CASE STUDY

Seamless ID management for healthcare and education

A top university's medical school finds a better solution for controlling and monitoring who accesses what data, where, when and why with One Identity and EST Group

Key Facts

Company
A university medical facility

Industry
Higher education and healthcare

Country
United States

Employees
4,500

Students
1,500

Challenges

A medical organization at a leading university needed to overcome identity and access management challenges that impeded security, regulatory compliance and overall efficiency.

Results

- Provisioning automation
- Compliance simplification
- Increases the efficiency of faculty, students and medical personnel
- Boosts IT staff productivity while cutting complexit

Products

Cloud Access Manager

One Identity Manager

Password Manager

One Identity Safeguard

Starling Two-Factor Authentication

University medical centers manage some of the most complex identity and access-management (IAM) solutions. In addition to meeting the IAM requirements all organizations face relating to identity verification, data access, privileged users and passwords, these organizations manage complex user roles that include conditional privileges for medical professors, staff and students. Plus they must comply with all major regulations including Sarbanes-Oxley, PCI DSS, HIPAA and FERPA.

One university's journey

A medical center at one of the nation's leading universities was facing all these challenges — and more. Its core applications, including an Epic health information system, were difficult to integrate with the existing IAM solution. Nearing end of life, the IAM product lacked modern tools, which meant IT staff also had to manually provision, monitor, deprovision and report on user

ONE IDENTITY

> "Our customer **meets its requirements** with One Identity products and **creates a very secure environment.**"
>
> *Tim Spires, President, EST Group*

access, privileged accounts and passwords for 4,500 faculty and staff, plus 1,500 students. People had to wait too long for system access and passwords. And when they switched roles, graduated or left the organization, their access privileges weren't immediately revoked, increasing security and compliance risks.

Why introduce more complexity?

To overcome its challenges, the organization engaged third-party EST Group. Tim Spires, president of EST Group, says, "We started our engagement by understanding everyone's roles and the overlapping relationships between the education facilities and medical facilities." Next, EST Group created solution options based on products from different vendors including One Identity. After evaluating its choices, the medical organization chose an end-to-end solution from One Identity because it was less complex, and easier to implement and support.

Improved control and security

Now that it's using its One Identity solution for IAM, the medical organization has greater control over data access. Administrators no longer have to manually grant, change or revoke access. Instead, they configure automated workflows in One Identity, based on roles in Active Directory, to manage these processes instantly and consistently. In addition, users who want to access certain systems or sensitive data must first verify their identity via multifactor authentication processes supported by One Identity Starling. The organization also has greater control over privileged accounts. It uses One Identity Safeguard to ensure access is granted and revoked based on established rules and processes.

Protected mobility and public-cloud service usage

Because Identity Manager works seamlessly with One Identity Cloud Access Manager, IT staff have extended these IAM and security benefits to external systems, along with mobile and remote users. As a result, it's easier for the medical organization to safely collaborate with other institutions and take advantage of third-party cloud services.

Increased IT staff efficiency

Instead of having to sort through log files from numerous systems, in just a few clicks authorized users now have detailed insight into who has access to what, when, where and why. They can also quickly generate the reports required for regulatory compliance. Nathan Wiehe, vice president of identity and security services at EST Group, says, "We saw a dramatic increase in the productivity of IT staff when they started using the One Identity solution because of their ability to model their processes, automate some lifecycle workflows and reduce help-desk call volumes."

ONE IDENTITY

> "We saw a **dramatic increase** in the **productivity of IT staff** when they started using the One Identity solution."
>
> *Nathan Wiehe, Vice President of Identity and Security Services, EST Group*

Better services for everyone

Students, faculty and business staff are saving time too. They get almost immediate access to needed systems and data based on their real-time role(s) in Active Directory. And if they must create or change passwords, they do so themselves with One Identity Password Manager. "Our customer meets its requirements with One Identity products and creates a very secure environment for its users and data — seamlessly and flexibly," says Spires. "It made the right solution choice."

About EST Group

EST Group is an IT solutions company, with a strong focus in providing integration and consulting services tailored around automating, managing and securing organizations' IT environments. Our goal is for our clients to achieve maximum efficiency and productivity.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

Learn more at OneIdentity.com

ONE IDENTITY