Rethink identity governance in healthcare

In modern healthcare organizations, thousands of identities are hard at work—and not all of them are clinicians. From nutritionists to pharmacists, students to researchers, social workers to biomedical scientists, the number of non-doctor healthcare workers has **more than doubled** between 1990 and today.[1] These fields have proliferated so quickly that healthcare provider organizations have more risks in cybersecurity than ever before.

Meanwhile, healthcare data breaches reached record levels,[2] and regulators are clamping down. No longer is it advisable to overprovision broad access to internal healthcare systems.

With a newfound sense of urgency, let us unpack the themes that uniquely affect identity security and governance in healthcare.

The challenges of governing identity

When it comes to identity security (also known as identity governance), hospital organizations that range in size from community hospitals to large delivery networks have several challenges, including:

- **Budget priorities.** Clinical transformation tops the agenda at most healthcare organizations, leaving limited room to address identity management and security.
- **Dynamic user populations.** The typical health system is staffed with an ever-shifting mix of personnel that includes employees, traveling nurses, outside contractors, students, affiliate physicians, and visiting professionals such as researchers and work-from-home personnel.
- **Complex roles.** The wide variety of clinical providers need to have the appropriate and very specific permissions to get the access they need to do their work.
- **Hybrid application environments.** The average hospital has a hybrid application environment comprised of solutions that are custom and off-the-shelf, on-premises and cloud-based, homegrown and best of breed, as well as new and decades-old legacy systems.
- **Reliance on legacy-based perimeters.** Legacy perimeter-based security is no longer enough. The rise of cloud computing, remote workforces, and interconnected devices have created a decentralized IT landscape where the old "castle wall" approach leaves critical security gaps.
- **Complex, multi-tiered, and distributed data.** In modern health systems, data enters via multiple sources. This includes EHRs and claims data that is inclusive of inpatient, outpatient, pharmacy, and enrollment, as well as wearable devices, including diagnostic and monitoring. That data is accessed by primary care physicians, post-acute care facilities, labs, and the patients themselves to boost outcomes and reduce the chance of re-admission.
- **Mergers and Acquisitions.** These outcomes often result in an exponential rise in identities that need to be secured. Newly acquired or merged healthcare organizations often lack visibility into all their identities and may have, over time, over-provisioned access. In this scenario, identity security can easily slip through the cracks if not properly managed.

[1] Peterson-KFF Health System Tracker: "What are the recent trends in health sector employment?", Telesford, Wager, Hughes-Cromwick, Amin, & Cox, (March 27, 2024)

[2] HIPAA Journal: "Healthcare Data Breach Statistics", (April 18, 2024)

Taking the friction out of identity security

Across the industry, consolidation is ongoing. Payer organizations are becoming providers and vice versa. Value-based care models are on the rise. The challenge of all this activity is that the business of healthcare is changing faster than the IT organizations that support them—putting their organizations at risk.

Here's where we will introduce the SailPoint platform with actionable insights and automation. Artificial intelligence (AI) and machine learning make it possible to continuously reduce friction in identity security through processes such as:

Access Modeling

AI and machine learning is used to quickly create and implement user roles to support a least privilege model.

Non-Employee Risk Management

Extend advanced identity security controls so you have the same visibility with non-employees (such as contract nurses and medical students) just as you do employees.

Access Requests

AI algorithms analyze access request patterns and behavioral data to identify any anomalies or potential threats along with recommendations for future requests that contribute to smoother processes.

Access Reviews

Lifecycle Management (or Day-one Access) manage all identities with AI-powered insights and processes to confidently determine what access should be requested, approved, or removed.

Reduce Risk

Visualize risk data to make informed access decisions based on an identity's third-party risk scores.

Meeting a higher standard

Healthcare organizations are held to a higher standard in terms of regulatory compliance and making sure that access to sensitive applications and data is limited to those who truly need it.

Typical scenarios include:

- **A compliance audit.** Between the duty to shield health records and the strict penalties that healthcare data breaches can trigger, organizations need a way to increase visibility, control potential access risks, and prove compliance quickly with automated reporting.
- **Reducing non-employee risk.** Healthcare organizations manage a wide range of identities beyond employees. Contractors, affiliate physicians, travel nurses, flex nurses, and medical students make up a large percentage of their workforce. Manually reviewing and granting access leads to cyber risks.
- **An M&A transaction or other major organizational event.** A merger or acquisition often involves the onboarding of thousands of identities, a process that can result in disruption, delay or overprovisioned user access.

