SailPoint | GCA
MANAGING YOUR DIGITAL IDENTITIES

Software Solution

Optimizing Identity for Healthcare Organizations

Table of Contents

The Complexities of Securing Health Data

The healthcare industry is rapidly evolving. Among the many significant industry changes are the ongoing mergers and acquisitions, the proliferation of accountable care organizations and the integration of multiple health IT vendors into day-to-day hospital operations.

Couple these changes with the fact that more patients are accessing their healthcare records electronically, and providers must cope with the growing demand for sharing highly sensitive patient data between organizations and individuals.

With increasing demand comes increasing risk, particularly with information security and regulatory compliance. To ensure timely and proper access to applications, files and data, providers must navigate through a myriad of hurdles.

This guide covers common identity management challenges in healthcare and how SailPoint solves for them.

Healthcare IAM Complexities

Multiple Authoritative Sources

Many provider organizations have multiple authoritative sources including human resources applications (HR), contractor management systems, electronic health record systems (EHRs), learning management applications (LMS) and physician credentialing applications often referred to as MSOW. These and other systems and applications are deemed by the provider organization as the true source for defining user identity and access rights. However, having to manage multiple identity sources and their access rights creates difficulty in ensuring consistent execution of policies and resource optimization.

Diverse User Population

Within the healthcare-provider setting, there is typically a diverse and transient population that requires access to health information as a part of their regular workflow. This may include hospitalists, employed staff, contracted physicians, students, volunteers, vendors, etc. Ensuring the right people have the right access at the right time is a daunting task. However, the consequences of not doing so can create security gaps with serious financial and operational repercussions.

Multiple Roles (Personas)

User access is not always managed by any single department or team. At the same time, it is often managed through functionality native to the specific application. This creates a disparity in processes that leads to security gaps and unnecessary burden on IT administrators and application owners.

Clinical Workflows

From a workflow perspective, the disparate systems and processes could also affect clinical care. For instance, due to accidental oversight, a contracted physician may be given access to the EHR, but not the enterprise content management system where scanned clinical media and images are stored. As a result, the physician's efforts to fully understand a patient's condition and provide timely care may be delayed.

Simplifying the Complex

1. Create What and Why Personas

Multiple authoritative sources in addition to the HR system means a complete record of a person could involve incoming data points from ancillary systems not controlled by the HR team. Such systems may include the EHR, LMS and the physician credentialing application. For healthcare provider organizations, effectively managing multiple personas can be extremely difficult.

For example, should a resident physician have access to sensitive patient data when they are doing research for one of their classes? Is it appropriate for a hospital-employed clinical assistant to have the same access entitlements when they are doing volunteer work for a health association? The challenge of managing data access for users with multiple roles or personas is especially pronounced within the healthcare provider space. Left unaddressed, providers may find themselves at risk of breach and regulatory non-compliance.

Personas help to build an identity by defining the various ways in which an individual engages a healthcare organization. In many cases, an identity may have multiple personas – meaning they may perform more than one function during any given day. SailPoint enables you to manage access and entitlements for users within multiple personas.

> **SailPoint manages access and entitlements for users with multiple personas within the healthcare industry.**

2. Implement Flexibility to Meet Your Organizations's Unique Requirements

Different healthcare organizations have different requirements and data structures. SailPoint provides multiple ways within IdentityIQ to meet these requirements. Here are just a few examples of how SailPoint can approach the multiple persona issue:

Persona Relationship

This approach is ideal when there is a well-defined authoritative source or application (like HR) for an identity (like an employee). SailPoint can also create a primary identity for user types not sourced from HR, such as student accounts and contingent workforce. SailPoint further allows providers to establish secondary identities that are linked to the primary identity. This allows providers to have complete view of the user's entitlements and enables effective management of different personas.

Linked Relationship Persona

Where there are multiple authoritative sources – each being the authority for a different identity persona – the linked relationship persona approach can be very effective. In this case, SailPoint provides a global identifier where all personas are tied to that individual. Additional personas appear as an application account that are transparently linked back to the main identifier. This model not only builds the relationship but also shows all accesses in one uniform way in IdentityIQ.

Role-Based

While this is a simpler approach, it is contingent on the environment. Where individuals do not have multiple employee IDs or different managers, personas can be managed via roles. Provider organizations may want to delineate between personas for approvals, certifications and attestations.

3. Go Beyond Compliance to Fill the Security Gap

Proving compliance with regulations is, of course, a very important goal for healthcare providers. Still, even if the audit passes, the organization could be at risk if it does not address the larger security concern of employees' access to its data and applications. Taking a governance-based approach to security – where the tools used to meet compliance can see into every part of the organization – helps to ensure decisions about users' entitlements are based on all the relevant information.

