okta

Overcoming Barriers in Healthcare Digital Transformations

The healthcare industry is in the midst of a substantial shift toward a quality focused care model. While the transition from fee-for-service care to value-based care has been underway for some years, provider organizations are still grappling with implementing systems and processes to support this new model of healthcare. Meanwhile, costs continue to rise, with healthcare spending in North America projected to surpass $4 trillion by 2022 and global spending to be north of $10 trillion.[1] In addition, regulations like HIPAA and HITECH in the United States continue to hold healthcare organizations to high levels of accountability for security and privacy practices.

In order to curb costs and adopt new care delivery models focused on improving patient outcomes and access to services, healthcare organizations have turned to technology to help them scale. However, these healthcare digital transformations present their own set of challenges as organizations must implement solutions that are secure, and at the same time provide seamless experiences for end users.

This whitepaper will explore three major challenges healthcare organizations need to consider for their main user populations - patients, partners, and internal employees - and how identity can help organizations excel across these use cases.

Challenge: Low Patient Portal Adoption

The premise behind value-based care is to provide patients with the highest quality of care possible. Achieving this requires an ongoing relationship between patient and provider. To this end, many healthcare providers offer online portals as a way to engage with patients outside the care facility. By offering a patient access to their health records, lab results and a means to communicate with their care team, patient portals provide additional resources and convenience for both patient and provider. There is also growing evidence portals can help improve access to care, self-management of health, care coordination, and reduced healthcare costs.[2] However, a lack of trust and poor user experience for patients can be detrimental to achieving these outcomes.

Patient portals don't serve anyone if they're not being used. One of the major barriers to use is the patient's perception of potential security or privacy risks. In a recent brief, the Office of the National Coordinator (ONC) for Health Information Technology found that 25% of patients do not access their online medical records because of security or privacy concerns.[3]

---

[1] Deloitte 2019 Global health care outlook
[2] Electronic Patient Portals: Patient and Provider Perceptions
[3] 2018 Office of the National Coordinator (ONC) for Health Information Technology Data Brief

Even those patients who trust a portal may have to overcome a poor user experience. This generally presents itself in two ways. First, the process for signing up for a portal can be challenging for many users. When faced with a complex sign-up experience, customers are likely to abandon the process. In fact, 71% of customers abandon sign on when faced with friction.[4] As patient portal sign-up often requires multiple complicated steps or requests for information the patient doesn't always have on hand, healthcare portals are at high risk for abandonment. This can be amplified even further as patients attempt to sign-up and access portals from mobile devices upon leaving the facility.

Second, patients can face portal overload. For example, a single clinic visit can actually involve many different players. There's the main hospital or clinic entity the patient visited, but labs could be done by a separate organization. The payer or insurance company is yet another entity. If all these organizations have their own separate portals, that's already three portals a patient will have to navigate through to get the complete picture of a diagnosis, treatment plan, and costs. Not to mention the branding and user flow is often completely different across all three portals. These challenges present insurmountable barriers for some patients, especially the elderly and others in medically underserved communities who may not have access to technical resources.

Solution: Identity as the Foundation for Patient Portal Engagement

In order for healthcare providers to get the most value out of patient portals, they must first ensure a secure experience followed by a simple sign-up and sign-on process and an engaging and user-friendly portal experience. Identity solutions can integrate with patient portals to help achieve all these goals.

Earning a patient's trust and ensuring the security and privacy of personal health information requires additional security measures.

Dignity Health

Dignity Health, which is part of CommonSpirit Health, a leading healthcare system in the United States, is committed to serving its communities across the country. The organization boasts 60,000 employees and a network of 10,000 physicians, 41 hospitals and 400 care centers. Operating under the brand promise "Hello humankindness," Dignity Health is a vibrant healthcare system, known for clinical excellence and accessible service for all.

The organization resolved to streamline patient processes and deliver the digital accessibility today's patients crave. Instead of multiple logins and passwords, telephone calls and mail, Dignity Health sought a "one person, one login, one password" identity solution and looked to the marketplace for an identity partner.

Dignity Health used Okta's User Management, Authentication and Authorization products to develop a consistent, frictionless experience that streamlines patient access to health services and records. "In order to provide a frictionless customer journey, we wanted to make sure that we don't have multiple patient portals with multiple logins and multiple passwords for a single patient," Rabir Samra, who leads data, architecture and platform engineering for the Digital division of Dignity Health, explains. "We want one login, one password, and one digital identity that unlocks the door to many of the services that the Digital division provides."

