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, pastors to janitors, social workers to biomedical scientists, the number of nondoctor healthcare workers **soared 3,200 percent** between 1970 and 2009.[1] These fields have proliferated so quickly that healthcare provider organizations have struggled to keep up.

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

We unpack the themes that uniquely affect identity governance and administration (IGA) in healthcare and show you how SailPoint addresses them through an intelligent IGA platform. Browse the sections in the order they appear or skip directly to the one that's of greatest interest.

The challenges of governing identity

When it comes to governing identity, hospital organizations—whether a small community hospital or a large delivery network—have a number of challenges. They include:

- **A lack of budget focus**. Clinical transformation tops the agenda at most healthcare organizations, leaving limited room to address issues like identity management.
- **Dynamic user populations**. The typical health system is staffed with an ever-shifting mix of personnel that includes employees, outside contractors, students, and visiting professionals such as researchers.
- **Multiple authoritative sources**. Health systems tend to have several (or even a few dozen) credentialing systems for their different user populations.
- **Hybrid application environments**. The average hospital has a hybrid application environment composed of solutions that are custom and off-the-shelf, on-premises and cloud-based, homegrown and best of breed, and new and decades-old legacy systems.
- **Complex, multitiered, and distributed data**. In modern health systems, data enters via multiple sources, such as EMRs and claims data that is inclusive of inpatient, outpatient, pharmacy, and enrollment, as well as wearable devices, including for diagnostic and monitoring (such as cardiovascular devices), therapy (such as insulin management devices), injury prevention and rehabilitation (such as fall detection devices), and lifestyle and fitness (such as fitness and activity trackers). That data is accessed by primary care physicians, post-acute care facilities, labs, and the patients themselves in order to boost outcomes and reduce the chance of readmission.

These challenges add up to a highly complex IT environment that creates a unique IGA quagmire for healthcare.

[1] Source: Health Care Costs: A Primer, The Henry J. Kaiser Family Foundation) State of the Industry

[2] HIPAA Journal: "Analysis of 2018 Healthcare Data Breaches" (January, 28, 2019)

Taking the friction out of IGA

Across the industry, consolidation is ongoing. Payer organizations are becoming providers and vice versa. Value-based care models are on the rise.

The upshot of all this activity is that the business of healthcare is changing faster than the IT organizations that support them. IT is being asked to do more and more, with the same or fewer resources. In this scenario, identity governance can easily slip through the cracks.

Here's where an IGA platform with cognitive capabilities comes in. AI and machine learning make it possible to continuously reduce friction in identity governance processes such as:

— **Access certifications**. AI algorithms provide recommendations to reviewers on what kind of access a user needs upon assuming a role or reaching a recertification milestone, easing the review burden for IT and security organizations.

— **Real-time tracking**. AI can streamline compliance and audit performance by making each user's access history available for review on demand.

— **Cybersecurity**. With cognitive capabilities, an IGA platform can perform analysis on peer groups and their respective access to quickly identify outliers possessing abnormal or excessive permissions that may not surface with manual approaches.

By injecting their governance strategy with cognitive capabilities, hospital IT teams can position themselves to more effectively align with best practice security frameworks and become more proactive in their defense against fraud and cyberattacks.

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. The ability to meet this standard in an effective way can come to a critical juncture on certain occasions.

Three of the most typical 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 quickly address issues that surface through the audit process.

— **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 and delay if carried out manually.

— **A modernization initiative**. Organizations facing provisioning challenges are weighing a fully automated identity governance strategy that takes them where they need to be, not just today but well into the future.

A common thread in addressing all of 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. Either way, the intelligent IGA platform offers a significant degree of flexibility in bringing security and compliance to the health IT environment.

Rethink identity in healthcare

Provisioning and compliance are two sides of the same coin when it comes to IGA. Healthcare organizations shouldn't provision users without knowing what they have access to already. At the same time, if a compliance review reveals users have access permissions they shouldn't have, there should be a way to automatically remediate or deprovision that access.

Given this tension, integrated identity solutions can help healthcare organizations rethink their approach to identity governance. What objectives should hospitals aim for? Here are five high-impact ones to start with:

— Gain 360-degree visibility into who has access to what across the user population.

— Govern access for the duration of each user's role.

— Demonstrate strong access controls for sensitive data and applications.

— Protect the organization's brand and reputation from unauthorized access.

— Relieve the IT team of manual access management processes, freeing them to pursue innovative new projects.

IGA has become a critical security and risk management challenge in healthcare. At the same time, modern hospitals are highly complex organizations, making a crisp, fully automated way to govern identity a necessity. In the end, IGA can be evaluated by how effectively it enables different user populations with access to the right applications and the right data at the right time to improve operational efficiencies and drive patient outcomes—all while shielding the organization from practices that create risk.

In the United States, KPMG serves over **50 percent of the top 45** pediatric hospitals. We serve almost **60 percent of the top 150 healthcare systems** and **70 percent of academic medical centers.**

— KPMG is a top deployment alliance 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 IIQ.

— Our 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.

We've enhanced SailPoint and 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, saving time and money and accelerating long-term ROI.

Identity security for the cloud enterprise

sailpoint.com

SailPoint is the leader in identity security for the cloud enterprise. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, ensuring workers have the right access to do their job—no more, no less.

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