> **90% of healthcare providers have experienced a data breach in the past two years.**

The question has become not if a healthcare provider will be attacked, but when. Often, providers have unique combinations of commonplace, proprietary or other systems that are usually disconnected from each other all while holding important pieces of information – and not just about clients and patients. While the compliance tool may secure access to each of those systems independently, holistically knowing who has access to what, where that access overlaps and if it's a violation of your policies is instrumental in reducing the risk of breaches, theft and fraud as a healthcare provider.

Marrying the IT solution to good business policies and procedures ensures that both compliance and the security of your systems are addressed.

Implementing an identity management system to meet compliance with the applicable laws is the first step to securing an organization. But in order for providers to truly mitigate their risk, they must know who has access to what data and applications. Clinical and operational staff, contractors, partners, etc., may all have access to different sets of data. In order to safeguard and manage access to sensitive data, providers need consistent and unified policies and procedures that complement their compliance systems.

4. Incorporate the EHR

The EHR is among the various systems and applications that providers should incorporate into a comprehensive unified governance approach. When properly integrated together, providers can extend continuity in their approach for governing access to one of the most-used technologies within the provider-care setting. In doing so, integration with a proven IGA should:

- Minimize interruptions to hospital operations: Reduce downtime for new hires and transfers by automating changes to access rights the EHR.
- Reduce compliance risks: Mitigate risk of regulatory non-compliance by automating processes to reduce human errors and recording governance activities to demonstrate proof-of-compliance.
- Increase efficiency: Eliminate disparate processes that can quickly consume IT time and resources.

While incorporating the EHR into your identity governance program should be a top priority, it is not exclusively beneficial. A unified approach means incorporating all other applications and systems that are essential to provider operations. Whether HR, MSOW, billing, accounting, etc., even if providers are not using them from a clinical workflow, they play a crucial part in the operations.

For that reason, providers cannot leave out other critical technologies, as that will leave vulnerable gaps in security, increase the likelihood of error, and unnecessarily tax already-lean resources. To maximize the efficiencies and effectiveness an identity governance program can bring, providers need to think globally and implement a strategy designed to mitigate gaps in security.

SailPoint Use Case Examples

Here are several examples of how providers use SailPoint to address cybersecurity and compliance challenges:

- Provider organizations typically have a mix of legacy and more current systems and applications. Managing access consistently across all of these technologies can be achieved through SailPoint's unified governance approach.
- SailPoint enables providers to create, manage and document information access policies and user access rights. This helps providers to confidently meet healthcare regulatory compliance and audit requirements.
- It is of utmost importance that providers balance security and compliance with clinical and operational workflow. SailPoint solutions automate formerly manual processes for requesting, granting and provisioning access, thus delivering timely information for clinicians as they provide quality patient care.
- SailPoint can extend identity governance beyond systems and applications. This allows providers to find, classify and control access to data files wherever they reside.

SailPoint Predictive Identity

Many organizations use SailPoint Predictive Identity to create a holistic identity governance program.

Manage Identities Effectively
Securely govern access lifecycle of a diverse user population.

Simplify Complexities
Effectively govern around user identities with multiple personas.

Maintain Compliance
Establish audit trails and automate periodic reviews of access rights.

Improve User Experience
Govern consistently to all applications and optimize operational workflow.

Enhance Audits
Gain historical view of how access has been accumulated over time for more complete auditability.

Create Hyper Efficiencies
Automate and enable self-service processes to reduce IT demand.

Mitigate Risk of Breach
Enforce consistent governance controls and simplify access delivery.

Reduce Fatigue
Leverage machine learning to make more efficient decisions in review processes and reduce certification/approval fatigue.

Adapt to Change
Leverage machine learning to create access and risk models in real time.

Analyze and Visualize
Assess performance of your identity governance program by providing a 'big data' platform and rich visualizations of data.

Rein in Data Files
Locate, classify, control and monitor access rights to data files.

Working With a SailPoint Consultant

An Intelligent Approach for Healthcare

Reduce Security Risks
Leverage time-series analysis and machine learning to determine normal and anomalous access within the healthcare organization.

Drive Efficiencies
Automate low-risk access approvals for all clinical and non-clinical users, streamline access certifications, and reduce false alerts of policy violations.

Govern Access
Rapidly highlight unusual access held by individuals and eliminate potential risk to the provider organization.

GCA offers SailPoint consulting services to help your organization implement reliable security and compliance. We specialize in healthcare IAM and have served a variety of clients in the healthcare space.

Not only are we IAM consultants, but we're also experts on business optimization and automation. That means every engagement is holistically strategic, helping you align your IAM program with your organization's larger goals—like boosting productivity, integrating SailPoint with Cerner or Epic, streamlining workforce management and staying within budgetary limits.

Contact us to let us know how we can help optimize and secure your organization.

Contact GCA

SailPoint | GCA