eBOOK

Effective Identity Governance Programs for Modern Hospitals

SailPoint

Is Identity Governance a technology solution or an enterprise cybersecurity discipline? The answer is both. As such, it requires a programmatic and strategic approach that coordinates with every stakeholder of a sprawling modern healthcare organization.

An Identity Governance program recognizes the importance of prompt, need-to-know access to hospital applications and data. It also acknowledges the obligation to maintain confidentiality, integrity and availability of the electronically protected health information (e-PHI) that flows through these systems. This is not the kind of program that runs itself. Its success depends on the management team's ability to continuously evaluate it beyond technicalities and make it an intrinsic part of day-to-day business processes.

The move to electronic health records (EHRs) began in earnest with passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). Key objectives of EHR adoption, as outlined in HITECH and furthered by the Federal Health IT Strategic Plan 2015-2020 are to help the the U.S. healthcare system achieve high-quality care and lower costs while driving improved population health. However, health policy objectives and IT implementations don't always have a symbiotic relationship that aligns to the realities of a modern, fluid healthcare ecosystem. For example, data breaches have been one unintended consequence of increased EHR utilization:

The annual number of electronic protected health information (**ePHI**) **breaches increased** from 18 in 2009 **to more than 365 in 2018**.[1]

Nearly **13% of the U.S. population's healthcare records** were **"exposed,** impermissibly disclosed, **or stolen**."[3]

From 2013 to 2018, **the average cost of a data breach** to healthcare organizations **rose to $3.92 million**.[2]

Unauthorized access and disclosure incidents were the **second largest cause of data breaches,** representing nearly (29%) of incidents involving **more than 11%** of all records breached.[4]

[1] "Main Causes of Security Breaches in the Healthcare Industry," RSI Security, October 2019, https://blog.rsisecurity.com/main-causes-of-security-breaches-in-the-healthcare-industry/.
[2] "2019 Cost of A Data Breach Study Reveals Increase in U.S. Healthcare Data Breach Costs," HIPAA Journal, July 24, https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/2019.
[3] "Report Reveals Worst State for Healthcare Data Breaches in 2019," Sarah Coble, InfoSecurity Magazine, February 14, 2020, https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/.
[4] Ibid.

Operational Agility for Modern Hospitals

Healthcare systems today enable better patient outcomes by improving care coordination and operational efficiencies. The proliferation of different types of devices coupled with diverse platform, application, and cloud ecosystems have transformed healthcare organizations into interconnected mobile societies. Examples include clinicians pivoting to telehealth, contingent workers arriving at a disaster scene, and staff shifting roles in response to new medical protocols. There's also the surge of new users that can come onto existing healthcare IT infrastructures when healthcare organizations undergo mergers and acquisitions or pandemic or large catastrophic events. Without the ability to manage these access requirements in a short and proficient time period, patient safety issues and quality of care are deeply affected.

These and other scenarios depend on healthcare organizations that can adapt and deliver care without delay. That can be a tall order for hospitals where IT staffing is modest and manual user provisioning can take days or even weeks. Vendors, contractors and other non-staff users can further complicate the issue because their activities may lie outside the hospital's direct control.

With evolving healthcare business models, few hospitals and medical practices today operate entirely independently. Most are part of a complex network of joint ventures, partnerships and community support, each with its own part to play in the continuum of care.

These dynamics have prompted hospital executives to reexamine their approach to Identity Governance and how to answer three basic questions:

- **Who has access to what?**
- **What should they have access to?**
- **How are they using their access?**

Without modern tools and processes, healthcare organizations can struggle to address the operational, clinical security, and compliance risks posed by hybrid IT architectures, changing regulations and an increasingly diverse user base. They can also slow hospitals' ability to adopt innovations and best practices at a time when emerging digital technologies are poised to transform the biomedical world.

The Platform

SailPoint's predictive identity engine applies artificial intelligence (AI) and machine learning technologies to autonomously recommend user access permissions and compliance policies. Intelligent agents find new access and bring it under governance automatically. They also discover and mitigate risky user behaviors.

The upshot is that properly deployed, SailPoint provisioning is autonomous. The platform analyzes user role, user behavior, compliance policy and other data to gain insight about what assets a user should have access to. Then it uses these insights to make the appropriate decisions and/or recommendations on the organization's behalf. Over time, the provisioning decisions become smarter as the platform learns and adapts to its environment. Meanwhile, the hospital IT team remains in complete control.

The Delivered Value

A successful transition to autonomous provisioning certainly requires an effective Identity Governance platform. But it also demands refined business processes that can make the most of that technology and data.

To maintain continuity, identity and risk management professionals help the healthcare organization implement the new platform before decommissioning the legacy system. This gives the organization a chance to phase out old software licenses in a cost-effective manner. Importantly, however, it also enables SailPoint to begin collecting the data it needs for machine learning. The larger the data stores, the better the platform becomes at predicting user access needs and identity-related risks.

An effective Approach to Identity Governance

Given the unique challenges of Identity Governance in healthcare, even the most expansive knowledge base is insufficient to developing a resilient, effective identity and access management solution. Other elements must come together, including:

- A practical understanding of healthcare clinical and business practices
- Deep expertise in, and a tailorable framework for, governance of access rights in a healthcare setting
- The ability to address the people, process and technology aspects of identity decisions
- A relentless focus on delivering patient care against operational objectives

To learn more about Identity Governance and the solutions SailPoint can deliver, please visit **www.sailpoint.com/identity-for/healthcare**.

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

EB1590-2008