The Journey to IAM Success in Healthcare

ONE IDENTITY™

See how six
healthcare organizations
#GetIAMRight
with One Identity

Identity and Access Management (IAM) is many things.

For some, it's all about streamlining the user experience through technologies and practices that make it easier for them to securely log on. For others, IAM is about identity lifecycle management—ensuring that accounts are set up, modified and retired in a timely, accurate and secure manner. For still others, IAM means security and compliance, whether through technologies and practices that make governance activities such as attestations easy and complete, or by adding a layer of control and visibility to privileged accounts and "superuser" access.

The reality is IAM is all of this, and more.

For the healthcare industry, IAM is about granting the right people the right access to the right resources and in the right ways, thus reassuring stakeholders that security and compliance are in place. That's a lot of "rights," and it's not surprising that many in the healthcare field struggle with the implications for IT security.

At One Identity, we believe that IAM is a journey, not a destination. This journey is no casual walk in the park. Rather, it is a complex journey full of obstacles and lacking a clear map pointing the way to success. And yet no matter how arduous this journey is for any healthcare organization, it is both achievable and worthwhile.

On the following pages, read how six healthcare organizations are using One Identity solutions to

#GetIAMRight

Page Index

4 **B. Braun**
Identity Manager and Services

5 **A health sciences university**
One Identity Starling and Safeguard

6 **Laya Healthcare**
One Identity Safeguard

7 **New Hanover Medical Center**
Identity Manager

8 **Texas A&M University Health Science Center**
Identity Manager and Password Manager

9 **Swiss National Accident Insurance Fund**
Identity Manager and Services

Customer Profile

Company: B. Braun Melsungen AG

Industry: Healthcare

Country: Germany

Employees: 61,583

Solution: Identity Manager and Services

"Our investment in Identity Manager is enabling the business to pursue its cloud-IT strategy, while ensuring access management is locked down."

Andreas Mueller,
IT Project Manager,
B. Braun Melsungen AG

A cure for legacy access management ills

B. Braun in Germany automates identity and access management for greater security and compliance while enabling digital transformation

Today, B. Braun…
Protects company data through automated account provisioning and deprovisioning. B. Braun also boosts security with a hybrid environment that features cloud and on-premises systems. **As a result, it:**

Gives the right people the right access

- Automated account creation and termination enhance protection of company data.
- By ensuring that access for its 61,000 employees is more closely managed, the company can focus on business development and innovation.

Enforces the right level of control

- The company is now in greater compliance with data security regulations, with a lower risk of unauthorized data access.

Uses the right processes

- Employees know the position of their requests within the workflow at any given time.
- The company has a solution that links its on-premises infrastructure to cloud services such as Office 365.

Back to Index

Read the full B. Braun case study here.

Customer Profile

Company: A Medical School

Industry: Higher education and healthcare

Country: United States

Employees: 4,500

Students: 1,500

Solution: One Identity Manager, One Identity Safeguard, Starling Two-Factor Authentication, Password Manager, Cloud Access Manager

"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

Seamless ID management for healthcare and education

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

Today, the medical school...
Enjoys a solution that offers greater control over access to data, with other improvements in productivity, compliance, collaboration and the end-user experience. **As a result, it:**

Gives the right people the right access

- Administrators no longer must 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.