A common thread in addressing these situations is cloud transformation. To some, that boils down to avoiding the need for additional hardware in their on-premises IT environment. To others, it can mean a move to software as a service (SaaS), with the vendor taking responsibility for administration and infrastructure. SailPoint's identity security solutions offer a significant degree of flexibility in bringing security and compliance to the healthcare IT environment.

Modernizing your Identity Program

Healthcare organizations can use identity security to reduce cyber risk by properly managing user access, ensuring the privacy of patient data, and scaling effectiveness with SaaS-based solutions. Advantages include:

01

A unified identity security cloud platform

Leading AI technology, a unified approach, and scalable architecture automates user lifecycle management ensuring a strong security posture, lower costs, and risk while strengthening access controls, policies, and processes with unique insights and governance simplification.

02

Scalability

SaaS-based identity security solutions can easily scale up or down based on the changing needs of an organization.

03

Cost-effective

SaaS-based identity security solutions are cost-effective since healthcare organizations do not have to invest in hardware infrastructure.

04

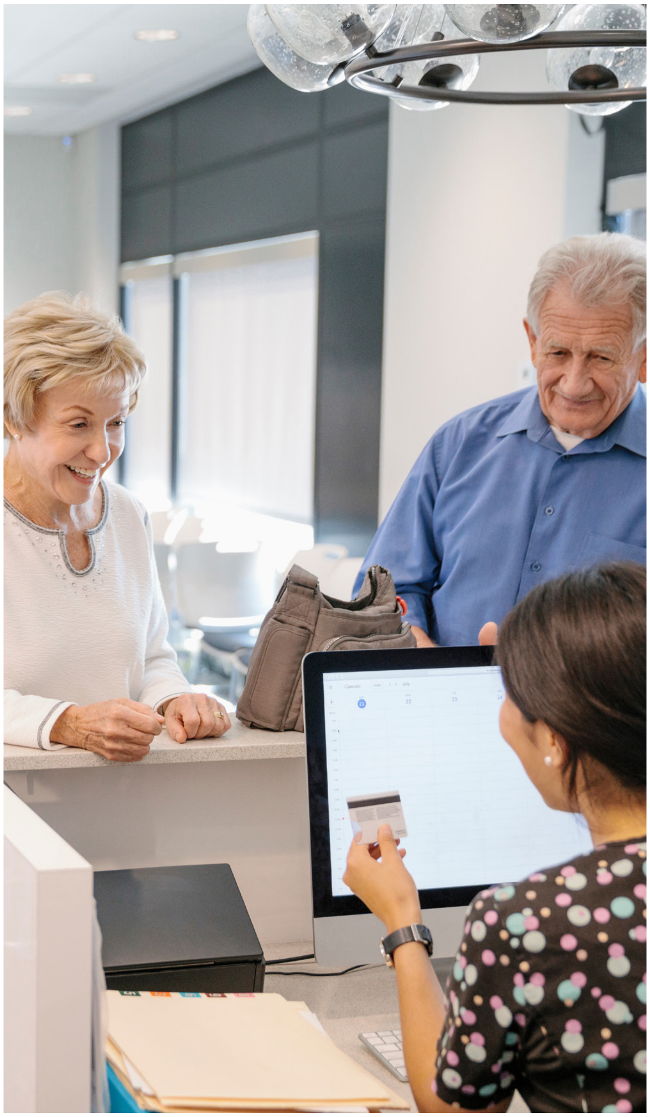
User self-service

Identity security cloud solutions enable hospitals to offer self-service options to users, reducing IT support costs.

05

Compliance management

Ensure Zero Trust with least privileged access. Protect sensitive ePHI data and prevent disruption to patient care. Identity security cloud affords you the flexibility to align to various frameworks such as NIST and HITRUST and easily meet regulatory requirements such as HIPAA, GDPR, and others.



Contact us

Doug LaGore
Principal, Advisory
T: 313-230-3000
E: dlagore@kpmg.com

Adam White
Managing Director
T: 949-344-5674
E: arwhite@kpmg.com

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

Learn about us: in | **kpmg.com**

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

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.