HealthManagement
Promoting Management and Leadership

The Growing Threat to Healthcare Data: Addressing File-Sharing Vulnerabilities

In today's digital age, healthcare data is under unprecedented threat. The year 2023 saw a staggering one in three individuals in the U.S. affected by healthcare data breaches, highlighting the severity of cyberattacks targeting this critical sector. These breaches not only expose individuals to identity theft and other cybercrimes but also tarnish the reputation of healthcare organisations. With stringent regulations like HIPAA and GDPR in place, the failure to secure sensitive data can result in hefty penalties. A recent report from Metomic explores the vulnerabilities in healthcare file-sharing practices, the types of data at risk, common file-sharing mistakes, and the importance of Data Loss Prevention (DLP) solutions.

The Types of Sensitive Data at Risk

Healthcare organisations manage a vast array of sensitive data, making them prime targets for cybercriminals. Among the most critical types of data to protect are:

1. Protected Health Information (PHI): This includes health records, treatment information, and payment data that can identify individuals. PHI is essential for patient care but must be rigorously protected to comply with various data protection regulations.
2. Personally Identifiable Information (PII): This encompasses personal data such as names, addresses, and Social Security numbers. Protecting PII is crucial to prevent identity theft and comply with privacy laws.
3. Payment Card Information (PCI): Financial details like credit card numbers and banking information require stringent security measures to prevent fraud and ensure regulatory compliance.

Additionally, healthcare organisations must safeguard sensitive credentials, such as access keys and passwords, and commercially sensitive business data, including trade secrets and strategic plans. The relative importance of these data types varies across organisations, but all must be securely managed to prevent cyberattacks and comply with regulations.

Common File-Sharing Mistakes in Healthcare

Healthcare organisations often inadvertently expose sensitive data through insecure file-sharing practices. One of the most significant issues is the public sharing of files, particularly those containing PII. For instance, 25% of publicly shared files in healthcare organisations include PII, creating a substantial risk of data breaches. This can occur due to employee oversight, such as not revoking permissions after sharing files or misunderstanding the security capabilities of cloud providers.

Another common mistake involves exporting sensitive data from internal systems to personal drives or publicly accessible locations. Employees may do this to perform specific tasks, such as analysing customer data or conducting tests, without considering the security implications. Sharing files with external parties, like contractors or clients, without proper oversight also increases the risk of unauthorised access.

Even files shared within a company's domain or stored on private drives can pose risks if not adequately monitored. For example, passwords and other sensitive credentials are sometimes found in shared files, which could lead to significant security breaches if accessed by malicious actors.

The Role of Data Loss Prevention (DLP) Solutions

Given the high stakes, healthcare organisations must adopt robust measures to secure their data. This is where Data Loss Prevention (DLP)

solutions come into play. DLP platforms like Metomic are designed to automatically detect and mitigate the risks associated with the exposure of sensitive data. These solutions can identify where sensitive data is located, who has access to it, and take automated actions to safeguard exposed information.

Key features of an effective DLP solution include ease of use and deployment, comprehensive visibility into sensitive data across various SaaS applications, and the ability to generate detailed reports at both high and granular levels. Additionally, DLP tools should provide real-time redaction capabilities, correct authorisation protocols for data sharing, and timely alerts to both employees and IT teams when potential security issues arise. Good customer support is also essential to ensure that organisations can effectively utilise these tools.

The healthcare sector faces a critical challenge in securing sensitive data amidst increasing cyber threats. The exposure of PHI, PII, and PCI through insecure file-sharing practices poses significant risks to both individuals and organisations. To address these vulnerabilities, healthcare companies must prioritise implementing robust data security measures, including using advanced DLP solutions. By doing so, they can better protect sensitive data, maintain regulatory compliance, and uphold the trust of their patients and clients.

Source: METOMIC

Image Credit: iStock

Published on : Thu, 25 Jul 2024