SailPoint

eBook

The compromised identity in healthcare

How identity security can reduce your cyber risk

Healthcare's battle against targeted cyber attacks with a shortage of IT and clinical staff is a cruel reality the industry is facing today. Indiscriminating ransomware gangs have shown no mercy when it comes to healthcare and seek out lucrative opportunities to exploit any identity security gaps they find[1].

93% of healthcare organizations have faced a breach in the last two years[2] and the costs exceed any other industry at currently over 10 million dollars.[3] In fact, according to a recent report[4], the healthcare industry was the most common victim of third-party breaches in 2022, accounting for almost 35% of all incidents – up from 33% in 2021.

Cyber attacks persist into 2023 and in addition to severe cybersecurity risks, the industry faces compounded risk from IT skills-gaps, limited budgets, manual processes, M&As, and shifts to the cloud. Digital transformation initiatives such as migrating to the cloud, implementing new technologies, forging third party relationships, and use of big data have driven growth for both human and non-human identities. And since each user has an identity with associated credentials and access rights to the organization's resources, cyber risk is increased as the attack surface expands.

In this eBook, you will learn why leading healthcare organizations are turning to AI to modernize identity security to reduce their risk, gain efficiency, enhance clinician productivity, comply with regulations, and improve overall patient care.

We will provide ways AI-driven identity security (also known as identity governance) can increase visibility and access control to employee and third-party identities, resulting in not only in more secure digital identities, but also improved efficiencies and significant cost savings for your organization.

The compromised identity

Despite increased investments within a security ecosystem, healthcare continues to get breached. Why?

With credentials like passwords stolen through phishing emails, external attackers can gain initial access to systems to execute threat vectors like dropping malware. Having gained entry, attackers can also pursue more entitled, risky access to resources if strong identity security processes are not in place.

Building a strong identity program

To mitigate cyber risk related to identity and access, organizations need a risk management strategy: A framework of actions and activities to reduce or control the likelihood of risk turning into a breach or enabling cyber-attacks involving malware or ransomware.

A strong identity security program can be forged from solutions that help organizations reduce risk and build resilience across all use cases, including credential compromise and theft, third party and supply chain, identity and access management, and more.

Four key things are required to modernize the management of identity security:

Increase visibility

- Overcome internal data silos by integrating cloud identity into your applications to synchronize user identities.
- Centrally manage and control identity access to all data, applications, systems, and cloud infrastructure across your hybrid infrastructure.
- Extend advanced identity security controls so you have the same visibility with non-employees as you do employees.

Control access

- Measure access risk across your organization.
- Ensuring the right people have the right level of access to resources and apps with the least amount of friction.
- Detecting and preventing toxic access combinations that could lead to fraud or data theft.
- Secure sensitive data PHI and PII across all environments.
- Prevent excess entitlements or orphaned accounts (for example, a nurse that has changed roles and accumulated access over time but never had access revoked).

Leverage AI-driven automation

- Automating the discovery, management, and control of ALL user access.
- Reducing human error and security risks (i.e., rubber-stamping, etc.) with intelligent automation of routine tasks.
- Minimize security risks by automating identity processes and decisions such as access requests, role modeling, and access certifications.

Reduce third-party risk

- Gain visibility to what employees and non-employees such as travel nurses, students, and affiliate physicians have access to in your organization, why they have access, and what they're doing with that access.
- Execute risk-based identity and access lifecycle strategies to mitigate your risk of a third-party breach.

Improve efficiencies while reducing risk

Cybersecurity and IT teams aim to find a better way forward, to reduce cyber risk while also improving IT efficiencies. AI-driven identity security answers this mandate in several positive ways:

- **AI identified access risks:** Identify and eliminate high-risk excess entitlements. AI can make it easier to identify access risks, monitor behaviors, and refine roles.
- **Integrating applications:** Securely connect EHR, credentialing, HR, ERP, learning management, and other applications to accomplish an identity security ecosystem; this leads to a more secure environment for health records and alleviates highly manual and costly EHR provisioning efforts.
- **Improving compliance and avoiding fines:** Healthcare organizations must efficiently comply with strict regulations such as HIPAA to protect sensitive patient data and leverage frameworks like NIST and HITRUST. Organizations can gain action-oriented insights through real-time data visualization to easily track activity and simplify compliance.
- **Improving patient care:** AI-driven identity security helps improve patient care by replacing time-consuming manual processes with automation, which gives healthcare staff more time to focus on patient care.

Control access in a complex identity population

Healthcare clinicians need the right access to the right applications, systems, and data when they need it most — not only so they can deliver the highest quality of care to their patients but, tied to that, to maximize their job satisfaction and retain their services.

The kind of access they have is defined by who they are: their identities, differentiated in terms of roles, locations, and responsibilities.

AI can make it easier to identify access risks, monitor behaviors, and refine roles. Hospitals and healthcare organizations have complex and dynamic identity populations, including employed clinical staff and non-employee contracted staff, students, volunteers, and other identity types.

A single practitioner often has multiple roles and many transfers. An academic hospital nurse may work in multiple locations and departments, is a student of the hospital, and maybe even a volunteer.

Properly governing access means determining the type of identity an individual is (their role and attributes in the organization), the type of clinical application access required across the organization, and what validations need to be completed with multiple authoritative sources before a clinician can be granted the access they need to treat patients.

Further, clinical applications have multilevel security permissions models that drive what any single user can do within that application.

Prevent third-party breaches

Healthcare organizations today utilize a large and diverse number of third parties, from travel nurses to affiliate physicians to contractors. The number and variety of third parties utilized by healthcare organizations can be limitless and unfortunately, creates a greater risk of data and access-related breaches.

