Business White Paper

How Life Sciences Companies Can Achieve HIPAA Compliance In The Cloud

ClearDATA
SECURE • HEALTHCARE • CLOUD

How Life Sciences Companies Can Achieve HIPAA Compliance In The Cloud

Table of Contents

The winds of change pushing America's healthcare profession into a new value-based era are impacting the life sciences industry with similar challenges and opportunities. Drug development cost is dramatically increasing[1] and will continue as payers and employer groups demand greater proof of benefits and use their purchasing power to lower costs. These new demands spur collaborative projects among life sciences companies looking to increase operational efficiency (such as TransCelerate Biopharma) and meet the new burden of proof that value-based offerings demand. Massive data sets result and will continue to grow. Life science companies are hungry for deep data to drive decisions on what to invest in for their drug pipelines, diagnostics and devices.

In order to enrich these massive data sets patient records and profiles are needed. Life sciences companies are quickly becoming confronted with Protected Health Information (PHI) covered by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule[2]. Dealing with volumes of PHI is uncharted territory for an industry used to dealing primarily with the FDA. Who and what does the HIPAA rule protect? Which federal agency enforces it?

The quick answers are that the HIPAA Security Rule is meant to protect patient privacy and is enforced by the Office of Civil Rights, a division under the federal department of Health and Human Services. And no doubt, strong protections and security are warranted. As we will soon discuss, there are sharks circling the perimeters of any organization that has access to patients' medical records, which have exploded in value on the black market.

But as is often the case with federal regulations, HIPAA compliance can be complex rather than simple. It also covers issues beyond patient data privacy and security—most notably, the right of patients to access their own medical records and know who else is accessing these records. In a word, trust[3].

[1] Tufts Study: http://cen.acs.org/articles/92/web/2014/11/Tufts-Study-Finds-Big-Rise.html

[2] "The Security Rule." Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

[3] https://www.whitehouse.gov/precision-medicine

The Market Advantage Of The HIPAA-Compliant Cloud

Companies that can demonstrate patient outcomes will hold a distinct competitive advantage. To gain that advantage, they must know how to comply with the HIPAA rule—or better yet, find a partner that can navigate and help them achieve this compliance. As it happens, another market force is driving ease in securing, storing and analyzing the data needed for collaborative research projects—the switch to highly scalable cloud technologies and services.

Of immediate importance for the life sciences industry to understand is how a healthcare-exclusive cloud is purpose built for HIPAA-compliant security. This white paper describes these layers of compliance in detail, providing life sciences companies with a helpful aid as they research both HIPAA compliance and cloud security. It also offers a preview into extending the cloud's impact into areas such as R&D, clinical trials and consumer engagement. The paper closes with essential next steps to gain HIPAA compliance and protect patient records.

First, a look at why the Life Sciences industry must protect this data with stringent adherence to the HIPAA security rule.

The Seedy World of Medical Data Trafficking

As earlier alluded to, life sciences are increasingly involved in patient outcomes research. It is at this point that many companies will capture patients' sensitive personal information for collaborative projects—and put a giant target on their backs for cyber thieves that traffic in stolen medical records.

For companies that have never made a foray into this underworld market, a recent NPR report gave a fascinating introduction to the online forums where these miscreants gather to hawk and buy stolen patient data[4]. In an ironic twist, the report's investigators noted that many of these sites use Yelp-like rating systems to score

[4] The Black Market for Stolen Health Care Data. (February 13, 2015) Retrieved from http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data

a dealer’s trustworthiness. One dealer who got high marks, for example, had a “value pack” of 10 stolen Medicare numbers for sale at a cost of 22 bitcoin. In US dollar amount, this works out to about $4,700.

To understand why one Medicare number can go for close to $500, consider that these records typically include names, birth dates, social security numbers, policy numbers and billing information that can be used for an equally exhaustive list of profitable activities. Using a valid Medicare number, thieves can open multiple credit lines, create fake IDs, and purchase medical equipment or pharmaceuticals that can be resold at a profit and defraud insurance companies. And unlike credit card fraud, which usually shows up within days and is quickly shut down, medical data theft can go undetected for months or even years.

Which leads to another reason this type of crime is on the rise: the healthcare organizations that house medical records have been easy targets, thanks to aging and fragmented infrastructure and constrained staff. Life sciences companies must go into this new landscape understanding that hackers are hungry for patients’ medical records and will be constantly testing network perimeters for an access point.

Additional HIPAA Encounters

Cybertheft is not the only concern, although it is one that is always present. Capturing patients’ sensitive medical information creates additional responsibilities for the life sciences industry. Here are just some of the scenarios where HIPAA regulations potentially come into play:

A drug company calls a doctor and records the conversation; the data is considered business-related and exempt from HIPAA privacy precautions. However, when a drug company engages patients in conversations about their conditions, this data is considered highly sensitive, and additional regulations may come into play.

