coresecurity
by HelpSystems

CUSTOMER STORY *(Cybersecurity)*

From Surviving to Thriving:

How a Large Healthcare Organization Established a Comprehensive Identity and Access Management Approach Using IGA Solutions from Core Security

Overview

Healthcare organizations today face extraordinary challenges in a dynamic, complex landscape. During the last two decades, the healthcare industry has seen increasing regulations, an acceleration of technology and workforce growth, acquisitions and consolidation, and the pressure to increase operational efficiencies and decrease overall costs, while meeting growing patient demands.

Because many healthcare organizations lack a centralized process to manage user access to accounts and resources, they often have limited visibility into access levels users possess to data and systems within the organization. And unfortunately, when accounts are not managed properly, they are more easily compromised and potentially lead to costly data breaches. In fact, according to the latest Cost of a Data Breach Report by the Ponemon Institute, data breaches across healthcare organizations cost an average of $7.13 million, higher than any other industry.

The Challenge

A large healthcare organization with nearly 10,000 employees, known as a national leader in providing healthcare solutions for people in need, serves more than five million Medicaid, Medicare, and Children's Health Insurance Program (CHIP) members. In order to address its top identity-related access risks, the organization had to navigate and tackle a complex web of challenges both inside and outside of the organization.

With pressure to ensure that sensitive health information was protected, the organization had to regularly prepare for audits that demonstrated compliance with the Health Insurance Portability and Accountability Act (HIPAA), while also expanding digital adoption of electronic health records from the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Meeting these increasing regulations presented an ongoing manual burden to the organization. In addition, the health system was under pressure to increase operational efficiencies even in the midst of a large restructuring effort. With multiple lines of business to manage and a complex environment of nearly 100 applications, mitigating access risks became increasingly difficult.

With this complexity of user roles across its application environment, including a high number of contingent workers, the organization had limited visibility into which users had access into each system and could not pinpoint what users could do with their access. It had no formalized or automated access provisioning, password management, or access certifications processes, and could not identify or prioritize its highest risk applications. On top of this, any introduction of more centralized identity and access management (IAM) programs would require attaining stakeholder and leadership buy in from across the organization.

The Solution

To address the complexity of this environment and ensure transparency, the healthcare organization set about on a journey to build an identity and access management strategy that would tackle these significant challenges. Guided by the Manager of Identity Management, a team of security professionals began building from the ground up, leveraging a three-fold strategy—put in the hard work required, break apart the complexity in the organization, and communicate and collaborate with stakeholders across the health system.

Putting in the Hard Work

Without formalized processes to work from, the team quickly recognized the importance of cleaning up all of the data within its environment. This sentiment is echoed by Gartner, which indicates organizations willing to put in the hard work of 'getting their house in order' through cleanup analytics demonstrate twice the ROI for identity and access management programs than those organizations that don't. The team also took painstaking effort to uncover and understand each of the organization's systems, applications, authentications, and entitlements across its complex network of business lines.

They also understood the importance of establishing strategic processes that would enable the organization to govern identities and manage the access of users across the nearly 10,000 employees and contingent workers. Recognizing the ongoing pressures to comply with increasing regulations, coupled with pressures to compete with other healthcare organizations and deliver quality patient care, the team identified Identity Governance and Administration (IGA) solutions as a strategic part of the overall IAM strategy and selected Core Security as a provider of choice. IGA solutions from Core Security would enable the organization to intelligently and efficiently manage who has access to what systems and when, and ensure valuable patient data was protected from identity-related access risks.

> *"You really have to put in the time and effort to understand your environment—from the applications to the entitlements across your organization—so you can truly recognize what they mean and how you can address their complexity. But if you are willing to dig in and stick with it, you will uncover the solution and build the processes that will improve your environment."*
>
> **- Manager, Identity Management, Large Healthcare Organization**

"You really have to put in the time and effort to understand your environment—from the applications to the entitlements across your organization—so you can truly recognize what they mean and how you can address their complexity," said the Manager of Identity Management. "But if you are willing to dig in and stick with it, you will uncover the solution and build the processes that will improve your environment."

