Securing a Compliant Path Through the Healthcare Cloud

ClearDATA
SECURE • HEALTHCARE • CLOUD

Introduction

Healthcare organizations and health IT developers are looking to new and emerging technology to improve clinical decision-making, care delivery while working to lower costs for healthcare. Supporting innovation in care delivery while maintaining compliance with federal and state laws governing sensitive health information remains a challenge for many.

The cloud provides scalable computing resources and data storage to put useful applications and actionable data in the hands of end users. As of last year, HIMSS Analytics found that nearly two-thirds (65%) of surveyed hospital technology leaders reported using the cloud or cloud services, mainly hosting applications, disaster recovery and backup, and storing primary data.

The healthcare industry is moving forward with leveraging Software-as-as-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) to meet the data and service demands of end users and reduce their onsite IT footprint. Projections from leading research firms estimate the global healthcare cloud computing market to approach approach $10 billion by the turn of the decade.

Not all healthcare organizations and health IT developers migrating to the cloud are building with a security by design model, or mapping to regulatory and compliance frameworks. These cloud users run the risk of non-compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other federal, and now international requirements. HIPAA-covered entities (CEs) and business associates (BAs) need to do their due diligence in identifying and addressing potential threats to protected health information (PHI) regardless of whether they are on premise or in the cloud.

Even the most technically skilled in healthcare are turning to qualified managed cloud providers to ensure that their cloud models are designed with privacy and security in mind. The end result is a secure platform that enables IT staff to focus on strategies for putting the most effective tools in the hands of clinicians for the benefit of patients, while they innovate and scale with speed and agility.

Industry Leader Urges Healthcare to Move to the Cloud

In the keynote for the most recent annual meeting of the Healthcare Information and Management Systems Society (HIMSS), former Executive Chairman of Google and Alphabet Inc., Eric Schmidt, told attendees to neither crawl nor walk but run to the cloud to enable innovation.

"Get to the cloud," he said. "Most of you sit in institutions that have proprietary data centers, which have some sort of logic about them. Most of that logic may have been true five or ten years ago, but it isn't today." According to Schmidt, the tech industry has developed cloud-based servers that are much safer, more HIPAA-compliant, and easier to use than anything sitting on premise as part of existing health IT infrastructure.

"The cloud is more secure," he continued. "I don't want you repeating the infrastructure work that we're doing. I want you all to focus on the innovation."

The freedom to focus on innovation rather than maintain data centers is a major selling point for all the top cloud service providers working to attract healthcare organizations and health IT developers to their platforms, such an Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

As ClearDATA Senior Vice President and Co-Founder Carl Kunkleman points out, healthcare is migrating to the cloud and adopting new technology. "The migration into electronic medical records happened

pretty quickly. If you really think about it, eight years is pretty fast for any industry to go from ground zero in 2010 to where we are today."

> "Get to the cloud. Most of you sit in institutions that have proprietary data centers, which have some sort of logic about them. Most of that logic may have been true five or ten years ago, but it isn't today."
>
> —Eric Schmidt
> former Executive Chairman
> Google, Alphabet Inc.

In his time at the HITRUST-certified, healthcare-exclusive cloud security and compliance company, Kunkleman has overseen thousands of risk analyses of healthcare environments that led to some alarming findings.

"The security risk assessment is the most important thing we can do," he explains. "I am stunned when I'm reading our final reports from our risk analysts. The issues they've identified are sometimes pretty basic like patch management, lack of an incident response program, no backups—easy enough fixes, but often overlooked."

Over a decade, security risk assessments (SRAs) have become a core component of federal and state programs aimed at promoting health IT use to improve care coordination, clinical decision-making, and ultimately patient outcomes. And the SRA will remain central to the approach taken by the Centers for Medicare & Medicaid Services to move forward with implementing the Medicare Access and CHIP Reauthorization Act (MACRA) and the Quality Payment Program, which comprises the Merit-based Incentive Payment System (MIPS) and Advanced Alternative Payment Models (APMs).

For meaningful use's successor, the Advancing Care Information component of MIPS, a risk analysis remains a core requirement that has flown under the radar of many eligible clinicians.

"Doctors in many hospitals are just learning that last year was the base year for 2019 MACRA/MIPS. If you didn't get your risk analysis done last year, not only are you not eligible for incentive dollars in 2019, but you in fact will have a four-point reduction because you didn't meet the requirements," Kunkleman observes.

"So it's pretty ugly right now for these providers and they're scared," he continues. "The good news is that if you walk them through the SRA process and then assign committed IT team to it, they use our risk analysis and adjudicate those risks pretty quickly."

If healthcare organizations already have gaping security holes or small leaks in their health IT infrastructure or management processes, the cloud is not going to supply a magical repair. It makes sense to see exactly where those gaps are and repair them as you move to the cloud.

Value of a Thorough Security Risk Assessment

During a session at the HIMSS18 Cybersecurity Command Center, University of Florida Health's Health IT Security Manager Craig Gormé wasted little time noting that the value of PHI and personally identifiable information (PII) has not gone unnoticed to black hats.

