okta

FedRAMP HIPAA

How to Achieve Frictionless Identity Management in Government Healthcare

The healthcare industry is undergoing a substantial shift toward a quality-focused care model. While the transition from fee-for-service care to value-based care has been under way 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, federal healthcare agencies have turned to technology to help them scale. However, these healthcare digital transformations present their own set of challenges as agencies must implement solutions that are secure, while also providing a seamless experience for citizens.

This whitepaper explores three challenges healthcare agencies need to consider for each of their main user populations — patients, partners, and government employees — and how identity and access management can help them 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 federal agencies offer online portals as a way to engage with patients outside a care facility. By offering patients access to their health records, lab results, and a means to communicate with their care teams, portals provide additional resources and convenience for both patients and providers. There is growing evidence that portals also improve access to care, encourage self-management of health, ensure better coordination of care, and reduce healthcare costs.[2]

But that's possible only if patients use the portals. There are several barriers to use, including lack of trust, poor user experience, and portal overload. In a recent brief, the Office of the National Coordinator (ONC) for Health Information Technology found that 25 percent of patients who do not access their online medical records do so because of

[1] Deloitte 2019 Global health care outlook

[2] Electronic Patient Portals: Patient and Provider Perceptions

security or privacy concerns.[3] Even patients who trust a portal may have to overcome a poor user experience. Signing up for a portal can be challenging, and patients that encounter a complex sign-up process are likely to give up. The portals often require multiple complicated steps or information patients may not have on hand.

In fact, when faced with such friction, 71 percent of customers abandon signing up.[4] This can be amplified even further as patients attempt to sign up and access portals from mobile devices upon leaving the facility.

Add to that the fact that patients are often asked to use many different portals. A single clinic visit often involves many different players: the clinic, an outside lab, and the payer. If each has its own separate portal, that's already three portals a patient must navigate to get the complete picture of a diagnosis, treatment plan, and costs. And navigation can be completely different from one portal to the next.

These challenges present insurmountable barriers for some patients, especially the elderly and people in medically underserved communities who may lack access to technical devices and resources, such as Internet access and technical support.

Solution: Identity as the Foundation for Patient Portal Engagement

To get patient adoption and value from portals, organizations must provide a secure, friction-less, user-friendly experience.

Earning a patient's trust and ensuring the security and privacy of personal health information requires striking the right balance between robust security and a positive user experience. This can be done through a tailored approach, known as *progressive profiling*, in which users are asked the right questions at the right time to deliver both a secure and frictionless experience, which ensures only approved individuals can access a patient's medical and health information. A single sign-on (SSO) process removes friction by allowing patients to use one set of credentials to securely access all their health-related resources, including appointment scheduling, communications with their health team, lab results, billing and payment options, and other integrated wellness apps. Because many healthcare providers use portals provided by EHR vendors like Epic and Cerner, it's helpful if the identity platform has direct integrations with these EHRs.

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 team. An identity provider who is able to unify web, mobile, and omni-channel experiences will also further decrease friction and enhance the user experience for patients.

Challenge: Interoperability Problems Undermine Continuity of Care When Multiple Organizations are Involved

Government healthcare organizations work with a multitude of public and private partners to provide comprehensive continuity of care to citizens. Think of the organizations involved when a veteran is enrolled in a clinical cancer trial, for example: National Cancer Institute, the National Institutes of Health, and the Veterans Affairs Department need to share sensitive patient information to do their jobs. In addition, private organizations, such as hospitals and outside lab services, typically play important roles as well. Each of these various organizations needs access to certain pieces of patient information, but not other pieces of patient information, such as billing or payment information.

[3] 2018 Office of the National Coordinator (ONC) for Health Information Technology Data Brief

[4] Customer Experience Silos Research Report

The challenge is to be interoperable — providing appropriate access to the information each organization needs and thus creating continuity of care for the patient, all while ensuring security and protecting data privacy. Each organization uses its own system, which requires a separate login and password. Access to specific data and apps should be assigned as needed and revoked as needed, such as when a healthcare individual or organization is no longer involved in a patient's treatment. Managing who has access to what information in each system is a complex, time-consuming challenge that, if mishandled, can introduce security vulnerabilities. If an agency doesn't immediately revoke the access privileges of a doctor or healthcare facility partner that has left the system, for example, patient information can be left exposed and unprotected, creating a potential breach.

In addition to creating potential security vulnerabilities, interoperability problems can result in a fragmented and frustrating digital experience for healthcare agencies and patients when they try to navigate across different systems to retrieve needed information or when they must enter the same information repeatedly.