According to the United States Department of Health & Human Services, an insider threat in the Healthcare and Public Health (HPH) Sector is potentially a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems. The person could use this information in a way that negatively impacts the organization.[5]

Insider threats are not just internal employees but can also take the form of third parties:

- 94% of organizations give third parties access to their systems.
- In 72% of case studies, third party vendors were provided elevated permissions on these systems.

These insider threats include:

- Careless or negligent workers
- Malicious insiders
- Inside agents
- Disgruntled employees
- Third parties

Examples of healthcare related data breaches cited in the HHS report include a report from a major U.S. pharmaceutical company that launched an investigation after an employee downloaded 12,000

confidential files on a cloud system before leaving to work for their competitor.
Also, this: a Texas hospital employee filmed himself infiltrating the hospital network and creating a backdoor in a HVAC unit that could impact medicine and patients if the system shut down.

In its mid-year (June 2022) report on data breaches in healthcare, HHS found:[6]

- 337 incidents affecting or potentially affecting 19,992,810 individuals
- 123 of all incidents (36%) involved business associates. One of these incidents impacted more than 650 covered entities.
- Hacking/IT incidents accounted for 269 of the 337 reports, but unauthorized access/disclosure accounted for another 50 of those reports (15%)

> **"If you have contract employees with access to your network and biggest clinical application, you need to know about it and have some type of structure in place. This would not have happened without implementing SailPoint.[8]**
>
> **James Landers**
> Identity Access Management Security Engineer, Integris

In a Varonis exposure report[7], when it comes to stale user accounts (those that are enabled accounts but appear inactive and often belong to individuals no longer with the organization) 56% are still enabled at 90 days and 33% still enabled at 180 days.
In other words, enforcing least privilege is a basic step every organization can take to protect data from theft and misuse while ensuring compliance with regulations.

To recap

When it comes to managing identity security and minimizing risk in healthcare, concerns and considerations include:

- Manual processes causing cyber risk, clinician access delays, and operational costs
- Increased risk managing a high volume of clinician transfers and role changes
- Meeting complex compliance and regulatory requirements
- Reduce practitioner downtime by automating data access so practitioners can treat patients earlier
- Demonstrate security controls to compliance auditors and cyber insurance underwriters
- Reduce the cost of compliance by automatically generating audit trails and access reports on all key applications and data
- Remedy short staffed IT teams and the urge to rubber stamp access

How SailPoint helps

Hospitals and healthcare organizations are struggling to quickly enable their staff while securing against targeted cyber attacks. Here's how SailPoint helps healthcare reduce cyber risk:

- **Consolidating identity management** Bring all resources, including EHRs, under a single, unified governance platform, including access requests, certification reviews, and automated lifecycle management when someone joins, changes roles, or leaves the organization.
- **Reduce clinical onboarding friction** Reduce friction between clinicians and IT Teams with rapid and secure access. Alleviates manual provisioning and prevents manual work across disconnected applications.
- **Seamlessly integrate with EHRs** Visualize the identity permissions within the clinical application to improve decision making capabilities.
- **Increase accuracy preparing for compliance audits** Create and detect cross-application violations with cross-domain clinical application and enterprise policy violation rules.
- **Integrating applications:** Securely connect EHR, credentialing, HR, ERP, learning management, and other applications to accomplish an identity security ecosystem; this leads to a more secure environment for health records and alleviates highly manual and costly EHR provisioning efforts.

As a result, healthcare practitioners can:

- Quickly and securely enable a clinical workforce with faster onboarding access that remains secure
- Relieve the IT team of manual access management processes, increasing accuracy and reducing risk
- Protect the organization's brand and reputation from unauthorized access and damaging breaches
- Demonstrate strong access controls for sensitive ePHI data and applications.
- Minimize risk by dynamically informing you exactly which non-employees need access, why they require it, and when it's appropriate.

In summary, when it comes to securing digital identities and minimizing risk in healthcare and hospital settings, visibility (e.g., seeing who is accessing sensitive PII such as health records and patient data) and control (e.g., and what they are doing with it), is everything.

It's why leading healthcare organizations are turning to AI-drive identity security to proactively identify and manage risky access, enhance provider satisfaction, empower IT teams, and deliver significant cost savings.

SailPoint Non-Employee Risk Management provides healthcare organizations with a powerful identity security solution that extends advanced governance controls to large and complex populations of non-employee users. Together with SailPoint Identity Security Cloud, you can secure your

third-party identities and automate provisioning to ensure productivity on day one while reducing shared, over provisioned, and orphaned account access in the same way you manage employee identities.

SailPoint Identity Security Cloud harnesses the power of AI and machine learning to deliver unmatched intelligence, frictionless automation, and comprehensive integration needed to easily manage access across the largest, most complex cloud healthcare organizations worldwide. To learn more, visit **Identity Security Cloud | SailPoint.**

[1] No relief in sight for ransomware attacks on hospitals | TechTarget
[2] Healthcare Identity Security - White Paper | SailPoint
[3] Average Healthcare Data Breach Costs Surpass $10M, IBM Finds (healthitsecurity.com)
[4] Healthcare Organizations Most Common Victims in 3rd Party Data Breaches (hipaajournal.com)
[5] 202204211300_Insider Threats in Healthcare_TLPWHITE (hhs.gov)
[6] 2022 Mid-Year Healthcare Data Breach Deep Dive (protenus.com)
[7] Varonis-The-Great-SaaS-Data-Exposure.pdf
[8] The Power of Identity Gives Integris Health the Power to be Compliant and Secure | SailPoint

About SailPoint
SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.