KPMG SailPoint

Thorough, intelligent identity for healthcare

Many healthcare organizations place a heavy emphasis on keeping outsiders out of their information technology (IT) infrastructure. While the value of perimeter security is undeniable, what do you do once an outsider gets inside?

With the volume and impact of costly security breaches on the rise, it has become increasingly apparent that providers must place identity at the heart of any program to ensure secure access, maintain compliance, and reduce risk.

Data access challenges for healthcare providers

The digitization of healthcare continues to change the threat landscape. Among the more difficult challenges is the proper and efficient governance of user identities and their access to patient data and other sensitive information. Consider these examples:

- With provider organizations using hundreds of applications and systems to store and transmit sensitive information, administrators and data owners face the daunting task of consistently governing access to mitigate breach and compliance risk.
- The need for data sharing continues to rise with ongoing mergers and acquisitions, growth of accountable care organizations, and the advent of health information exchanges. However, exchanging digital information can lead to the improper exposure of data. A response to any crisis around data security could have a significant impact on speed of operation for clinical and operational teams.
- The ever-increasing presence of personal devices (BYOD) within the provider-care setting means more data access points to manage. Such an environment broadens the scope of managing data from determining who should have access to what and when, to include how data is accessed. These complexities require a sophisticated level of security that balances against the need for prompt data access through the clinicians' native workflow.

Address access challenges through identity

- Deliver timely and appropriate access to patient records by giving healthcare providers greater visibility and control of who has access to what, when, and where.
- Reduce operational costs by streamlining access to systems and applications and improving data sharing between clinicians.
- Enable confident data sharing by mitigating risk of exposing sensitive information to unauthorized users.
- Drive compliance through process documentation for audits.

A thorough approach

Many identity governance programs focus solely on managing access to applications and structured systems, with the notion that the data within these applications is fully protected. However, through the normal course of business, this data is extracted and exported by users to create reports, presentations, and other user-generated content. As a result, it is common to find sensitive information across various ungoverned file storage systems. This typically means provider organizations have minimal control and visibility to where these files reside, what data the files contain, and how that information is being used.

By extending identity governance processes beyond systems and applications to also include data stored in files, healthcare providers can apply the same access controls across the data most used by the business.

Through SailPoint, provider organizations can locate, classify, and manage access to data files containing sensitive content (Health Insurance Portability and Accountability Act [HIPAA], General Data Protection Regulation [GDPR], Payment Card Industry, etc.) whether the information resides on premises or in the cloud.

It is estimated that 80% of data breaches have a connection to compromised privileged credentials.[1]

An intelligent solution

Healthcare organizations cannot govern what they cannot see. To enforce security policies and reduce risky behavior, it is essential for IT administrators and data owners to monitor, analyze, and quickly synthesize every identity interaction with every piece of data and application (clinical or nonclinical).

While this may sound daunting, it is achievable. Incorporating artificial intelligence can do the heavy lifting by ingesting vast amounts of identity and event data to provide advanced insights to gain greater efficiencies and mitigate risk.

By deploying this IAM technology, SailPoint solutions can perform peer group analysis, behavioral pattern matching and statistical analysis to detect and alert anomalous behaviors and potential risks. This next-generation technology can then be used to contextualize and focus identity governance controls on high-risk scenarios, such as inappropriate access and compliance gaps.

Through machine-learning capabilities, provider organizations can supercharge their identity governance processes.

SailPoint features and benefits

- **Reduce inconsistencies** by unifying the governance approach to multiple systems and applications, including Electronic Health Records (EHR) such as Epic and Cerner, through numerous out-of-the-box connectors and integration modules.
- **Improve security coverage** by locating, identifying, and applying access controls to sensitive data files.
- **Mitigate risk** by applying artificial intelligence to gain deep insight on anomalous access.
- **Support compliance** by deploying business-friendly access certification, streamlining audit reporting and documentation, and automating policy management.
- **Manage access** for users to systems, applications, and data files located on premises or in the cloud.
- **Streamline processes** through secure self-service access, automated provisioning and deprovisioning, and password sync to drive efficiency and improve operational workflow.
- **Minimize blind spots** by aggregating multiple access rights associated with a single identity due to multiple personas/roles.

Get to know SailPoint

Whether it's managing identities with multiple roles (personas), classifying and managing HIPAA- and GDPR-related content wherever the files reside or integrating with clinical applications to deliver a unified approach to governing access, SailPoint provides capabilities that are specifically relevant to healthcare providers.

In addition, SailPoint continues to be recognized as the leading authority in Identity Governance for the past five consecutive years. Forrester and KuppingerCole have also recognized SailPoint similarly. Discover how thorough, intelligent identity from SailPoint can help healthcare providers take security to the next level while enhancing operational workflow.

[1] CIO's Guide To Stopping Privileged Access Abuse – Part 2," Forbes, April 2019

At KPMG we understand that healthcare and life science organizations are operating in a highly regulated environment, with changing business models, disruptive technologies, and significant amounts of data. We offer a market-leading portfolio of methodologies, tools and services to assist you in the areas of value-based growth strategies. KPMG is a top deployment partner of SailPoint solutions with a focus on achieving business goals through technology.

- As a SailPoint Delivery Admiral since 2018, we've delivered over 200 engagements including some of the largest and most complex deployments of SailPoint IdentityIQ.
- KPMG's SailPoint implementation methodology is based on industry leading practices and is continually refined by collaboration between our delivery teams. We strive to learn every day, on every implementation and to improve our processes continually.

KPMG enhanced our IAM implementation methodology through investments in building an extensive catalog of intellectual property, enablers, and accelerators. This helps us design platforms that meet our clients' business needs today and are ready for the future, designed to accelerate long-term return on investment.

Identity Security for the Cloud Enterprise

SailPoint is a leader in identity security for the cloud enterprise. SailPoint's identity security solutions help secure and enable thousands of companies worldwide, giving their customers visibility into the entirety of their digital workforce, helping workers have the right access to do their job – no more, no less.

sailpoint.com

Contact us

Jim Wilhelm
Principal, Advisory
T: 267-256-7271
E: jameswilhelm@kpmg.com

Debbie Patterson
Alliance Director
T: 512-423-6150
E: deborahpatterson@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.