Best Practices for Safeguarding Patient
Records and Sensitive Information

White Paper

Best Practices for Safeguarding Patient Records and Sensitive Information

Symantec™

Symantec™

Best Practices for Safeguarding Patient Records and Sensitive Information

CONTENTS

Brought to you compliments of

Symantec™

When a health system suffers a data breach, it can cause serious and irreversible damage to patients, employees, third-party partners, the business and the trusted relationship between patients and their care providers. The trouble is, health data and other sensitive information stored in health provider systems by nature needs to be shared with other entities. For example, in the course of treatment, protected health information (PHI) can travel between medical and finance departments, other practices, family members and third-party entities such as insurance companies and home health agencies. All the while, health systems are legally bound to protect confidential information while coordinating care and payment.

TechTarget® Custom Media

A TECHTARGET WHITE PAPER

The need to share data isn't the only problem. Sensitive information is stored at all levels of healthcare organizations, and there's so much new, unstructured data being generated every day that it can be difficult for IT administrators to know where it all resides and how and by whom it is being used. Judging by the rising number of data breaches—and ransomware attacks resulting in hospital shutdowns—health systems are seriously lagging when it comes to safeguarding patient records and other sensitive data. In fact, healthcare records of more than 112 million individuals were compromised by data breaches in 2015, according to the U.S. Department of Health and Human Services.[1]

The need for security without complexity

The healthcare industry is facing serious pressure to change its defense strategies and behaviors. Drivers for change include:

- An increasing need to share data with patients, third parties and other entities.
- Escalating HIPAA audits.
- Growing concerns about malicious insiders, including people who access PHI out of curiosity, or for identity theft or other fraudulent reasons.
- A surge in large breaches and attacks.
- Federal and state privacy regulations that levy large and increasing fines for violations.
- Increasing consumer choices for care.

Though the risks of having an insufficient security strategy continue to mount for the healthcare industry, security budgets and staffing are often insufficient to meet the formidable challenges. Reliance upon point products is one way healthcare IT has attempted to combat data breaches, but such security solutions can actually add to the complexity of already cumbersome and complex systems.

For healthcare IT, the ideal solution will increase security without increasing complexity or hindering data sharing or clinician workflows.

Best practices for safeguarding patient records and sensitive information

The fact is, typical user ID and password security can no longer deter hackers. Multifactor authentication (MFA) for accessing data, apps and services is a key requirement for

[1] "Hackers accessed medical records of 1 in 3 Americans in 2015," *Health Data Management,* Feb. 1, 2016

healthcare IT, especially for remote access or critical functions such as electronic prescribing of controlled substances.

As the term suggests, traditional MFA requires more than one method of authentication to verify a user's identity. It combines two or more credentials that are independent of each other: something the user knows, such as a password; something the user has, such as a security token; and something the user is, such as biometric verification. If one of the authentication methods is compromised, there are other layers of defense.

MFA is implied and required by federal and state mandates because it helps IT determine what data can be accessed and by whom. In a healthcare setting, it's important that MFA is implemented in a way that doesn't inhibit efficient data sharing or patient care, and it must be easy for clinicians and administrative staff to adopt.

Other best practices include identifying where confidential information is stored and monitoring who is accessing it, from where, on which devices, and how it's being used. Once you've located the confidential data in all of your environments, you can secure and protect it when it's at rest and when it's being transmitted.

Manage and protect sensitive data, on-premises or in the cloud

For health systems, moving to the cloud has obvious benefits, including cost savings and scalability. However, security and complexity concerns have slowed adoption. Symantec offers a broad portfolio of security solutions designed to help healthcare IT manage and protect sensitive data, whether on-premises or in the cloud.

Data loss prevention and encryption

Data loss prevention (DLP) and encryption offerings allow you to monitor and protect confidential information wherever it is stored and however it is used.

- Described content matching technology looks for matches on regular expressions or patterns.
- Exact data matching identifies sensitive data directly in your database.
- Indexed document matching applies a full file fingerprint to identify confidential information in unstructured data, such as PDFs, multimedia files and JPGs.
- Vector machine learning automatically learns and identifies the layout of sensitive document types.

- File-type detection recognizes more than 330 different file types, including email, graphics and encapsulated formats, as well as virtually any custom file type.
- Local scanning and real-time monitoring keeps data safe on Windows and Mac endpoints. This includes monitoring confidential data that is being downloaded, copied or transmitted to or from laptops and desktops through email or cloud storage.
- DLP monitoring and protection extends to iOS and Android devices, whether corporate- or user-owned.
- Scanning network file shares, databases and other enterprise data repositories identifies and protects confidential unstructured data.
- A single Web-based console lets you define data loss policies, review and remediate incidents, and perform system administration across all endpoints, mobile devices, cloud-based services, and on-premises network and storage systems.
- Robust workflow and remediation capabilities streamline and automate incident response processes.
- A broad, comprehensive encryption portfolio provides maximum protection and increased security with DLP.

Hosted DLP Cloud Service for Email

Hosted DLP Cloud Service for Email allows you to quickly transition to the cloud and securely adopt software-as-a-service applications, such as Office 365 or Gmail. Cloud Service for Email provides real-time protection with automated response actions such as message blocking, redirection and encryption capabilities. It allows you to prioritize real incidents with accurate monitoring and analysis, and respond faster with one-click responses and automated workflow. Enforce data loss policies across both cloud and on-premises mailboxes with sophisticated policy authoring.

Validation and ID Protection

Validation and ID Protection (VIP) service ensures that only authorized users can securely access clinical and IT systems. This enables strong multifactor and risk-based tokenless authentication that eliminates up to 80% of breaches. VIP enhances existing static passwords by positively identifying users with a dynamic second factor of authentication that cannot be predicted or stolen. VIP can adapt to nearly any network, cloud or mobile app with built-in integrations.

Conclusion

Healthcare IT environments move and contain enormous amounts of sensitive data. This data is so valuable on the black market that healthcare has become the most targeted industry in the world. It is also one of the most regulated industries. When a health system suffers a data breach, there are serious consequences, including fines, brand damage and irreversible damage to patient well-being. However, to provide effective patient care, health providers must share data efficiently with other entities. Symantec's portfolio of security solutions allows health systems to enable all of the technology and workflows clinicians and administrators need while protecting sensitive data, both on-premises and in the cloud, at rest and in transit.

More Information

Visit our website

www.symantec.com/healthcare

Contact Us

1-855-487-1449

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com