[4] Customer Experience Silos Research Report

This should include the addition of adaptive or risk-based multi-factor authentication (MFA) to the login process to help ensure only authorized individuals have access to the patient's medical and health information.

For a simple sign-on experience, organizations should consider implementing single sign-on (SSO) to patient portals hosting multiple services. This allows the patient to use one set of credentials to securely access all their health-related resources, which may include appointment scheduling, communication options with their health team, lab results, billing and payment options, and other integrated wellness apps. As many healthcare providers leverage portals provided by EHR vendors like Epic and Cerner, direct integrations with these EHRs and the identity platform is highly beneficial.

Choosing an identity solution with customizable, out-of-the-box functionality can help healthcare organizations quickly create a modern onboarding experience without extensive time or resources from their IT teams. An identity provider who is able to unify web, mobile, and omni-channel experiences, as well as easily allow for consistent branding, will also further decrease friction and enhance the user experience for patients.

Challenge: Connecting with Partners Drains Resources and Creates Security Risks

Many healthcare organizations work with a multitude of business partners to provide comprehensive care and services. For example, a hospital that may work with outside ambulance services and EMTs in the emergency department. These business partners may need access to sensitive information like patient health records in order to do their jobs, but they don't need access to all the hospital's business applications like Workday or Salesforce. Similarly, other functions in the hospital like food services may be contracted out and do not need access to patient health information at all.

With large and diverse user types, healthcare organizations face the challenge of ensuring each user has access to the necessary apps for their job, but nothing more to meet security and regulatory requirements. They also must consider managing the entire life cycle of a partner user to ensure that access is assigned and revoked appropriately. This can be a daunting task for a healthcare organization's IT department. In many situations, the healthcare organization has no visibility into the employment status of a partner user and doesn't know when access to applications should be revoked.

For end users at partner organizations, it can be equally frustrating having fragmented experiences and redundant logins for multiple systems to perform job duties if partner apps are not integrated. Forgotten passwords or reuse of passwords across different systems becomes both a headache for users and a security risk for the organization. Plus, usability difficulties can again take up IT and helpdesk resources as partner users file tickets and request support.

Solution: Identity Enables Efficient Partner Collaboration

The ideal solution addresses partner user experience and closes security gaps for the healthcare organization without burdening the IT department. To eliminate multiple logins for business partners, healthcare organizations can use SSO to partner portals to mimic the same one-login, one-account, one-portal experience for their partner users as they use for patients and employees. An adaptive MFA solution with a directory integration to a partners' directory can also close security gaps. This would help ensure users requesting access are who they say they are, while directory integration allows partner organizations to manage their own user lifecycles. The primary healthcare organization's IT department would not have to manually revoke access for partner users as this could be done automatically if a partner user is removed from their own directory.

Challenge: IT Complexity Hinders Productivity

Healthcare organizations, like those of many industries, employ staff and contractors with varying access needs to resources. However, certain employees also need access to particularly sensitive information, like patient health records, that is frequently targeted by cyber attacks. Even users with approved access to protected health information (PHI) often have to go through additional verification for certain procedures. For example, doctors performing electronic prescribing of controlled substances (EPCS) must use MFA to sign prescriptions. On the other hand, some employees, such as those performing business or IT functions, should have no access to PHI but may have access to other sensitive data like financials and security systems.

Balancing security requirements with employee user experience is critical to keeping healthcare professionals focused on their most important work. Managing multiple credentials and repeating login processes across applications is not only tiresome for medical staff whose time can be better spent treating patients, but also it often results in poor password habits like using the same credentials across multiple accounts for convenience.

Mount Sinai

The Mount Sinai Health System is an integrated health system based in New York City committed to providing distinguished care, conducting transformative research, and advancing biomedical education. With over 38,000 collaborators across 7 hospitals and a medical school, Mount Sinai realized the lack of interoperability between healthcare partners in acute care, primary care, and community services created barriers to healthcare for underserved populations and drove up healthcare costs. Also wanting the ability to scale on demand, Mount Sinai looked to Okta to help achieve their goals of integrating partners and make care more accessible to all.

