SailPoint

SOLUTION BRIEF

The Case for Cloud Identity in the NHS

Too little money and too few people with the right skill sets create a disastrous combination for healthcare organisations trying to protect sensitive patient data. While this condition exists across the National Health Service (NHS), cloud computing can counter its negative effects. Because cloud applications are cost-effective and less complicated to deploy compared to on-premises software, healthcare organisations can do more with less. And now, cybersecurity solutions can also be administered from the cloud – enabling NHS trusts to efficiently govern access rights to the sensitive health information they house.

Why Cloud? Why Now?

In recent years, the number of health data breaches in the UK have dramatically risen. In the face of ongoing cybersecurity threats, NHS trusts have struggled with mustering sufficient funds and filling the skills shortage required to adequately secure sensitive patient data. To address these concerns, the NHS recently announced additional cybersecurity investments, and its intent to embrace a "cloud-first" approach, which would lead to cost savings and flexibility to modernise the health IT infrastructure. These conditions are ideally suited for cloud identity – a technology that enables NHS trusts to efficiently and securely govern the access rights of health information users.

100K

Unfilled UK cybersecurity jobs by 2022[1]

211%

Rise in UK health security incidents from 2016 – 2017[2]

€150m

Recently added cybersecurity funding by NHS[3]

[1] Computerworld UK, Most in-demand cyber security jobs in the UK
[2] CIS, Healthcare experiences 211% increase in disclosed security incidents in 2017
[3] Health Business, Transforming healthcare through cloud technology

The Role of Cloud Identity in NHS Cybersecurity

Cloud identity governance gives NHS trusts the ability to identify and control who has access to what applications and files, who should have access to these resources, and how that access is used. The technology is less difficult to manage compared to "smart cards" currently used by many trusts to not only access facilities and devices, but also applications. For instance, retrieving these cards from separated employees and contractors can prove very difficult – thus leaving access cards in the hands of those who should no longer have such entitlements to an IT network. This is a huge security risk for any healthcare organisation.

With cloud identity, these challenges no longer exist as credentials and access entitlements are managed online. Moreover, healthcare organisations can apply cloud identity without the need for initial capital expenditure or a large, dedicated identity team to maintain and update the system. In fact, it enables rapid deployment of controls to address critical healthcare use cases that affect security and compliance.

Healthcare Use Cases	How Cloud Identity Helps
Drive IT Efficiencies and Reduce Costs With tight budgets, lean staff, and growing requirements due to an expanding IT network, the NHS trusts need to create efficiencies to adequately address security and compliance matters.	• Reduce resource requirements for updating and patching identity software solution. • Reduce capital expenditure costs by eliminating the need to maintain a hardware infrastructure. • Reduce helpdesk calls through self-service access request and password reset.
Securely Manage Diverse User Population The user population within a healthcare provider organisation consists of staff, non-employed staff, partners, contractors, and volunteers.	• See and govern access across the entire organisation, including systems, applications, and data both on-premises and in the cloud. • Proactively monitor for inappropriate or malicious access to reduce risk.
Comply with Government Regulations NHS trusts must comply with government regulations (ex. GDPR and UK's Data Protection Bill).	• Automate periodic review of access rights to reduce cost of compliance while improving effectiveness. • Apply preventive and detective controls to ensure access complies with organisational policy. • Establish identity audit trails to help ensure that you can pass internal audits and adhere to regulatory mandates.

Healthcare Use Cases	How Cloud Identity Helps
Remove Disparate Processes Securing digital identities and their entitlements to systems, applications and data requires a consistent and unified approach. This reduces delayed access for users, avoids improper provisioning, and cuts down workload for IT administrators and data stewards.	• Integrate with the entire spectrum of systems, applications and data used within the organisation to rapidly deploy identity and drive ongoing consistency in access governance.
Improve User Access Workflow All provider organisations must balance security with workflow. CIOs and CISOs must ensure that clinicians and other operational staff have timely access to the necessary data to deliver care.	• Empower end-users and reduce burden on IT by deploying self-service access requests and password resets. • Automate provisioning to ensure fast delivery of access to users upon joining the organisation, moving to a new role, or leaving the organisation.
Reduce Inconsistencies from Managing Multiple Authoritative Sources Many healthcare organisations have multiple authoritative sources including human resource (HR) and physician credentialing applications. Managing multiple identity sources and their access rights creates difficulty in ensuring consistent execution of policies and resource optimisation.	• Correlate and link all access and profiles to simplify the challenges with managing multiple authoritative sources.
Simplifying Complexities Around Users with Multiple Personas Is it appropriate for a hospital-employed clinical assistant to have the same access entitlements when they are doing volunteer work for a health association? The challenge of managing data access for users with multiple roles, otherwise referred to as personas, is especially pronounced within the healthcare provider space.	• Remove the complexity for securely governing identities with multiple persona. • Transparently show all personas and their access rights in a centralised view.

How to Know if Cloud Identity is Right for You?

While the benefits of cloud identity are clear – faster deployment times, cost savings, simplified management, and increased operational agility – there are still elements to consider before deploying identity governance from the cloud. The several following questions will help you determine if implementing a cloud identity governance solution is right for your trust.

- **Is your organisation flexible enough to redefine its approach to governing identities?**
  First, regardless of how it is deployed, an effective identity governance solution must provide complete visibility across all applications and data whether they are on-premises or in the cloud. This provides the foundation required to build policies and controls essential for security and compliance with various regulations. It should also include the ability to automate these controls to reduce human error and relieve an overburdened IT. Cloud identity governance solves all these identity-related problems – but it does so by using a configurable best practices framework approach. For the NHS trusts that may not have the time or expertise to create custom identity policies or compliance processes from scratch, this provides an ideal and rapid approach to identity governance.

- **Do you have limited resources for administering an identity governance program?**
  Effective identity governance requires an artful blend of people, processes and technology. If you have limited resources, either in size or expertise, the cloud is a good option. With minimal hardware to upgrade, no software patches or updates to install, or infrastructure to manage, deploying and administering an effective identity governance program becomes exponentially simpler. This makes cloud identity an ideal option for NHS trusts that have smaller identity management teams or IT and security teams that don't have a deep bench of expertise.

- **What is the right vendor for me?**
  Cloud identity governance maximises security and compliance while minimising impact on IT resources. Thus, it's important to work with a vendor that possesses a deep understanding of how identity impacts healthcare organisations. The vendor should also be invested in your long-term success and approaches the relationship as a partner. NHS trusts should expect demonstrable proof that the vendor's approach has benefited other similar healthcare organisations.

Cloud identity gives NHS trusts the ability to mitigate cybersecurity and compliance risks without heavy impact to IT resources. Without heavy initial expenditures and large expert teams on site, this technology can efficiently deliver fine-grain control over access to all your cloud and on-premises applications and data files, while providing secure, self-service capabilities for your entire user population.

To learn more, contact us for a free initial consultation at **sales@sailpoint.com** or call **1-888-472-4578**.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1292-1904