"Healthcare is an attractive target," he warned. "Along with the complex landscape we have to deal with, the attackers have unlimited time, unlimited resources. They are constantly attacking our networks and our people. They are constantly doing phishing attacks and reconnaissance against our systems, throwing in attacks like malware. We are always behind the eight ball."

As if the healthcare industry needed any additional pressure, sensitive health data (i.e., PHI) has increased in monetary value for bad actors. Therefore, the time is now for CEs and BAs to take swift action to identify and remediate vulnerabilities in their health IT systems.

As healthcare organizations consider moving any portion of their IT infrastructure to the cloud, they should ensure their house is in order to comply with health data security and privacy rules. Plenty of self-service tools are available to conduct security assessments, but they can easily lead to a false sense of security.

> "Healthcare is an attractive target. Along with the complex landscape we have to deal with, the attackers have unlimited time, unlimited resources. They are constantly attacking our networks and our people. They are constantly doing phishing attacks and reconnaissance against our systems, throwing in attacks like malware. We are always behind the eight ball."
>
> —Craig Gormé
> IT Security Manager
> University of Florida Health

"Many customers have paid $1500 for a software program and spent all weekend answering yes to hundreds of questions. They contact me because they know that can't be right. I'll ask four or five questions and soon they're understanding they needed to think about their environment differently," Kunkleman observes.

A lack of understanding about health data security and privacy vulnerabilities is still a challenge throughout the healthcare industry, and regulations continue to become more complex.

"Often, people don't fully understand the context behind the questions, and that's where we can really provide value" Kunkleman emphasizes. "We guide them through those six to eight weeks to that final report. The report is presented in both technical and non-technical terms, with the result being an understanding of the business case of why HIPAA compliance is important and how it impacts their bottom lines."

The final meeting unites the C-suite in understanding their risks, and helps them recognize the importance of the process and allocates resources for remediation. The ultimate goal is to develop a plan with achievable objectives.

"There are lots of things you can and can't do in any organization. We help them make sure they can put remediation steps in place that not only meet HIPAA compliance, but also can actually be executed successfully," Kunkleman says.

Conducting a thorough SRA with the support of external subject-matter experts such as ClearDATA establishes an important baseline for any healthcare organization going forward, especially those with plans for cloud adoption or expansion in the cloud.

A Cloud Platform with Security by Design

Scalability is a defining feature of cloud computing. Most often in healthcare, organizations are growing as a result of mergers, acquisitions, and expansions that make scalability a core component of the health IT infrastructure moving forward.

Without a solid foundation of security and privacy, healthcare organizations could be scaling bad practices for safeguarding PHI as they increase the size and complexity of their cloud platform.

"You can secure data better in the cloud than an entity can in their own environment," says ClearDATA Founder, Chief Privacy & Security Officer Chris Bowen, CISSP, CCSP, CIPP/US, CIPT. "Healthcare organizations have often thought that they have control over their data so long as that information sits within their four walls. In the past, if that data were to sit outside those walls and they couldn't see the infrastructure, they had trepidations about allowing their information to be other than in their own facilities."

In recent years, a change has taken place. Healthcare organizations are unable to scale their on-premise health IT infrastructure to support the data and service demands of their complex care environments while cloud providers have become more secure and transparent about their offerings.

"With the advent of the major public clouds (AWS, Microsoft, and Google), the security controls are much more visible. They're much more auditable. They're much more scalable," Bowen adds.

However, that trend is not enough. Healthcare organizations and health IT developers looking to the cloud need to make appropriate use of readily available frameworks (e.g., HITRUST, NIST, ISO) to achieve scale without compromising on privacy and security.

"If you coupled that with security and privacy by design—that is, building the guard rails in the automation and eliminating the human component as much as possible from that—then you have something that will actually scale," claims Bowen.Automating safeguards and addressing the human component must be part of a shift in mindset among CEs and BAs. As Bowen notes, the recent major breaches can trace their origins back to a failure on the part of sometimes a single individual.

Perhaps an IT professional forgets to implement a critical patch. Or, in the case of phishing, one individual with access to tens of millions of records can have his credentials compromised through social engineering.

A new thought process must begin with a close inspection of an organization's data using a strategy known as defense in depth.

"The time to start thinking about security of data happens at the time you collect the data," Bowen explains. "Know where the data is, then focus on designing your automation for scale around hardening

Flexibile Scalability at Genoa Healthcare

In 2014, a merger with a QoL meds, LLC, grew the organization from 125 to more than 220 facilities, creating an organization whose existing health IT infrastructure could not support an application that enables pharmacists to provide important medications to patients with behavioral health and addiction conditions.

"When that happened, we realized that our current hosting provider wasn't able to scale any of its services to support the larger organization," said Genoa Healthcare Chief Information Officer John McConnell. "And while they were contractually obligated to comply with HIPAA rules, we didn't have any comfort that they actually understood what that meant."

The merged organization had a 180-day window to move from a co-located hosted environment to an AWS environment without prior experience setting up a HIPAA-compliant cloud platform.

"We started looking at the suite of AWS services," McConnell explained. "Picking the things we needed, gluing them all together, and staying compliant was just too much for us to consider. We didn't have the expertise. It was not going to be a comfortable project."

