Rethink Identity Provisioning in Healthcare

SailPoint

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 non-doctor healthcare workers **soared 3,200%** between 1970 and 2009. These fields have proliferated so quickly that healthcare provider organizations have struggled to keep up.

Meanwhile, healthcare data breaches recently reached **record levels,** and regulators are clamping down. No longer is it feasible to give users broad access to internal healthcare systems. Hospital IT teams must put governance controls around sensitive clinical data to make sure it doesn't end up in the wrong hands, even as they facilitate the appropriate access so that staff can carry out their work without interruption. That means they need a practical way to manage identity in the fluid, highly complex environment that defines modern acute and post-acute care organizations.

In this e-book, we unpack how SailPoint addresses access and provisioning through an intelligent Identity Governance and Administration (IGA) platform.

Identity Provisioning Across the Governance Lifecycle

There's a lifecycle to the relationship users have with a healthcare organization: They join, they leave, and they often change roles in the meantime. Each of these lifecycle stages has its own provisioning challenges.

Stage 1: Onboarding

It's not unusual for new staff members to wait as long as a week to gain access to the systems they need to do their job. In that time, hospitals are paying personnel who are unable to see patient records, write scripts, or cross-reference information. In an industry where the median annual wage was $66,440 in 2018, lost work due to slow provisioning could cost the organization **$277 a day, per employee.**

The good news? With an IGA solution, nurses, physicians, and other hospital personnel can gain complete access on day one, automatically, freeing them to do their jobs the moment they walk in the door.

Stage 2: Role Model Management

Not all hospital jobs are static. A student, for example, can become a full-time nurse. A nurse can work in the main hospital full time during the week and at an outpatient clinic part time on the weekends. A clinician may spend time on the patient floor, then later go into research. All may be the same person, but each role they take on is associated with different permissions to system applications and data.

Managing this process manually can be extremely time-consuming. However, the role-modeling software engines and simulators in an IGA platform offer a simpler way to manage multiple roles and multiple permissions based on the organization's security policies. The result is that the right people gain access to the right applications at the right time—automatically.

Stage 3: Offboarding

Staff departures mark the end of the governance lifecycle. Failure to revoke permissions at that time can expose the organization to unauthorized access of sensitive clinical data or applications that contain clinical data. Such occurrences are particularly costly for healthcare organizations, amounting to **$425 per record, per year.**

Effective IGA defends against data breaches by automatically locking down access the moment a staff member leaves the organization. At the same time, it tracks every lifecycle event associated with onboarding, role transfers, and offboarding, making the history readily available for routine security audits.

Rethink Identity in Healthcare

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:

1. Gain 360-degree visibility into who has access to what across the user population.
2. Govern access for the duration of each user's role.
3. Demonstrate strong access controls for sensitive data and applications.
4. Protect the organization's brand and reputation from unauthorized access.
5. 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.

To learn more about Identity Governance and Administration and SailPoint's identity solutions for healthcare, please visit **www.sailpoint.com/identity-for/healthcare**

A SailPoint reseller and implementation partner, Forward Advantage has more than 25 years of healthcare experience and a deep understanding of customer needs from purchase through implementation and beyond. Our professional services are structured to meet each customer's unique needs so you and your providers can spend more time on what really matters: improving patient health.

Let Forward Advantage help make your goals a reality. Talk to one of our solution experts today!

forward® advantage

877.636.7927
info@forwardadvantage.com
www.forwardadvantage.com

ABOUT SAILPOINT

SailPoint is the leader in identity security for the modern enterprise. Harnessing the power of AI and machine learning, SailPoint automates the management and control of access, delivering only the required access to the right identities and technology resources at the right time. Our sophisticated identity platform seamlessly integrates with existing systems and workflows, providing the singular view into all identities and their access. We meet customers where they are with an intelligent identity solution that matches the scale, velocity and environmental needs of the modern enterprise. SailPoint empowers the most complex enterprises worldwide to build a security foundation grounded in identity security.

PC2052-2111