Enforces the right level of control

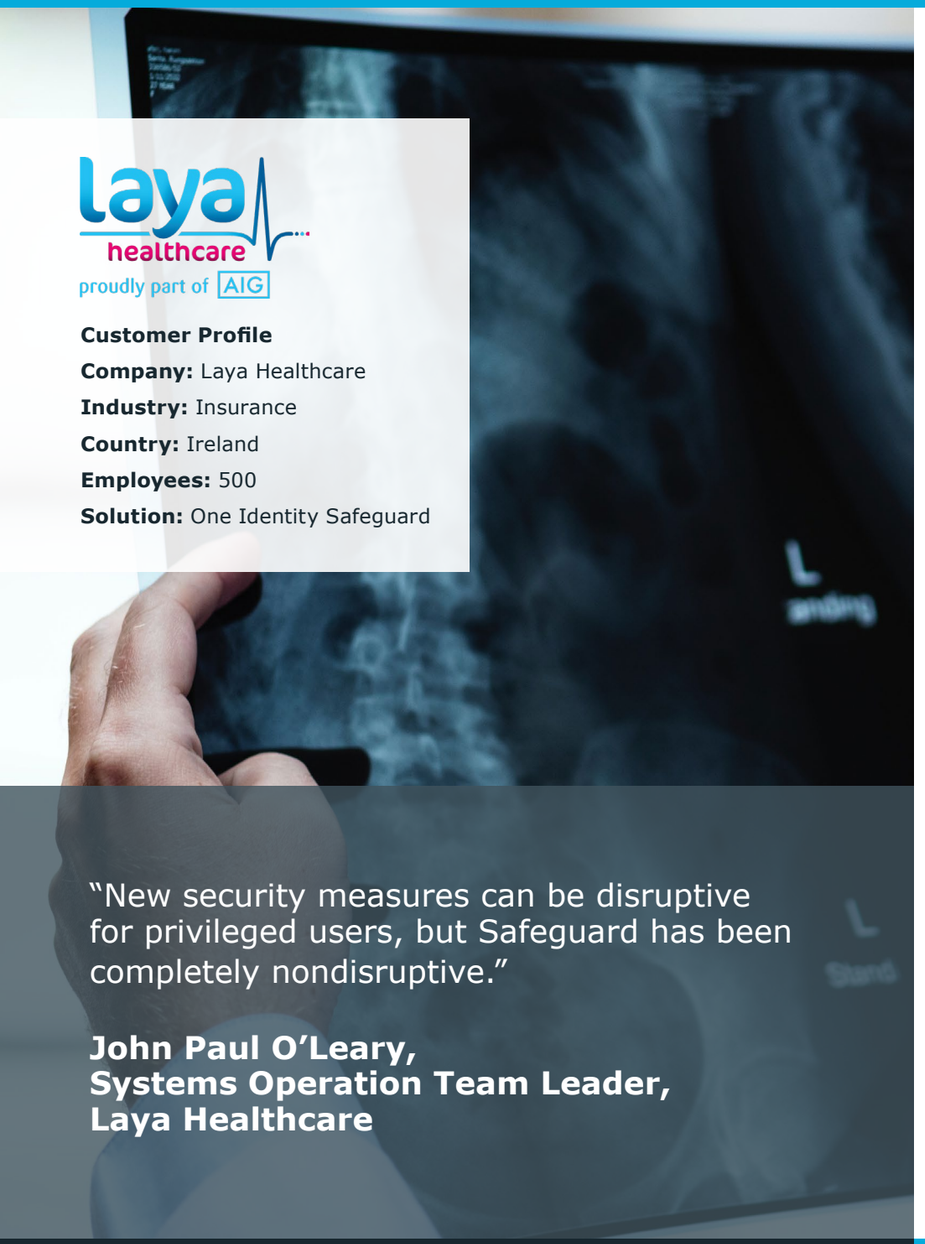
- Physicians, students and other healthcare professionals who want to access certain systems or sensitive data must first verify their identity via multifactor authentication processes supported by One Identity Starling.
- The medical school now has greater control over privileged accounts, using One Identity Safeguard to ensure access is granted and revoked based on established rules and processes.

Uses the right processes

- Connected seamlessly and securely to external systems, as well as mobile and remote users, the school can safely collaborate with other institutions and take advantage of third-party cloud services.
- IT staff have detailed insight into who has access to what, when, where and why, and can quickly generate reports for regulatory compliance.

Back to Index

Read the full health sciences university case study here.



Customer Profile
Company: Laya Healthcare
Industry: Insurance
Country: Ireland
Employees: 500
Solution: One Identity Safeguard

"New security measures can be disruptive for privileged users, but Safeguard has been completely nondisruptive."

John Paul O'Leary,
Systems Operation Team Leader,
Laya Healthcare

Better care outcomes with powerful identity management

Laya Healthcare enables faster patient services by streamlining privileged-user-access approvals and regulatory compliance

Today, Laya Healthcare...

Keeps sensitive information secure, complies with data management regulations, and enables privileged users to work efficiently at the right level of access. **As a result, it:**

Gives the right people the right access

- With the One Identity Safeguard solution, privileged users are able to obtain passwords in a single click.
- At the same time, administrators have session management oversight to ensure that sensitive data and applications remain secure.

Enforces the right level of control

- Laya can securely store, manage, record and analyze privileged access.
- One Identity Safeguard enables password storage, session management, monitoring, threat detection, and behavioral and biometric analytics.

Uses the right processes

- Laya now saves between 10 to 30 minutes with each privileged-user request, allowing medical staff to access patient information more quickly.
- Audit reporting has been greatly simplified.
- Laya meets the most stringent regulatory mandates for compliance, including General Data Protection Regulation (GDPR).

Back to Index

Read the full Laya Healthcare case study here.

New Hanover Regional Medical Center

Customer Profile

Company: New Hanover Regional Medical Center

Industry: Healthcare

Country: United States

Employees: 7,000

Solution: Identity Manager

"I have been able to report out to the board a compliance rate of 100% since we went live [and we] have a total of seven steps eliminated from the account-provisioning processes. Also, we had a first call resolution in our help desk calls go from 65% to 79%."

