How Cloud-Based Identity Can Drive Cost Savings and Greater Efficiencies in UK Healthcare and Pharma

Introduction

Healthcare in the UK has traditionally lagged most other industries in terms of technology adoption. Many hospitals, GP practices and other organisations still rely on paper records, handwritten notes, siloed data stores and IT systems, and even film-based radiology images. Information sharing across providers can be inefficient and data portability rare. It's not unusual to see many NHS providers rely on outdated communication platforms, and collaboration and coordination of care processes is a challenge.

However, things have already changed dramatically over recent years, and digital transformation is increasingly at the centre of government efforts to cut costs and boost efficiencies while improving the delivery of key services. NHS Digital is tasked with driving this change and has an ambitious target of turning the entire health service paperless by 2020.

It claims that better use of data and technology can:

- Give patients more control over their health and well-being
- Empower carers
- Reduce the administrative burden for care professionals
- Support the development of new medicines and treatments

It's also important to remember the crucial role that pharmaceutical companies play in the UK healthcare ecosystem. They're a key collaborative partner to many healthcare organisations (HCOs), exchanging highly sensitive patient data to facilitate important clinical trials for new medicines and treatments, as well providing patients with useful info on how to manage their conditions. New digital technologies have made this information sharing and management easier, but also expose both sides to greater cyber-related risk.

In the rush to streamline processes and empower patients by migrating to cloud and app-based systems, identity and access management (IAM) therefore becomes vitally important. Healthcare and pharma organisations are a major target for hackers and mistakes by employees can also expose highly sensitive patient data and IT systems.

That makes Identity as a Service (IDaaS) the only choice to ensure HCOs can leverage the transformative benefits of new digital platforms whilst staying safe, secure and compliant.

Healthcare goes digital

Gartner Research VP and industry expert, Barry Runyon, believes the growing infrastructure, system and support requirements of healthcare organisations, alongside increasingly tight budgets and staffing challenges, are driving them towards greater cloud adoption. Cloud services are already being used in some cases to support content management, medical record systems, portals and clinical collaboration.

The challenges facing UK HCOs and pharma firms

“The healthcare provider has been taking measured steps toward the cloud over the past few years and while it hasn't embraced the cloud entirely, it has accepted the fact that it has its place and will play a bigger role in IT service delivery in the next few years as cloud service providers mature.“

> "My sense is that a significant percentage of the healthcare providers' workload will move to the cloud in the next 5-10 years"
>
> **Frost & Sullivan Senior Industry Analyst, Swapnadeep Nayak**

NHS England Chief Digital Officer Juliet Bauer believes digital apps and products "have enormous potential to empower patients to take control of their healthcare and improve the services we can offer." In fact, she has made £45m available to run several pilot programmes which have helped democratise patient access to services via apps/websites.

However, these digital transformation efforts must be viewed in the context of a growing range of challenges facing UK HCOs and pharma firms. These include:

Cost pressures: The 2015 Spending Review set out plans provide the NHS in England £10 billion per annum more in real terms by 2020-21 than in 2014-15. However, the NHS is expected to deliver £22 billion of efficiency savings—as set out in the Five Year Forward Plan—without diminishing the quality of healthcare. Savings on this scale have been described by experts as "unprecedented" and at least one leading think tank has predicted a spending gap of over £20 billion by 2022/23.

The need to reduce costs and improve efficiencies inside the NHS makes the case for digital transformation even more urgent.

Staffing crisis: Over 86,000 NHS posts including IT positions were vacant during the period January-March 2017, in what some have described as a "skills crisis". With Brexit exacerbating the problem, the need to streamline, automate manual processes, and empower patients to self-serve becomes ever more acute.

Fluid and diverse users: Healthcare is one of the most complex environments you can imagine when it comes to granting and enforcing access rights. There's a multiplicity of different roles to consider among healthcare professionals. Even among doctors there's a range of roles from consultant down to Year One medical student, all of whom need access to different systems across multiple departments and facilities, with differing permissions. There are also potentially third party contractors and/or business partners that may need access to some data.

Compliance: There are already strict codes of practice governing how records should be managed and data secured. These will be expanded by the EU General Data Protection Regulation (GDPR), which requires strict data security controls to keep employee and patient PII safe and secure at all times. The new law, set come into force on 25 May 2018, includes fines of up to 4% of annual turnover or £17m, whichever is bigger.

Collaboration: As mentioned, there's a growing need for pharmaceutical companies to interact with HCOs, accessing and sharing sensitive patient data for clinical trials and ongoing treatments. However, doing so in a seamless, user-friendly and secure way can be a challenge, especially given the potentially large number of HCOs and pharma companies that need to collaborate with each other.