Breaking Apart Complexity

Another key element of introducing a comprehensive IAM strategy was identifying the applications that were considered high-risk within the environment. The team identified Active Directory and its PeopleSoft HRIS as critical applications that the organization must address to implement an effective access management program. According to the Manager, "Both of these applications were sources of truth and served as interconnection points across the organization."

By prioritizing this critical data, the team was able to gain stakeholder buy in for standardizing naming conventions within Active Directory. They also worked to certify access for all user types, including contingent workers, and then incorporate each user type into PeopleSoft, the HR system of record. This fundamental step enabled the organization in identity mapping user access across the organization.

Breaking down the complexity even further, the team developed a strategic, phased approach in implementing the Core Security Password Management, Access Management, and Access Certification solutions. These solutions enable organizations to deploy simple, secure self-service password resets to automate password management, centralize access requests and approvals in a single interface, and manage and certify access rights to enforce last privileged access.

"Implementing an IGA program can often seem like boiling an ocean—you can't do it all at once," said the Manager of Identity Management. "By focusing on ease of implementation and cost avoidance as our primary drivers, we were able to begin our phased approach with password management." This strategy would then set the stage for justifying the other solutions from Core Security in subsequent stages.

Collaborating and Communicating

Because many of the high-risk applications identified as mission-critical for the organization were managed by other departments, the team recognized the importance of cross-functional collaboration as a key to success for developing the IAM strategy. IT and HR teams had to buy in to the vision for centralized, automated identity governance solutions and then partner with the security team to standardize data across both enterprise applications. This focus on working with the application owners supported ease of implementation and ensured communication was a central part of the strategy.

Another essential element for the healthcare organization was gaining leadership buy in from the top down. Proving the value of the IGA solution was essential for securing CEO support and made the entire effort more widely accepted across the organization. Similarly, with system-wide buy in, the team, over time, was able to make the case for hiring appropriate resources and building the broader identity management team internally.

The Outcome

With such a purposeful, strategic approach, the large healthcare organization was able to achieve its vision for a strategic IAM approach over time and gain organizational support that would address its greater institutional and access-related challenges. The healthcare organization has been able to streamline its password management solution, and in the first year alone, it saved nearly $190,000 in cost avoidance for supporting manual password resets across its user base. This savings enabled the health system to justify its phased implementation of other IGA solutions, including the Core Access, Core Provisioning, and Core Compliance solutions.

These intelligent identity governance tools have greatly mitigated identity-related access risks by ensuring visibility and management of user access across the complex array of systems, applications, and platforms within the organization.

Leveraging Core Compliance has transformed access certifications into a strategic priority, simplified the access review process, and ensured automated certifications are now a reality. This has enabled internal teams to easily respond to audit demands, particularly for HIPAA compliance, and remediate inappropriate or high-risk access where necessary. By leveraging a single interface, the organization can now more effectively identify and manage access rights and has largely eliminated manual certification processes—boosting operational efficiencies across the organization.

"With such a purposeful, strategic approach, the large healthcare organization was able to achieve its vision for a strategic IAM approach over time and gain organizational support that would address its greater institutional and access-related challenges."

Perhaps most important, the healthcare organization has enhanced its brand reputation as a provider of choice in protecting patient data. As organizations in the healthcare industry know, if you are not meeting regulatory compliance in one state or region, or your reputation is damaged in one specific line of business, it could adversely impact the organization in providing care in new locations or for renewing contracts within another state.

Throughout this entire process, the Manager of Identity Management and team have recognized the importance of the work they have undertaken. Since healthcare is such a high-target industry, they plan to expand the relationship with Core Security into the future. "Ultimately, it's all about making sure you are meeting ongoing requirements and minimizing risk. We have all seen the major breaches across our industry—and they result from not knowing who has access to what. I can't imagine not having visibility into our systems and platforms," said the Manager. "We recognized there was no magic bullet, but put in the effort to find the solution that makes our complex organization more secure."

coresecurity
by HelpSystems

www.coresecurity.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.