eBOOK

Data Security:

The Business Case for Taking Control of Healthcare Data Sprawl

SailPoint

Healthcare is a prolific generator of data. In 2018, healthcare organizations generated 8.41 petabytes of data–a roughly tenfold increase over just two years earlier.[1] Industry consolidation, increasingly sophisticated medical technologies and a decade-long drive to digitization are just some of the drivers leading to larger data files.

What's more, healthcare data can be infamously messy. Only about 20% of protected health information (PHI) sits neatly in structured data repositories, where hospitals tend to direct most of their data access and monitoring efforts. The rest is unstructured protected health information such as faxes, clinician notes and radiological images.[2] These records can be found on diagnostic machines, desktop analytics programs, chatbot programs–almost anywhere electronic data can be stored.

In other industries, organizations can lighten their data load by simply disposing of records when they're no longer needed. Not so much for hospitals and providers. Healthcare organizations are subject to data retention rules that limit their ability to reduce the amount of data they store. If that isn't complicated enough, there is no single, standardized record retention schedule for providers to follow. At the federal level, the statutory requirement is for providers to keep records for a minimum of five years.[3] However, states and agencies may require even longer record retention timelines, prompting some medical associations to recommend that hospitals retain medical records indefinitely.[4] Without a data access governance (DAG) solution, managing all this sensitive data is like playing the classic video arcade game Frogger[5]. Security officers are constantly crossing busy intersections of data streams, navigating new apps and platforms, all while staying compliant with Health Insurance Portability and Accountability Act (HIPAA) guidelines for safeguarding PHI. A leap in the wrong direction just might open the door to a data breach.

It doesn’t have to be that way. In this eBook, we look at three business cases where DAG has helped organizations protect PHI data. In each case, we break down specific ways a DAG solution can get unstructured data under control by enabling continuous access governance, usage tracking and policy enforcement across all users, apps and data. Browse the sections in the order they appear or skip directly to the one that’s of greatest interest.

Use Case 1:
Securing Access to Your Cloud

Use Case 2:
Heading Off Data Breaches

Use Case 3:
Consolidating Active Directory Environments

Starting the Journey
to Data File Protection

Use Case 1: Securing Data Access to Your Cloud

A key selling point of cloud-based IT services is the scalability they offer. Gone are the constraints of an on-premise implementation, with its hardware footprint and capital expense. With cloud technologies, hospitals can adjust capacity to accommodate surges in demand and the needs of their growing business. Data sharing and collaboration across satellite offices and campuses become significantly easier.

At the same time, cloud computing raises new implications for electronic PHI (ePHI) security and data management. The scalability of the cloud coupled with ease of implementation means additional pools of data outside the traditional purview of the information technology team. By the same token, cloud applications have been widely praised for fostering interdepartmental collaboration. That improves operational and clinical coordinate across the continuum of care, from appointment scheduling to bill payment. But seamless collaboration can mean more individuals have access to ePHI–access that may not be readily visible to the organization.

Even the cloud's cost-effectiveness has a flip side. **As more healthcare organizations store their data in the cloud, the process of transferring it from one server to another—or making it available for users to take action—can create the conditions for a data breach.** Similarly, letting petabytes of inactive data sit in cloud storage can make it a target for cyberattacks.

Healthcare organizations need to ask themselves: Are they truly optimizing the full benefits of their cloud investments? It's fair to say that most providers are only beginning to understand that investing in cloud infrastructure requires constant security vigilance and data due diligence. That extends to retention requirements and the activities and functions requiring routine access for each record type. With SailPoint's File Access Management solution, providers can proactively manage access to the files they opt to store on the cloud, both the ones they have now and the new files they'll add in the future. That includes knowing where the data is stored, who has access to it, how often they access it and how that access is used.

Use Case 2: Heading Off Data Breaches

The typical healthcare delivery system is home to hundreds of data processing systems containing information such as prescriptions, procedural codes and bank account information. Some data–such as street address or the three-digit card verification value (CVV) number on a credit card–may not amount to PHI by itself. Combined with other data, however, it becomes possible to create a holistic view of an individual that can prove devastating in the wrong hands.

It's no surprise, then, that hospitals are a lucrative target for cyber criminals. Ransomware attacks account for nearly 50% of the data breaches that occur in the healthcare sector.[6] For example, the hackers responsible for the Ryuk ransomware bug specifically targeted healthcare organizations by corrupting or partially destroying data files.

That said, **roughly 21% of all healthcare data breaches reported to the Office of Civil Rights are related to unauthorized access or disclosure.**[7] Often such breaches are unintentional and stem from an individual inadvertently using unsecure collaboration tools to share documents that contain sensitive information.[8]

A data access governance solution provides visibility into all data access, not just the kind that takes place inside a structured system. The DAG solution can recognize patterns indicating a security event, like rapid changes to a file extension (a hallmark of Ryuk ransomware). Identity security experts can also configure a predetermined response to keep the source of the activity from entering the organization.
If the activity originates from inside the organization, DAG can track the individual and what they accessed, and take steps to reduce that individual's exposure.