When entering a clinical trial agreement (CTA), clinical researchers and research study sponsors need to be keenly aware of HIPAA and HITECH regulations that their research partners, physicians and providers live with every day.

A drug company wants to screen patients to find the best candidates for an expensive, targeted therapy. The screening requires extensive identified, clinical information from tests and electronic medical records (EMRs) sometimes even including genomic information.

A drug company follows patients on a medication by collecting lab and other clinical values from caregivers and the patients themselves. This data helps the drug company and the FDA understand the effect on larger populations, the potential side effects based on long-term use, and quantifies the ROI of drugs to buyer groups and the patients they serve.

If there’s a suspected breach, what are the investigation steps? What are the reporting requirements to states, the federal government, partners and patients?

With more patient data under their jurisdiction, life sciences companies will need to consider a number of key questions: how will patient consent be captured and recorded? What are the terms the patients have given to use the data? And how should data that is no longer needed be removed and by whom?

Cloud Platform Designed To Comply With Federal Regulations

It is plainly obvious at this point that wherever protected health information resides, it should be in a location staffed by professionals with the deepest knowledge of the government regulations that oversee patient privacy and use of protected health information. The systems that support those professionals also need to support those regulations. Rather than take on the daunting work of making such a highly regulated, highly defended environment a core competency within their own IT departments, more organizations are partnering with cloud-managed services vendors instead.

Very few of these vendors focus exclusively on the healthcare industry, leaving the customer responsible for directing, managing and training those vendors on what is needed today and tomorrow. Life science companies can benefit from teaming with a healthcare-excusive vendor, one with the required expertise—indeed, daily familiarity with—HIPAA compliance and health data security that requires a very specific and ever-evolving knowledge set.

Privacy and security aren't the only data needs for large collaborative projects. Turning the data from a compliance liability to an asset to support decisions across the continuum of care requires applications and analytics. The very top tier cloud vendors offer a combination of these services through partners to create one-stop solutions built with these make-or-break services. More on those in a later section. For now, let us turn our attention to the layered security levels within a top tier cloud vendor's data center, particularly in the context of adherence to the HIPAA Security Rule.

Critical Layers Of Cloud Compliance

The HIPAA Rule requires "covered entities" and their business associates to put in place administrative, physical and technical safeguards to secure protected health information[5]. The rising number of breaches in the healthcare industry indicates the challenge is an unmet need. Prior to the HITECH Act, many providers and practices weren't even encrypting healthcare data. Still today, many are working with aging and fragmented legacy IT infrastructure - a recipe for holes to go undetected for months or longer until the breach occurs.

IT staff availability is another consideration. IT professionals are in great demand across the enterprise - and there aren't enough of them to upgrade systems, develop applications, collect data for

[5] Summary of the HIPAA Security Rule. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

multiple department reports or a host of other ongoing duties, all while keeping a continuous eye out for a data breach attempt. And so, the hacker pounces on the unprepared.

By contrast, in a premier vendor's hosting environment, there are multiple layers of compliance internal departments simply don't have the resources to replicate. This takes a multi-layered or "defense in depth" approach to repelling a determined enemy. The core premise of this strategy is that given sufficient time and resources for an attack, at some point there will be a breach in the protection. But having layers of security—think of a castle with a moat, towers, outer walls, inner walls and a series of inner chambers—gives the defenders time to identify the breach, delay the attackers and ultimately repel the attack in order to keep the most valuable assets safe.

It is an approach that has obviously become necessary with today's determined cyber thieves in mind.

Physical Security Compliance

The HIPAA Security Rule requires covered entities to develop policies around facility access and device security. Reputable cloud vendors will be able to demonstrate their own policies for an impenetrable data center. At a minimum, these features will include:

- Controlled Secure Facility, Staffed 24/7/365
- 24/7/365 Physical Security Monitoring
- 90-Day Video Surveillance & Retention
- Cabinet/Cage Perimeter Security
- Badge and Biometrics
- Compliance Based Audit Reports
- Security Incident Response Notification

Cloud Infrastructure Compliance

Needless to say, the HIPAA rule requires covered entities to put technical safeguards in place to protect data housed in technology infrastructure. And no doubt, a proven healthcare cloud services provider will have the latest innovations available to safeguard protected health information from digital intrusion and theft. However, it is vitally important to note that security products are but one component. The reality is that successful hackers often use old techniques to successfully break into networks that may have all the latest bells and whistles in security products—but aren't being properly utilized by overextended IT staff.

