PharmaForce IQ

Why SaaS companies in the pharmaceutical industry must be vigilant of data privacy laws

Business | Science

As hackers upturn the business world, SaaS (software as a service) firms entrenched in pharmaceuticals must ensure the utmost diligence be exercised in regard to data security. Pending consequences for business missteps in this regard can prove catastrophic, not only for the company, but also for the individuals whose personal information has been entrusted to said company. Clients see operation within the esteemed realm of medicine as assurance of confidentiality, but that isn't always the case.

To that end, there exists several key data measures within the pharmaceutical industry that companies must adhere to. Such measures include, but are not limited to, the implementation of strong security protocols, the adherence to relevant laws and regulations, the conduct of regular risk assessments, the provision of employee training on data privacy and security, and the establishment of clear policies and procedures for handling data.

In terms of regulatory bodies, companies within the pharmaceutical trade may be subject to a range of oversight depending on their location and the specific laws and regulations applicable to their business. Health regulatory bodies, data protection authorities, and industry-specific regulatory bodies are just a few examples of the entities that these companies may have to answer to.

It bears mentioning, stakes are high when it comes to data privacy, regardless of industry. However, big pharma does not tread lightly in the wake of any violations. There have been numerous instances of SaaS companies breaching privacy laws. Industry giant, Pfizer suffered a breach in 2020 after a misconfiguring a Google Cloud database that exposed the personal and medical information of millions of customers, causing the loss of patient names, addresses, and birth dates. The fallout of this breach was significant, not only putting customers at risk of identity theft, but also damaging the company's reputation

and undermining public trust in its ability to uphold general checks and balances. In 2018, Merck experienced a cyber-attack that resulted in the theft of research and development data, as well as employee and customer information, disrupting the company's operations and leading to considerable financial losses in both operating power and market value. Similarly, Bayer and Roche underwent a data breach in 2018, facilitating the exposure of sensitive data banks, the majority of which held insurance records. Victims of the aforementioned attacks went largely unscathed, however, most had to reconvene under troubling circumstances and at some expense.

Incidental damage caused by such a calibre of breaches can be irreparable, not just in terms of financial losses, but also in terms of public trust and confidence. It is therefore imperative that firms operating within this industry specifically, take all precautionary measures to safeguard sensitive data and ensure compliance with relevant laws and regulations. This may include the employment of encrypted data storage to safeguard sensitive information, the regular updating of software and security protocols to stay ahead of potential threats, and the implementation of stringent access controls to prevent unauthorized access.

Coinciding with recent innovations in data mining tools and technologies, clear policies and procedures for handling data must be updated on a yearly basis to account for fields that have yet to be harvested. This process may include the creation of policies for the collection, storage, and sharing of data, and not limited to the establishment of procedures for responding to data breaches or other security incidents, as other industries undertake heavier reliance on data as a conventional backbone.

As the pharmaceutical industry amalgamates data caches, the handling of sensitive data grows increasingly crucial. In order to safeguard against potential data breaches and protect the integrity of their information, it is essential for organizations within this sector to implement robust security measures.

Methods to Achieve Effective Data Security for SaaS Companies

One effective means of achieving this is through the use of technical security assessments such as HITRUST, SOC, HIPAA, and penetration testing. These assessments provide a comprehensive evaluation of an organization's systems and processes, identifying vulnerabilities and weaknesses and offering guidance on how to address them.

The Health Information Trust Alliance (HITRUST) framework, for instance, is specifically designed to protect sensitive healthcare data, offering a standardized approach to security that organizations can utilize to assess their current practices and identify areas for improvement. Similarly, a System and Organization Controls (SOC) assessment helps organizations understand their risk profile and identify potential areas of weakness, while HIPAA assessments ensure compliance with the Health Insurance Portability and Accountability Act's requirements for the protection of personal health information.

Penetration testing, also known as "pen testing," stands as another valuable tool in the arsenal of security measures. This process involves simulating a cyber-attack on an organization's systems and processes, enabling experts to identify vulnerabilities and weaknesses that could be exploited by malicious actors. By understanding the risks they face and implementing measures to mitigate them, organizations can significantly reduce the likelihood of data breaches and other security incidents.

Technical security assessments are not only vital for organizations operating within the pharmaceutical industry, but in any industry. Given the growing dependence on technological channels, the practice allows business to safeguard sensitive data and protect against potential security breaches. Big pharma does business across the world, often overstepping industry borders and dipping toes in territory untried by smaller, independent firms. Leveraging tools such as HITRUST, SOC, HIPAA, and penetration testing, streamlines a management strategy that maintains security posture and intel integrity.

The handling of sensitive data is a fundamental aspect of the daily operations, and as such, it is imperative that all employees are properly trained and equipped to uphold the stringent data privacy and security protocols that are necessary for the success and integrity of the company.

It is for this reason that such a premium is placed on the use of data privacy and security training materials, both as part of the onboarding process for new employees and as a regular part of ongoing employee training initiatives. Whether it be in the aftermath of a security incident, the introduction of new technologies or processes, or simply as a means of reinforcing best practices, these materials serve as a crucial resource in ensuring that all employees are well-versed in the proper handling and protection of sensitive data.

Highly competitive and fast-paced, the nature of the pharmaceutical industry requires that this practice remains at the forefront of legal developments and regulations related to data privacy and security. Thus, its essential that employees are provided with the knowledge and tools necessary to navigate this evolving landscape, and to remain in compliance with all relevant legal and ethical standards. By prioritizing the appropriate handling and protection of sensitive data, companies are able to uphold the very highest of standards.

Conclusion

As aforementioned, blunders in adhering to laws related to data privacy can lead to costly penalties and a negative perception of the business. In order to ensure that they are operating in accordance with these regulations, companies in the pharmaceutical sector that utilize Software as a Service will benefit from seeking policy guidance from regulatory agencies such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA) in Europe, as well as consulting with legal professionals and implementing robust data protection strategies such as encryption and secure data storage. It is imperative that SaaS companies remain informed about current developments in data privacy legislation and take proactive measures to guarantee compliance in order to safeguard the confidentiality and security of their data, and thus, their customers.

When engaging with clients, all our account managers and team leads are trained to discuss PharmaForceIQ's extensive data security and privacy standards and policies put in place to ensure the utmost compliance standards.