SailPoint

SOLUTION BRIEF

The Blueprint for **Securing HIPAA-Related Data**

An estimated 80 percent of all the data in the world is stored in files that are typically unsecure. Furthermore, many healthcare providers have no visibility into where these files reside, what each file contains and who can access this data. For organizations that manage highly-regulated, extremely-sensitive patient data, this creates significant cybersecurity vulnerabilities and risk that cannot be ignored. If you don't know where sensitive data resides, you cannot protect it. For this reason, providers need identity governance capabilities that extend beyond databases and applications. They need visibility and control of data files that can be stored in less secure locations such as network file shares, SharePoint and cloud drives.

Understanding the Data Lifecycle

The collaboration and sharing of information needed by modern healthcare organizations to deliver excellent patient care can create blind spots where sensitive data is not well-protected. One of the most significant examples of this occurs during the data lifecycle.

As patient data and other sensitive information are extracted from applications and databases, it is often manipulated and saved in file formats such as PDFs, presentations, text documents and spreadsheets. These files may be edited further, resulting in multiple versions being stored in a variety of locations, and some of these locations may not be secure. Here are just a few examples of how this happens:

Copied and Pasted Information

- A clinician conducting a research study may copy and paste medication administration or flowsheet data from the Electronic Health Records (EHR) system into an application such as Word, PowerPoint or Excel for tracking.
- An assistant may copy and paste historical data for the day's scheduled visits into Word for a provider's consumption outside of the EHR.

Reports

- The provider organization's Health Information Management department may run a real-time operational report for auditing purposes. The report may be later saved to a network drive for future reference.
- Overnight EHR batch reports may be run and distributed on a network drive or SharePoint site.

Scanned Documents

- Insurance cards and other enrollment paperwork may be scanned when the patient is admitted. Later, it may be downloaded by Patient Financial Services to work on the file.
- Occupational Health records not stored in an EHR may be scanned and stored in folders on a network drive.

With 80% of all data located in digital files across the health system, providers must exercise precision in securing the most sensitive data.

Three Steps for Securing Files Containing PHI

Once you understand the challenges associated with governing HIPAA-related information and other sensitive data, you can begin to build a game plan for securing it. HIPAA has very specific rules defining what type of information and/or combination of information need to be protected. It also defines significant financial consequences for failing to secure that information from unauthorized access by individuals or groups. With the fine of up to $1.5 million per violation per year, the healthcare industry witnessed $23 million in HIPAA settlements in 2016 alone. For this reason, healthcare providers would be wise to track down and govern access to any files containing HIPAA-related data. Here are three essential steps for doing so:

1

Step 1: Discover and Prioritize

The amount of sensitive data stored in files is growing at an exponential rate. Just locating data files, much less managing access to that information, can be overwhelming and lead you to a sense of ineffectiveness. To streamline efforts and minimize impact on IT resources, a targeted approach is far more reasonable and achievable. Rather than boiling the ocean, providers should conduct comprehensive discovery and flag files that contain sensitive content. This enables them to prioritize efforts, and exercise precision in securing HIPAA-related information and other sensitive data.

2

Step 2: Assess Who and What

Analyze who has access and who is accessing the data (employees, contractors, vendors, business partners, etc.). While these two groups may overlap, they are not necessarily the same. To control and govern access to sensitive data, it is critical to build out a model that correctly identifies users who have business justification to access specific types of sensitive data. Providers will want the ability to automatically compare the actual state-of-access with the desired state and eliminate over-entitled users on a regular basis. This can be formed through regular access review processes, or more automated reconciliation tasks. This assessment will help set the foundation of critical governing policies moving forward.

3

Step 3: Empower Data Stewards

Who in the provider organization would have the best understanding of which users should have access to what and when? While IT departments often end up with the responsibility, they rarely know the data or the users. On the other hand, data stewards have contextual understanding of the data and users, as well, the bandwidth to govern access. For these reasons, it is essential that provider organizations determine and designate data stewards.

As you set policies around access, it's important to ensure the processes for granting and validating access are conducive for the desired security results, while minimizing impediments to the users' day-to-day operations.

SailPoint's Advantage

SailPoint helps healthcare providers eliminate cybersecurity and compliance risks with a comprehensive identity governance solution that applies to all data wherever it resides. Our approach streamlines the process for finding HIPAA-related data and other sensitive information in files and documents located throughout the hospital or across the entire health system. We further enable IT administrators and data owners to prioritize and focus on managing data that poses the greatest healthcare compliance and cybersecurity risks.

Furthermore, SailPoint is recognized by Gartner and Forrester as the leading authority in identity governance and administration. This is essential because knowing and governing identities is a central tenet to protecting sensitive information and ensuring reasonable freedom of access for those who legitimately require information as part of their daily workflow. Below are some benefits we can provide to organizations:

Enhance Visibility into HIPAA-related Information and Other Sensitive Data

- Locate and classify sensitive data based on content or who is accessing data
- Support more intelligent governance decisions with deeper insight about users and access that provide complete identity context
- Monitor on-premises and cloud data access in real-time

Drive Compliance with Corporate and Regulatory Requirements

- Help drive compliance with proven policies, rules, and search expressions (e.g. SSN, disease codes) designed to support HIPAA regulation
- Streamline access reviews and certifications to quickly respond to audits and maintain compliance
- Maintain a real-time health status across all governed data sources and take action on potential compliance risks

Establish Governance Control with Business Accountability

- Utilize targeted crowd-sourcing to more accurately identify owners responsible for sensitive data
- Ensure only authorized users (defined by HR, IdentityIQ/IdentityNow or role modeling) are provided access with streamlined access requests
- Detect and respond to policy violations in real-time with automated alerts

Remediate Risk with Actionable Intelligence

- Enable IT, security, and business users to identify and remediate risk with actionable dashboards
- Address permissions creep and establish one permission path per user with access normalization and cleanup
- Avoid human errors while reducing IT workload with automated access fulfillment

If you are interested in learning how our solutions can help your provider organization locate, secure and manage sensitive data and files, **contact us to set up a demonstration**.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries, including: 6 of the top 15 banks, 4 of the top 6 healthcare insurance and managed care providers, 8 of the top 15 property and casualty insurance providers, 5 of the top 15 pharmaceutical companies, and six of the largest 15 federal agencies.

SB1181-1710