Cybersecurity: Patient data is a potentially lucrative and popular target for hackers. Data stores can be targeted via phishing attacks designed to harvest account log-ins. Ransomware is also a major concern with the potential to knock out key services for days. The WannaCry attack of May 2017 caused an estimated 19,000 cancelled NHS appointments and operations and disrupted over a third (34%) of Trusts in England. These rising threat levels have forced the government to fund a £20m Security Operations Centre for NHS Digital.

There's also the risk of patients being targeted by info-stealing threats aimed at harvesting their log-ins, and of staff accidentally or deliberately leaking/stealing information.

Enter cloud-based identity

The UK's HCOs and pharma firms need a way to accelerate access to patient data while minimising password management problems. They need strong, MFA to negate the risk of phishing and password stealing/cracking/guessing attacks. And they need to do all of this to stay compliant with current regulations and the forthcoming GDPR. Doing so in a user-friendly way and with a dwindling budget becomes an increasing challenge. This is where single sign-on (SSO) can help, but be aware that legacy IAM tools are fast becoming obsolete.

The truth is that on-premises IAM tools are a poor fit for the kind of modern, cloud and app-based systems

UK HCOs and pharma firms are increasingly migrating towards. They're costly and time consuming to integrate and are inflexible, requiring significant ongoing maintenance and upgrade work every time a new app is added.

To manage an environment as complex as a typical NHS Trust, for example, you need to outsource IAM to the experts. IDaaS is the answer: securing access at the cloud app layer rather than the perimeter and providing granular visibility into all apps, users and devices from a single interface. It's also highly scalable—new apps and users can be added and managed with ease —it's reliable, easy to set-up, and there's no unnecessary downtime.

In this context, SSO comes alive, allowing approved doctors, nurses, and others to access any cloud services with just one username, one password and one session. This helps improve productivity by reducing the time spent logging into each application; reduces costly helpdesk password reset requests; and improves account security as users are less inclined to use the same simple password for all apps. It becomes even more powerful when backed with MFA for extra account security, which means attackers can't guess, steal or crack log-ins in any meaningful way.

Enhancing security for Major Healthcare company

Major Healthcare company is already leveraging the benefits of the Okta Identity Cloud. The firm is transitioning to a new cloud and application-based services infrastructure to stay agile and competitive while keeping costs down and improving patient care for diabetes sufferers. It chose Okta to support these efforts whilst meeting strict cybersecurity requirements for what is a heavily regulated industry.

"The Okta Identity Cloud features chosen by Roche included Single Sign-On (SSO) backed with adaptive Multi-Factor Authentication (MFA)," explains the Okta champion. "The beauty of Okta is its ability to integrate with the customer's legacy infrastructure and new cloud-based tools like Office 365, for which the firm has to manage 500,000 log-ins each month and 9,000 mailboxes," he says.

MFA in particular has enabled this team to enforce strong authentication without disrupting the business; for example, restricting access based on where the user is located and what app they're trying to use. Tight integration with Active Directory has made managing the identity lifecycle of each employee and contractor child's play.

"Our experience of working with the Okta team has been very good so far. The tool itself is very solid so we haven't had any problems with availability or stability. We've also received support from the Okta team to accommodate our specific requirements," says Okta Champion.

"The mission of IT is to support the mission of our company: to improve the life of our patients. We're very proud of now being able to offer this kind of support … and with Okta we're growing together all the time."

Supporting UK healthcare and pharma

Okta's Identity Cloud platform supports UK healthcare and pharmaceutical providers' efforts to move to improved and more cost efficient digital services whilst keeping data and mission critical IT systems secure. It offers:

Secure cloud access: You need a scalable, agile foundation to manage apps and secure highly sensitive patient data. Okta provides cloud identity that benefits both IT departments and end users.

Agility for mergers and acquisitions: Don't let identity slow your consolidation efforts. Okta helps to avoid the friction and cost of consolidating AD domains, so you can seamlessly transition any number of organisations to a common set of tools quickly, without interruption.

Secure & efficient collaboration for value-based care: Population health initiatives require collaboration among many providers. Okta's flexible architecture enables secure and efficient access to any apps shared across providers, without compromising the user experience or security.

Secure & seamless patient experience: Patients want to engage on their own terms. Whether you're a payer looking to acquire new customers online, or a provider who wants to unify a constellation of patient portals, Okta makes web and mobile access secure, compliant, and frictionless.