To that end, an experienced cloud services vendor is hyperfocused on securing and managing valuable data, and will pair strong products with even stronger human vigilance. A sample blend of these strengths includes:

- Encryption of data at rest and in transit
- Multiple layers of hardened enterprise-grade hardware
- Advanced firewall configurations
- Real-time intrusion detection and prevention
- Private cloud environment
- Multi-tier authentication
- SSL/VPN Secure Access

Managed Services Compliance

Take note of this list—these are the data security management tasks that hackers count on internal IT staff being unable to keep up with. Often they can't. In a cloud environment, however, there is consistent focus on these activities.

- Integrity monitoring
- Intrusion detection and prevention
- Comprehensive patch management
- Security and compliance audits
- Malware protection
- Log management

Policies, Procedures and Certifications

Policies and procedures must also exceed the requirements of the HIPAA Security Rule. At a minimum, seek a cloud vendor with these credentials and credentialed professionals in place.

- HITRUST-Certified
- Onsite Chief Privacy Officer (CIPP/US, CIPP/IT Certified)
- Documented security policies and procedures
- Documented third party security audits
- Mandatory HIPAA training for all employees twice a year
- Comprehensive Business Associates Agreement to provide maximum protection

One of the arguments against moving to the cloud is the desire to protect and maintain control over data. Many CIOs feel safer when data is managed in an internal data center. Yet in today's world, it is becoming clear that the opposite is true. A HIPAA-compliant cloud provider will already have created the multi-layered approach required to secure protected health information, which CIOs can inspect and test. They will have the capabilities to secure this data at rest and in-transit, with availability that is as good as or better than keeping the data in-house.

Extending The Cloud's Reach

The life sciences industry has never had access to more potentially life-changing and industry-changing data than it does today. Yet without a way to quickly transform this data into a usable, shareable environment, many will be left behind while others go to market. By working with a healthcare-dedicated cloud provider, healthcare organizations can shorten the transformation process and get to actionable information much faster. Once a company is assured that data is protected and that data safeguards are HIPAA compliant, it can look to broaden the cloud's impact into areas such as research and development, clinical trials and even consumer engagement.

Research and development. Cloud platforms provide unique opportunities to generate insights into consumer needs. Analytics engines allow life sciences companies to sort through various types of data to determine key drivers of patient behaviors. Meanwhile, EMRs have the particularly promising potential to help identify and recruit study participants; a timely development as inclusion and exclusion criteria becomes more restrictive based on biomarkers that can be found in real patient data. Through the cloud, the cost can be reduced and contained over the long term. Your people spend time on understanding and using the data to drive decisions not managing, securing, and worrying about where it is.

Clinical trials. A trusted cloud vendor is a valuable partner for aggregating the clinical trial data generated among different entities such as research organizations, academic institutions and teaching hospitals. The compliance is centrally managed and the data is unquestionably secure within one entity, not many.

Consumer engagement. By better understanding consumer segments and their needs, life sciences companies can develop more meaningful and targeted ways to engage consumers with innovative and relevant health solutions. Without the consent, compliance, and security, consumer engagement in healthcare will remain elusive.

Conclusion

Deploying rigorous standards and best practices significantly reduces risk of protected health information loss, breach or audit. Where exactly to begin this may seem overwhelming, but the first step is straightforward - begin with a comprehensive Security and Risk Assessment. This is essentially an audit focused on protected health information security, and includes thorough reviews of IT infrastructure, processes and protocols, physical security and more.

For companies that have protected health information under their care - both covered entities and their business associates - regular risk assessments are actually a HIPAA Security Rule requirement. Yet research shows that 33 percent have never performed one[6]. The public would be troubled to learn this statistic, especially given that one in 10 Americans has now been affected by a healthcare data breach.

After the Security and Risk Assessment, the logical next step is a full Analysis and Remediation Plan that identifies all security risks and includes pragmatic recommendations for improving information security and reducing the risk of breach. Remember - this must exceed HIPAA requirements[7].

A healthcare-exclusive cloud vendor can work with internal IT departments through both of these steps, and help migrate data and infrastructure to a HIPAA-compliant cloud. On that note, make sure to choose a vendor with Business Agreements that equally share in the risk in the event of a data breach. While such breaches will be far less likely in a protected HIPAA and HITRUST-certified cloud, it is an extra measure of protection to take. Protecting patients' personal health information calls for nothing less.

[6] 2014 State of Risk Report. (2015, January). Trustwave, 4-4. Retrieved from https://www2.trustwave.com/rs/trustwave/images/2014_TW_StateofRiskReport.pdf

[7] What is Risk Assessment? Retrieved from http://www.healthit.gov/providers-professionals/security-risk-assessment

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