost per record breached was $355—the highest of any vertical market.

The complexity of cloud configurations and the somewhat vague requirements of HIPAA compliance make tricky work of building and deploying a compliant cloud. Here are the 7 most common mistakes healthcare organizations make when building compliant clouds, and some suggestions for avoiding them.


EDIA/1/12
CONFIDENTIAL
MEDICAL RECORD
Patient name
Gender
D.o.B
I.D.
Date / Time of Admittance
Method of Admittance
Initial symptoms:
Initial diagnosis:
History / Past illness / Medication / Known allergies / Other
Action taken
Wh
By
Transfer / Discharge details
Use continuation form EDIA/1

7 MOST COMMON MISTAKES HEALTHCARE ORGANIZATIONS MAKE

1. NOT COMPREHENDING WHAT HIPAA IS AND IS NOT

Some organizations will approach the cloud believing there are checklists they can follow to ensure HIPAA compliance. The reality is that no such cloud-compliance checklist exists. The core rule of HIPAA simply states that an organization 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 their own unique cyber-breach disclosure laws. And some healthcare organizations may also need to comply with certain FDA requirements. Often, it takes a breach coach—a 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. These public cloud providers and cloud service providers may even state that their solutions are "100% HIPAA compliant." The truth is that HIPAA offers no such compliance certification. In the shared responsibility model, public cloud providers are responsible for protecting their infrastructure. Organizations are responsible for security and compliance of all their own data and applications. Thus, it is vital when establishing a relationship with a cloud provider to develop a clearly written security and compliance responsibility matrix between you and the cloud provider. Public-cloud providers do not provide antivirus, log and data management, 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 resulting HIPAA-compliance inquiry. SRAs are complicated by plans for cloud deployment of applications containing PHI. In essence, the SRA is an organization's assessment of the risks to PHI data as it moves from place to place, user to user, or process to process. Done properly, an SRA ranks these risks and shows 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. A trusted third-party security consulting firm is often indispensable when it comes to creating this critical document.

4. FAILING TO UNDERSTAND THE PENALTIES OF NON-COMPLIANCE

In a 2019 ruling on HIPAA compliance, the Texas Health and Human Services Commission was hit with a $1.6 million non-compliance fine after patient records were exposed. The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials. Fines and fees such as those heaped upon the Texas Health and Human Services Commission represent only a portion of the total losses incurred due to the breach. Additional costs include internal investigations, notifications, and further damage mitigation, not to mention the cost of lost revenue and damage to consumer confidence.

> **The Common Security Framework is "highly prescriptive and meets the bar for HIPAA risk analysis."**
>
> — Michael Frederick, VP 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 the requirement to include any third party that touched PHI data. This followed an investigation that revealed most breaches happened at the business associate level, such as medical transcribers, third-party billers and others. Thus, the BAA was born, which is a legal document between a healthcare provider and third-party contractor. It satisfies HIPAA regulations and creates a bond of liability that binds the two parties, making the contractor also responsible for securing PHI on their end. It is generally believed that in the aftermath of a breach, 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

Large healthcare organizations created HITRUST specifically to help ease the burden of HIPAA compliance. HITRUST developed the Common Security Framework (CSF) for organizations working with PHI. CSF included 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." 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. CHOOSING THE WRONG CLOUD-COMPLIANCE PARTNER: 2 CASE STUDIES

With all that's at stake with HIPAA compliance and specifically with cloud compliance, it makes good business sense to work with a trusted compliance partner to help avoid potentially costly mistakes. There are many 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 expensive maintenance medications, Rx Savings grew from concept to reality 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 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 only paying for the services needed at a given time
- The partner's ability to explain the solution's complexity in terms a non-IT person, such as Dr. Rea, could easily grasp
- A solution that is as secure and HIPAA-compliant as it is reliable

Rx Savings took one false start with another company but eventually settled on a partner that delivered on all requirements. This new partner had a collaborative relationship with HITRUST and was a provider for HITRUST. It was that level of HIPAA-compliance expertise that gave the Rx Savings team full confidence in their cloud-compliance partner.

ORTHO KINEMATICS

This Austin-based company revolutionized spinal imaging analysis with a solution that allowed doctors to capture videos showing the spine in full motion which enabled 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, the company had its 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 1-2 hours

Ortho Kinematics chose a cloud partner and entrusted them 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."

ABOUT ARMOR

Armor is a global cybersecurity software company that simplifies protecting your data and applications in private, public, or hybrid cloud—or in an on-premise IT environment. Armor Anywhere provides technology to detect and respond to threats and can be activated in minutes. Armor also helps organizations comply with major regulatory frameworks and controls. Armor's cybersecurity experts monitor customer environments 24/7/365 and, if an attack takes place, helps customers respond quickly and effectively. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167