What Pharma Needs to Know about Compliance Regulation in the Cloud

Cloud is a staple of today's pharmaceutical IT infrastructure for cutting-edge research and development, but it presents many health data compliance challenges for adopters.

An increasing portion of healthcare is moving its business and data to the cloud. About two-thirds of healthcare technology leaders reported using the cloud or cloud services, according to a 2017 HIMSS Analytics report. Research projections estimate the global healthcare cloud computing market could approach $10 billion by 2020.

Outsourcing services to a cloud security and compliance company can help pharmaceutical organizations free up internal IT and security staff to perform work more aligned to their core competencies, rather than trying to stay up to speed on ever-evolving cloud services and regulatory requirements. It can also speed their time to market.

Time is of the essence for pharmaceutical companies when it comes to research and development and working with other researchers through the cloud can offer a secure and powerful environment for exchanging ideas and information. These collaborations can accelerate research findings and bring new therapies to market, by leveraging larger datasets, such as those used with precision medicine. What's more, many leaders in pharma already have a strong foothold in the cloud, so the rest of the industry must move quickly or risk falling behind competitively.

Leveraging the cloud can also help pharma companies outperform regulatory mandates and improve efficiency, speed, and collaboration. However, much like with other healthcare organizations and biotechnology firms, pharma companies have a wide range of regulations to consider, like HIPAA, GDPR and HITRUST.

But in healthcare, those policies and laws can be complicated and timely to navigate. By working with a HITRUST-certified managed cloud provider, these companies can help with data locality planning and compliance.

Regulatory compliance (e.g., HIPAA, GDPR, GxP) is crucial to safeguarding health data and each individual's privacy. And understanding these elements can help pharma companies navigate the healthcare regulatory system.

Cloud Guidelines for HIPAA Compliance

The Department of Health and Human Services' Office for Civil Rights released guidance around HIPAA and cloud computing in 2016. HIPAA allows covered entities and business associates to use cloud computing services for access to networks, servers, and applications.

These guidelines have implications for covered entities and business associates that create, receive, maintain or transmit protected health information. Cloud service providers (CSPs) that qualify as business associates must also comply with HIPAA requirements. Even those CSPs that exclusively store or process encrypted patient data and lack the key to decrypt the data must comply with HIPAA. However, a cloud vendor only receiving de-identified data is not a business associate as long as they maintain and store the information according to HIPAA guidelines.

While covered entities and business associates may use cloud services to store and access ePHI, they must have a business associate agreement (BAA) in place to do so. Failure to have a BAA constitutes a HIPAA violation and can result in financial penalties. As an example, OCR settled with a Florida provider for $500,000 on Dec. 4, 2018, for failing to do just that. However, those vendors must destroy or return all patient data upon termination of the contract.

GDPR Considerations

On May 25, 2018, the General Data Protection Regulation (GDPR) went into effect in the European Union (EU). Anyone in the United States that routinely interacts with EU data must comply with the rule or risk penalties of up to 4 percent of their global annual revenue or 20 million euros, whichever is greater.

The primary difference between GDPR and HIPAA is that GDPR focuses on personal rights and HIPAA centers on data — who can share it and how it is used. Those who care for or handle EU citizen data or information need to consider data flows, cross-border data transfer, and privacy and security monitoring to ensure compliance.

For many US pharma companies, the biggest challenge will be GDPR's mandate of "the right to be forgotten," or the right to erasure. The law strengthens individual rights, and organizations must honor all patient requests to erase their personal data. And GDPR extends further than HIPAA, defining personal data as any information linked to an "identified or identifiable natural person," including computer IP addresses, photos, and credit card data.

GDPR also limits how long data can be stored, outside of data not considered valuable to the law's definition of data valuable to scientific research. As a result, organizations must implement technology capable of completely erasing personal data upon request — a significant difference from US regulations where data can be stored indefinitely.

GXP and Other Considerations

In addition to national and EU laws, there are state regulations and good practice compliance frameworks when operating in the cloud. For example, there are stringent breach notification laws in some states that require companies report data breaches in less than the HIPAA-mandated 60 days.

While cloud services are generally secure, these regulations and contracting obligations complicate the process of one's due diligence when choosing your managed services cloud provider. Organizations must evaluate both platforms and vendors to ensure the secure and compliant handling of patient data.

Partnering with a healthcare-exclusive cloud provider focused on healthcare-specific security and compliance can speed your development and compliant, secure deployment in the cloud, as they are familiar with the intricacies of the applicable privacy laws and can ensure compliance.

With pharma's top companies currently drawing new insights from cloud-enabled innovation, competitors cannot afford to ignore what has become a staple of today's pharmaceutical IT infrastructure for cutting-edge research and development.

About ClearDATA

Healthcare professionals across the globe trust the ClearDATA HITRUST 9.1 -certified cloud to safeguard their sensitive data and power their critical applications available across the major public cloud platforms. For healthcare organizations, customers receive one of the most comprehensive Business Associate Agreements (BAA) in the industry, combined with market-leading healthcare-exclusive security and compliance solutions. ClearDATA's innovative solutions protect customers from data privacy risks, improve their data management, and scale their healthcare IT infrastructure, enabling the industry to focus on making healthcare better by improving healthcare delivery.