SailPoint

Customer Success

Integris Health
Protects Sensitive Data with Identity Security

Overview

Integris Health is a not-for-profit organization that manages health care facilities in the state of Oklahoma. It is the largest health network in Oklahoma operating 16 hospitals with health providers in 49 Oklahoma towns and cities.

Challenge

Healthcare organizations house highly sensitive patient information and are increasingly the attack target of data breaches. After failing several IT audits, Integris Health knew they needed a solution that would protect their patient data, and their healthcare systems in the event of a breach. This solution needed to integrate well with their clinical applications and track who had access to what within the organization.

Solution

Leveraging SailPoint, Integris Health now has a complete view of who has access to what within the organization, including their contract employees and has not failed an IT audit since implementing.

Integris Health is a growing healthcare organization with more than 10,000 full-time employees and 5,000 contract employees across several facilities and clinics.

Identity Governance Challenges

Healthcare organizations are under increased scrutiny around how they protect and secure access to patients' private healthcare information. To ensure adequate privacy and security protections for PHI, more healthcare organizations have started to rethink investments into security. Integris IT leaders were making increased investments in IT security to address compliance pressures around protecting healthcare data, while also putting measures in place to proactively protect themselves from a potential data breach, both of which could have serious consequences for the organization if not properly addressed. However, they had a limited view into the applications and health systems employees were accessing.

Integris had disparate repositories of identity information. One of the bigger issues was the lack of visibility for all employees with access to Cerner, which was their largest clinical application at the time. For full-time employees, Integris had the ability to track what the user requested access to, but lacked a view of what access had finally been granted. There was also zero visibility into what contract employees were accessing. Moreover, PeopleSoft was used to track full-time employee access to applications and information, but contractors were not put into the tool, and instead were managed ad hoc. After failing several IT audits, Integris knew it was time to properly secure their employees and contractors, as well as PHI and the information within their health systems, by implementing an identity security program.

Identity Governance Success

Integris implemented SailPoint, an automated next-generation identity solution, which allowed the company to align policy and establish consistent, centralized access controls across the enterprise. SailPoint provided the ability to identify higher-risk users for immediate focus, and allowed for easy access to audit and compliance data via business-friendly dashboards. Integris has successfully onboarded all compliance-relevant applications into SailPoint and now has a full view into "who has access to what" within the organization.

Integris now runs regular access certifications that satisfy the regulatory requirements around knowledge of who is accessing patient data. James Landers, Identity Access Management Security Engineer, said, "Implementing SailPoint was a huge win for the organization. We have contract nurses and therapists who are constantly coming and going, and they need access to systems and information to

do their jobs. It's important for employees to have the proper access needed, in a safe and secure way."

Integris has seen an incredible impact to their business since implementing SailPoint. When asked where Integris has seen the most improvement after adopting SailPoint, Landers outlined three key areas:

1. Have a complete view of users accessing applications within the organization. Upon bringing Cerner users into SailPoint and prior to transitioning to another EHR, Integris learned there were quite a few Cerner accounts not mapped to Active Directory accounts. SailPoint helped Integris correctly map Cerner accounts to Active Directory accounts, eliminate unnecessary Cerner accounts and establish a governance process for future provisioning.

2. Manage contract employees. Implementing SailPoint forced the need for an authoritative single source to track all types of employees. Integris moved forward with putting contract employees in PeopleSoft to address this issue, giving them the holistic view of the organization they were looking for. It also became critical to put access certification and provisioning in place for all employees. "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," Landers said. "This would not have happened without implementing SailPoint."

3. Manage the entire IT infrastructure. Integris has developed a termination process using SailPoint to deprovision major applications from users who leave the organization in a timely manner. Integris also recently went through the process of transitioning from Cerner to Epic. SailPoint worked closely with them through this transition, allowing them to further evolve and strengthen their identity program and IT infrastructure.

> **"Implementing SailPoint was a huge win for the organization. We have contract nurses and therapists who are constantly coming and going, and eed access to systems and information to do their jobs. It's important for employees to have the proper access needed, in a safe and secure way.**
>
> **James Landers**
> Identity Access Management Security Engineer,
> Integris Health

Identity Governance Lessons

Understand the business and processes before implementing a solution. For healthcare organizations looking to implement an identity governance program, the team at Integris recommends spending as much time as possible on discovery and business analysis. Working with your clinical staff will provide visibility into what is going on in the systems. Spend time learning the business process before putting technology, resources, time and budget in place to improve it. This will help you prioritize the security efforts to achieve quicker results.

Talk to other organizations addressing identity security. Landers recommends looking to organizations, even outside of healthcare, to learn how they are addressing their identity governance programs. "This has been incredibly helpful for Integris, and regardless of what stage you are in, I recommend taking the time to talk to identity professionals who have been in your shoes. Chances are they have some very interesting insights you can learn from when implementing or growing your own program."

What's next for Integris?

Next on Integris Health's identity governance roadmap are plans to develop a transfer management process. They are also beginning to explore privileged access management.

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.