The Importance of Data Security for Healthcare Life Sciences Enterprises

October 13, 2021
Ashish Kaushik, CISO, SourceFuse Technologies

Ashish Kaushik is the CISO at SourceFuse Technologies. Ashish has an overall 13 years of experience. He started his career as a hardcore Programmer full time right after his studies and gained interest in Security Domain to help enterprises lay down a robust security practice. He has served as Security Analyst for various pentesting engagements related to network, infrastructure and application security. He has achieved several AWS Certifications, including the AWS Solution Architect Professional Certification, and was handpicked as an AWS APN Ambassador.

Why Healthcare Data Matters

Healthcare data is amongst the most sensitive and highly confidential information being accessed and processed on a daily basis. Not only does it contain private medical records, but it also contains personal information that could lead to a major incident if leaked – full name, home address, contact number, email, insurance details, and even bank details – a potential cyber criminal's dream.

Coupled with the fact that medical records need to be stored for such a long period, it is no wonder, then, that such stringent security legislation exists. The minimum length of time for retaining medical records varies between countries, ranging from three to eight years for adults, and 15 to 30 years for minors, with the British Medical Association going as far as saying: "*Electronic patient records (EPRs) must not be destroyed, or deleted, for the foreseeable future.*"

With the use of cloud computing in the healthcare industry predicted to grow at a CAGR of 18.1% by 2025, and around 37% providers opting for hybrid cloud solutions, the exponential increase in the amount of electronic data needing to be stored 'indefinitely' is exploding. More than ever before, as more healthcare organizations migrate from on-premise setups to the cloud, or take the hybrid approach, the number one priority has to be data security and compliance.

Healthcare Data and Cloud Security

Digital transformation within the healthcare industry has revolutionized how care providers and professionals can access, process and analyze the immense quantities of data contained in electronic health and medical records (EHRs and EMRs). Protecting data from unauthorized access and data corruption is key to avoiding the inconvenience and upheaval of lost data, financial or even criminal penalties, loss of reputation and patient trust, and associated costs involved with data recovery.

The regulatory standards, such as HIPAA and GDPR, can help. HIPAA has The Security Rule, which requires healthcare professionals to protect EHRs/EMRs through administrative, physical and technical safeguards, and GDPR stating 'appropriate technical and organizational measures' should be taken. The 'technical' part places great responsibility on cloud solution providers, and rightly so – this should be their area of expertise. The ability to keep pace with the up-to-date regulatory compliances, deploying the very latest in cyber-security software, and implementing cutting-edge technology, will all support data security risk mitigation, leaving healthcare providers to concentrate on patient care.

Data Security Technology

When it comes to working in a cloud environment, the security landscape is primarily focussed on concerns around infrastructure, inventory and configuration, encryption, denial-of-service risk mitigation, monitoring and logging, and penetration testing. Factoring in the need to adhere to industry regulations and policies, while managing scalability and TCO, it emphasizes the requirement for high tech, reliable and credible solutions. According to Amazon Web Services, the various cloud security services available fall within five broad categories, under which there is a wealth of proven security technology:

1. Identity and access management – ensures only authorized users or groups are granted permission to access specific services and resources. Additional layers of multi-factor authorization includes management of who has access to what data (AWS IAM), controls sharing permissions (AWS Resource Access Manager), and governs application identity (Amazon Cognito)
2. Detection – the ability to track user activity and monitor behaviour (AWS CloudTrail), detect data security threats (Amazon GuardDuty), continuous monitoring of resource configurations (AWS Config), and maintaining a unified security and compliance center (AWS Security Hub)
3. Data and Infrastructure Protection – continuous monitoring and customizable 'rules' to initiate proactive responses. Safeguarding data from prohibited access is achieved through controlled encryption management (AWS Key Management Service), automated encryption key rotation (AWS Secrets Manager), and the ability to shield cloud applications against the most recurrent targeted attack (AWS Shield)
4. Incident Response – analyzing, detecting and troubleshooting security issues, as well as the ability to track and automatically respond to data security threats (Amazon Detective). It also includes assessing data recovery competencies (CloudEndure Disaster Recovery)
5. Compliance – ensuring regulatory compliances are adhered and risks effectively managed, through automatic or on-demand reporting (AWS Artifact), and continuous monitoring and auditing (AWS Audit Manager)

That's a lot of technology to consider! However, cyber security experts exist that can ease the process by assessing your needs, and bringing together only the appropriate pieces of the jigsaw for *your* organization. For example, TrendMicro is a leader in cloud and enterprise cyber security, whose unified platform delivers central visibility for better, faster detection and response, and a powerful range of advanced threat defense techniques optimized for environments, such as AWS, Microsoft, and Google. Organizations such as TrendMicro, with deep security expertise and dedicated to global data security research, can help make the world a safer place for exchanging digital information.

Examples of Successful Cloud Migration for Healthcare Data

When all is said and done, integrating healthcare data in a secure platform can achieve analytical insights to enhance patient care and improve outcomes, streamline organizational processes, reduce errors, lower costs, and monitor health trends on a national or global scale. Some healthcare organizations are already benefiting from increased levels of data security, as in the following examples.

1. One leading pharma organization identified many unmet needs of patients undergoing cancer treatment, their care teams and caregivers. With extensive and complex treatment paths, engagement between the patients and their care teams throughout this time is vital, which drove the development of a ground-breaking HIPAA compliant custom application. Patients and care teams are able to collaborate better and work towards improving treatment outcomes, while data privacy is 100% guaranteed. Read More.
2. One of India's largest providers of integrated world class healthcare services was looking to automatically extract and consolidate data from 1000+ e-prescriptions per day. The HIPAA and GDPR compliant custom application automated manual processes to improve efficiencies, deployed free-text recognition, delivered real-time updates, and provided cost optimization for scalability. Read More.

Content Disclaimer

© 2024 CXO Outlook. All rights reserved.