Genoa partnered with ClearDATA to migrate its data warehouse and core pharmacy app to a managed cloud for shared responsibility, continuous compliance, and scaling of services. ClearDATA helped Genoa choose the right architecture for supporting its pharmacy applications, methods for splitting loads to the most appropriate place, and strategies for prioritizing solutions requiring high availability for redundancy, as well as isolating databases to support external-facing applications. The process was completed in 90 days.

Since then, Genoa has experienced 20- to 25-percent growth year over year. On March 15, 2018, Genoa announced the grand opening of its 400th pharmacy, expanding its organization across 45 states and serving 650,000 consumers.

the OS, database, and other pieces. Approach encryption from both a risk perspective as well as a logical standpoint to help with guarding against bad actors internally first and externally second."

In other words, automate privacy and security components to minimize the potential damage an individual could inflict on the entire environment. The goal is to isolate sensitive data and databases and leverage microservices that access the minimum information necessary for completing a given task in a healthcare setting.

Even a well-designed secure cloud environment still requires education and training around reacting to vulnerabilities and attacks.

"It comes back to people, process, and technology. You need an incident response plan — you can't just wing it. We like to provide drills for our customers with repeated simulations," Bowen reveals.

On the technology side, health data security and privacy professionals require visibility into their network and cloud as well as the traffic in and out of the environment, to ensure that only the right individuals are accessing information.

Another tool is logging, which provides a variety of details about activities taking place in a cloud-based ecosystem. Healthcare organizations and health IT developers should make a commitment to reviewing logs so as to address problematic events.

At a community level, healthcare organizations and health IT developers in the cloud should participate in threat intelligence sharing to strengthen the industry's ability to combat and prevent cybersecurity threats from having widespread implications for their partners assisting in the delivery of care as well as their peers.

By taking the time to design an approach to cloud computing that incorporates privacy and security as

Scaling Innovation at Roche Diagnostics

A multidisciplinary approach to delivering personalized medicine to cancer patients requires the aggregation of disparate data from numerous sources. Roche's Diagnostics Information Solutions (DIS) set out with a plan to provide precision health by combining data from electronic health records (EHRs), picture archiving and communication systems (PACS), genomics, clinical research, and other information.

"Precision medicine focuses on treating that patient in the moment with everything that we know about them. The work that we go through to get to that answer really leads us to a large accumulation of information about known populations," said Ram Balasubramanian, Sr. Director, Software Enginging.

Traditional tumor boards often rely on non-secure methods for sharing information that could lead to the exposure of sensitive data to the wrong individuals (e.g., printed materials, emails, thumb drives).

"The one thing that we see repeatedly is the need for more articulate use of data within the precision medicine and health environments," Balasubramanian explained. "But the task of bringing all of that information together can feel very overwhelming."

When creating the NAVIFY™ Tumor Board solution, DIS worked with ClearDATA to secure the data entry and exit points to its AWS cloud.

"Resources like ClearDATA allow us to build a firm foundation for the house we've created," Balasubramanian said.

The end result is a secure centralized, digitized experience for members of the tumor board that speeds clinical decision-making for cancer care teams.

"We are able organize and prepare all the information associated with the tumor board into one singular location. When they schedule the tumor board, they are able to connect everyone effectively so that the decision-making process becomes much more articulate and far more beneficial to the patient," Balasubramanian noted.

cornerstones of the entire system, resources are freed up to be brought to bear on more important activities.

"Ideally, IT staff get to focus on bigger problems: making the patient experience more positive, innovating an application that can solve their healthcare problem, using emerging technologies such as machine learning, artificial intelligence, and blockchain to improve healthcare overall. It's our desire to help make healthcare better, and by freeing up innovators from having to do some of the blocking and tackling in a best in class way is really our goal," Bowen concludes.

Conclusion

The cloud offers a multitude of services and opportunities for potential adopters in healthcare to develop and produce robust applications to support qualitative improvements in care.

However, healthcare organizations and health IT developers making their initial move to the cloud could very easily view this sea of options as overwhelming, leading to more questions than answers:

- Which cloud model is best for what business case?
- What are the implications of each cloud model for health data security and privacy?

In partnership with a trust managed cloud provider, new and existing adopters of the healthcare cloud can navigate a secure path to an environment offering robust computer resources, scalability of services, and levels of security and compliance not feasible within an onsite IT infrastructure.

By leading with a privacy and security mindset, healthcare organizations and health IT developers can develop confidence and trust in their cloud environments and shift their focus to strategies that will advance the practice of medicine across the country and around the globe.

Published by

Xtelligent Media

About ClearDATA

Healthcare professionals across the globe trust the ClearDATA HITRUST-certified cloud to safeguard their sensitive data and power their critical applications. We offer our customers the most comprehensive Business Associate Agreements (BAA) in the industry, combined with market-leading healthcare-exclusive security and compliance solutions. Our innovative solutions help protect our customers from data privacy risks, improve their data management, and scale their healthcare IT infrastructure, enabling our customers to focus on making healthcare better by improving healthcare delivery.