Mount Sinai leveraged Okta Authentication, Adaptive MFA, and B2B integration to create a community gateway for all their business partners to connect, access resources, and securely share information. With Okta, partner users' access to Mount Sinai resources was automatically revoked once they left their own organization, relieving Mount Sinai IT teams of the burden of managing partner user lifecycles. With a patient base that mainly interacts with care collaborators outside hospital walls, Okta's cloud-native identity platform was crucial to Mount Sinai's ability to rapidly grow and reach patients.

With the growth of telemedicine and new care methods, the modern healthcare employee also needs access to apps independent of physical location. The challenge for healthcare organizations is ensuring each employee has the right amount of access to the apps they need for their job wherever and whenever they need access to them. At the same time, organizations need to prevent over-provisioning access to unneeded apps to limit risk and possible attack surface area.

With a high volume of diverse user types, provisioning employees when they join may be a headache. However, not off-boarding employees immediately when they leave the organization can pose a huge security risk. As healthcare is the only industry where more security incidents are the result of internal actors instead of external threat actors, promptly revoking access to resources once an employee leaves is critical. [5]

These challenges are multiplied with the increasing trend of mergers and acquisitions in healthcare.

[5] Verizon Protected Health Information Data Breach Report

As healthcare organizations grow through acquisition, they also find the need to create faster, repeatable processes for onboarding acquired employees and providing secure access to necessary apps from day one. During this time, IT teams are also being tasked with managing and consolidating the networks, systems, and directories of acquired entities.

Solution: Modern Identity Provides Seamless, Secure Employee Experiences

A comprehensive identity and access management solution is required to address the challenges associated with providing secure access to applications for internal healthcare employees.

SSO to employee applications provides an easy, user-friendly way for employees to access all the apps they need through a single set of credentials. Assigning users into user groups and applying access policies to apps based on their role in the healthcare organizations also ensures the right privileges for the right people to the right applications.

Implementing additional context-based authentication with an adaptive MFA solution further secures access while also maintaining a good end user experience. And with respect to additional identity verification through MFA, choosing an identity solution with integrations to leading EHRs like Epic makes processes like EPCS simple for doctors and ensures compliance.

An ideal identity platform should also be able to tackle employee lifecycle management. Automatic onboarding and offboarding eliminates repetitive IT processes when employees join, leave, or change roles within the organization. This, plus a universal directory or directory integration, and directory consolidation also allows healthcare organizations to onboard new employees at scale after a merger or acquisition.

Finally, an identity platform should have robust logging capabilities to provide visibility into app access. These logs can also be aggregated with other security and network logs for threat detection, prevention, and analysis.

As one of the largest providers of physician services to hospital and health systems, Envision Healthcare is responsible for more than 30 million patient encounters in the United States annually. With three primary business units across physician services, ambulatory surgery, and hospice services, Envision Healthcare has a large contingent of mobile employees that needed secure access to applications from various locations. Mergers and acquisitions, a core part of the organization's growth strategy, also resulted in application sprawl with limited visibility into app access and onboarding challenges. Envision Healthcare teamed up with Okta to solve their workforce challenges.

With Okta SSO, Universal Directory, and Adaptive MFA, Envision Healthcare was able to provide employees with a single set of credentials to securely access all their applications from any device and from any location. By using Okta to create automated onboarding and offboarding processes, onboarding users from mergers and acquisitions was simplified. Individual hospitals could manage their own deprovisioning without the help of corporate IT teams, yet Okta's reporting capabilities also provided IT with the information needed to ensure adherence to regulations and pass audits.

Okta for Healthcare

Okta provides easy, centralized identity and access management for all key healthcare user groups: patients, partners, and employees. The Okta Identity Platform allows for flexible and customizable use cases to fit each organization's needs. This allows healthcare providers to easily create secure, customized patient portal experiences and to adopt digital transformation at their own pace. Our API-based infrastructure is designed for extensibility to fit healthcare's custom needs, accelerating your integrations across apps and services.

Okta also supports key healthcare integrations with technology partners like Epic and Cerner; business apps like Office 365 and Workday; and application delivery systems like Citrix, through our Okta Integration Network. Okta's vendor neutrality facilitates healthcare organizations' multi-cloud and best-of-breed strategies.

Plus, security is built into our infrastructure and services. Built in the cloud but also able to support on-premises systems, Okta is designed to be the foundation for a modern zero-trust security architecture, a necessity for the healthcare industry. We also help customers maintain and prove adherence to healthcare security regulations like HIPAA and EPCS.

To discover more ways on how Okta can help modernize and secure your healthcare organization, visit www.okta.com.