Solution: Automated Identity and Access Management Enables Efficient Partner Collaboration

A well-designed identity and access management solution that smartly incorporates automation and API capabilities can improve the experiences of health partners and patients and close security gaps without burdening the IT department. Automation can authenticate any individual needing to access records, ensuring that person is who he says he is, and then authorize which specific information can be accessed and how it may be used.

To eliminate multiple logins for partners, healthcare agencies can use single sign-on (SSO), which mimics the same one-login, one-account, one-portal experience they use for patients and employees. An adaptive multi-factor authentication (MFA) solution that integrates with a partners' directory

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

"Identity was one of the biggest hurdles we had to cross, but we also wanted to provide a good experience to QPP users. Okta helped us achieve both those goals." – David Koh, engineer, USDS.

The Centers for Medicare & Medicaid Services (CMS), an agency within the Department of Health and Human Services, administers the nation's major healthcare programs including Medicare, Medicaid, and the Children's Health Insurance Program (CHIP). It also oversees Healthcare.gov and quality standards related to the Health Insurance Portability and Accountability Act (HIPAA), long-term care facilities, and clinical labs.

As part of its shift to a value-based payment model, CMS worked with the U.S. Digital Service (USDS) to build a Quality of Payments Program (QPP) interface. The QPP replaced three government programs, each with its own identity management system. In addition to simplifying and securing access to the appropriate information, CMS wanted a system that ensured that the best healthcare providers received the greatest benefits.

CMS and USDS adopted an API-first approach, connecting to clinical data registries that already contained information on healthcare quality and outcomes. CMS chose Okta to manage identity and access because of its industry leadership and well-documented APIs. Okta API Access Management allows CMS developers to focus on streamlining the provider experience, while Okta securely controls access to the QPP website and API.

Key benefits of the project:

- 15 percent of Medicare claims are now submitted via the Okta-enabled API
- One website and API to gather information about healthcare quality and outcomes
- A modern identity infrastructure, with improved security, reliability and scalability
- A streamlined user experience, delivered on time and within budget.

Read the full story: okta.com/CMS

can close security gaps. This helps ensure that 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 need no longer worry about manually revoking access for partner users because it is done automatically when the partner is removed from its own directory.

Once an individual is authenticated, the next step is authorization. A cancer patient's primary care physician would need access to the information maintained by the NCI on the clinical trial, for example, and would probably also want to be able to upload routine patient information such as blood work. This can be done through an interoperable healthcare API standard called SMART on FHIR (Fast Healthcare Interoperability Resources), which enables different apps to access information appropriately and securely. The SMART on FHIR standard is being adopted by both private industry and the federal government. In fact, the VA recently rolled out a mobile phone health app based on FHIR, which enables veterans to access their own health records in a secure way. The VA plans to make the API available to other partners to deliver similar capabilities.

Challenge: IT Complexity Hinders Productivity

Healthcare organizations employ staff and contractors with varying access needs to resources. Certain employees 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 must go through additional verification for certain procedures. For example, doctors who electronically prescribe controlled substances (EPCS) are required to use MFA to sign prescriptions. On the other hand, employees performing regular business or IT functions should have no access to PHI but may need access to other sensitive data like financial information or technical security details, respectively.

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 it also often results in poor password habits like using the same credentials across multiple accounts for convenience.

With the growth of telemedicine and new care methods, healthcare agency employees also need access to apps no matter where they are located. The challenge for healthcare agencies is ensuring each employee has the right level of access to the apps they need for their job, wherever and whenever they need it. At the same time, organizations must prevent over-provisioning access to unneeded apps to limit security risks.

Adding to this complexity is the task of provisioning network access to new employees, managing and adjusting that access as employees move from role to role, and then removing that access when employees leave the organization. When agencies fail to do this in a timely way, it can pose significant security risks. This is particularly important in healthcare, which is the only industry where more security incidents are caused by internal actors than external actors.[5]

[5] Verizon Protected Health Information Data Breach Report

Solution: Modern Identity Provides Seamless, Secure Employee Experiences

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

SSO provides an easy, user-friendly way for employees to access all the apps they need through a single set of credentials. Assigning users into groups and applying access policies to apps based on their role in the healthcare organization 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 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 enables organizations to onboard new employees at scale.

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.

Okta for Healthcare

Okta provides easy, centralized identity and access management for all key healthcare user groups: patients, partners, and government. 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 in which Okta can help modernize and secure your healthcare organization, visit okta.com/solutions/government.