Eddie Parrish, CISO,
New Hanover Regional Medical Center

Simplifying Authentication, Strengthening Account Management

New Hanover Regional Medical Center implements One Identity, linking Epic, Active Directory and an ERP solution for more efficient and secure access management

Today, New Hanover Regional Medical Center…

Aligns its One Identity IAM solution with its Epic1 EHR system, achieving 100% automated provisioning and deprovisioning. **As a result, it:**

Gives the right people the right access

- Improved access management helps protect data and applications.
- Epic access for staff leaving the organization can be more quickly terminated.

Enforces the right level of control

- With the Person Identity feature, NHRMC administrators can see all account activity associated with each employee, making it easier to create and terminate accounts.
- Reporting is now consistent.

Uses the right processes

- Seven steps have been removed from the account-provisioning process, resulting in greater efficiency.
- There's now minimal variability in how accounts are created and terminated in the ERP solution.
- The compliance rate has improved from 72% before alignment to 100% today.
- Help desk and system engineer staff are no longer provisioning accounts, freeing them up for other tasks.

Back to Index

Watch the full New Hanover Regional Medical Center webinar here.

HEALTH SCIENCE CENTER
TEXAS A&M UNIVERSITY

Customer Profile

Company: Texas A&M University Health Science Center

Industry: Higher Education

Country: United States

Employees: 3,200

Solution: Identity Manager and Password Manager

"My teams are now looking at how to advance our solution for broader purposes. For example, we'd like to tie it into our card reader system so when a user's access privileges are revoked in Identity Manager, the card they use to get into buildings is also disabled."

Jody Harrison,
Associate Director of Systems Engineering,
Texas A&M University Health Science Center

Removing the bottlenecks and blind spots in IT access

Texas A&M University's Health Science Center streamlines identity and password management to improve security and staff efficiency

Today, Texas A&M University's Health Science Center…

Controls access privileges and passwords with a comprehensive solution that works seamlessly with Active Directory. **As a result, it:**

Gives the right people the right access

- Students, faculty and staff can use only the systems, services and data they need.
- The elimination of 500 inactive user accounts cut risk.

Enforces the right level of control

- The university consistently secures all its information and technologies — whether they're behind its firewalls or in a public cloud.
- People can access their informationand tools regardless where they are and what device they're using.

Uses the right processes

- Detailed reports and consistent policy enforcement simplify FERPA and HIPAA compliance.
- Users can modify their own passwords, which cuts down on help desk calls.
- Automated workflows provision and deprovision identities and access privileges via live feeds from HR and finance systems, reducing error and saving time and money.

Back to Index

Read the full Texas A&M University Health Science Center case study here.

suva

Customer Profile

Company: Suva

Industry: Insurance

Country: Switzerland

Employees: 4,200

Solution: Identity Manager and Services

"We're a lot more effective in how we manage access to our business roles with Identity Manager."

Sebastian Goodrick, Head of Identity and Access Management, Suva

Swiss National Accident Insurance Fund (Suva) takes the pain out of access management

Suva turns to One Identity for an IAM solution that lowers costs and makes access management easier, positioning the company to reduce premiums for its 2 million subscribers

Today, Suva...

Uses a simplified management solution that has reduced costs, increased security and accelerated development. **As a result, it:**

Gives the right people the right access

- The company's 4,200 employees can access the specific applications they need to fulfill 700 different business functions.

Enforces the right level of control

- Suva's IAM solution not only boosts data security, but it also reduces management complexity and future-proofs its IAM requirements.

Uses the right processes

- In the past, several teams were needed to manage access, but Suva has now moved IAM control to a small centralized team, reducing cost and complexity.
- With the new IAM solution, Suva's developer team can complete more projects, more quickly.
- Suva's IAM solution now seamlessly integrates with its existing SAP line-of-business applications.

Back to Index

Read the full Suva case study here.

Securing the right access for the right people in healthcare — #GetIAMRight with One Identity

Get the comprehensive IAM solution you need from One Identity to give the right people the right access, while enforcing the right level of control with the right processes.

Our customers get IAM right

29%

year-to-year growth

94%

of customers report overall satisfaction with their support experience

7,000+

global organizations use One Identity solutions to manage access, their way, for **130 million identities**

Industry experts recommend One Identity solutions for IAM

#GetIAMRight

Leader

Nine out of ten of the world's leading healthcare companies in the Fortune 500 rely on One Identity solutions

Readers Choice

Award winner for Governance, Risk and Compliance by Information Security magazine

Awarded

Best IAM Project by KuppingerCole at EIC to Identity Manager customers three years in a row

Comprehensive leader

and product leader in the 2018 KuppingerCole Leadership Compass for Access Governance and Intelligence

Recommended

identity and access management solution provider by SC Magazine

#GetIAMRight
with One Identity