Use Case 3: Consolidating IT Environments

The wave of business combinations in healthcare is continuing. By 2019, 67% of U.S. hospitals were affiliated with a multihospital or single diversified hospital system.[9] Transaction value is going up as well, with more mergers and acquisitions taking place between larger health systems.[10]

The healthcare executives who negotiate these deals have their eye on finding synergy in the relative strengths of consolidating entities. However, the combined business will rely on IT to drive value-based care and reduce operational costs. As a result, much of the real work of a merger begins only after the transaction has closed, when organizations confront the data ramifications. Often these relate to the underlying strategy that led to the tie-up, creating entities that are much larger targets for cyberattack. Broaden physician networks and expand access to patients can lead to more identities, more data creation and more files to manage.

Sometimes, an acquired organization has been in financial distress or for other reasons deferred investments in staffing and health information technology. DAG is particularly urgent in these situations since **disparate or older technologies can be weak links in the organization's overall data security.** The potential for data hygiene can also increase when the organization is preoccupied with finalizing a complex merger and acquisition process or moving new identities and permissions into another system.

For many organizations, the question becomes what to do with the data and permissions that were inherited. Often security and information executives have little bandwidth to investigate where their acquisition's sensitive data could reside. In these situations, the permissions collection and reporting capabilities of SailPoint's data access governance solution can make sense of complex data environments and help hospitals quickly gain control.

A typical scenario is when merging organizations consolidate their Active Directory environments. The hospital wants to make sure that none of the acquired health system's email addresses remain in the directory. They likely have other pre-existing policies to follow as well. DAG provides a way to identify those permissions and attributes, then tie them into the identity management platform with minimal manual intervention.

SailPoint's Three Pillars of Data Access Governance

An effective approach to data security rests on three pillars:

Data classification, or locating sensitive data

Permissions analysis, or understanding who has access to all the assets

Activity monitoring, or seeing what users are doing with that access

The pillars allow hospitals to track the location of sensitive information, control who has access to sensitive information and monitor user actions on sensitive folders and shares. Together, they form the basis for protecting your organization's sensitive data from unnecessary and unrestricted access.

Bringing Visibility and Control to Unstructured Healthcare Data

Healthcare data breaches are rising in number and severity. That's partly due to the volume and variety of data that healthcare entities collect. Another contributor is the sprawling array of networks, applications, platforms and BYOD devices. All this creates fertile ground for the misplacement and inadvertent sharing of sensitive data.

So how can healthcare organizations get started on securing their unstructured PHI?

Find and classify the data

Use a data discovery tool to **inventory and map the connections between different data sources.** This can help to determine what processes and solutions should be implemented to protect sensitive information.

Identify the data owners

A robust DAG solution can **automatically detect those who access a data resource most frequently.** Consider holding an "election campaign" in which the top users vote for the person they believe should be the steward of that particular resource.

Empower the data owners

These are the users who are most familiar with the data. **Delegate governance** responsibilities to them rather than leave it up to the IT or data security team (who may be forced to make arbitrary decisions about who should have access).

Remove barriers to collaboration

Bring business users, data owners and other stakeholders into your review processes for access certifications and requests. Have them **work together to manage and maintain the sensitive data** they're responsible for.

Data access governance is a balancing act–one that requires risk management and business enablement capabilities. A comprehensive and systematic approach to data security helps hospitals drive new care coordination models, expand revenue streams and improve operational decision-making. In other words, it sets your organization up for success by bringing visibility and control to your organization's most important decision-making tool: data.

How can SailPoint help?

We give your business unmatched visibility while automating and accelerating the management of all user identities, entitlements, systems, data and cloud services.

If you need help with managing PHI data sprawl, please contact us.

[1] Wall Street Journal, Melanie Evans, "Hospitals Give Tech Giants Access to Detailed Medical Records," January 20, 2020.
[2] Breakthrough Analysis, Seth Grymes, "Unstructured data and the 80 percent rule," August 1, 2008.
[3] Centers for Medicare and Medicaid Services, "Conditions of Participation," 42 CFR 482.24(b)(1), accessed on March 29, 2021.
[4] California Medical Association, "Retention of Medical Records," Document #4005, accessed on March 26, 2021.
[5] FROGGER® is a registered trademark owned by Konami Digital Entertainment Co., Ltd.
[6] ZDNet, Danny Palmer, "Ransomware attacks now to blame for half of healthcare data breaches."
[7] U.S. Department of Health and Human Services Office for Civil Rights, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," accessed on January 26, 2021.
[8] Fierce Healthcare, Heather Landi, "Many organizations are careless-sensitive paper documents-it-s-putting," September 30, 2019.
[9] American Hospital Association, "Fast Facts: U.S. Health Systems," accessed on March 17, 2021.
[10] Deloitte and Healthcare Financial Management Association, "Hospital M&A: When done well, M&A can achieve valuable outcomes," accessed on March 26, 2021.

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.