The Future of Healthcare Depends on Digital Collaboration. Does Your IAM Strategy Support It?

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

info@okta.com
1-888-722-7871

The Future of Healthcare Depends on Digital Collaboration. Does Your IAM Strategy Support It?

The healthcare model in the US is changing. Healthcare demands are increasing as the baby boomer population retires and switches from employer-sponsored healthcare coverage to entitlement programs like Medicare and Medicaid. According to the Census Bureau, "By 2029, when the last round of boomers reaches retirement age, the number of Americans 65 or older will climb to more than 71 million, up from about 41 million in 2011." As demand for healthcare is increasing, supply is decreasing. Available funds for entitlement programs like Medicaid and Medicare are declining. According to the Social Security and Medicare Board of Trustees, Medicare Part A, which helps fund hospital expenses, home services for patients after hospital stays, skilled nursing facilities, and hospice care for elderly and disabled people, will expire in 2028.

The healthcare system in the US is under enormous pressure. More and more medical expenses are being pushed onto healthcare providers, who are already operating with very thin margins today. As their financial burden increases, medical providers are turning to the new way of doing healthcare: the population health model. MACRA (the Medicare Access and CHIP Reauthorization Act) went into effect in April 2015 and is a new model for paying for the treatment of Medicare patients. It's designed to control Medicare spending by financially incentivizing physicians. Under MACRA, doctors are paid in part based on the quality and effectiveness of the care they provide, as opposed to merely the number of patients they see and the number of procedures they do.

At the center of MACRA is effective information exchange between healthcare providers. Medical information today is very dispersed across systems. Because of this, there are a lot of redundancies in the industry. For example, a patient may have recently had an x-ray or a blood test, but unless a physician or hospital has easy access to the results, they may simply order the test a second time. MACRA connects physicians with patient data so they can understand it and act on it without replicating it.

In order for MACRA to be successful, community-wide data needs to be accurately aggregated and analyzed. Healthcare providers need to be able to rely on accurate data from multiple sources. Yet many providers are struggling with how to share data across their partner networks.

Identity and access management is one of the biggest challenges plaguing medical providers as they move to share information with partners. The healthcare industry today is highly fragmented. Most healthcare providers are operating their own applications, their own systems, and their own user store. Collaborating and sharing data with other medical providers means signing in to a new VPN, portal, app or website with a username and password, and an additional set of credentials is a burden to partner users. Often, to easily remember new login information, users will reuse an existing password, thereby increasing the attack surface if they are ever compromised. There is additional IT overhead associated with managing partner-facing systems. And, there is the risk that, when a user at a partner organization leaves, there is no good way for a medical provider to immediately know, and that user may have lingering access to confidential medical information (PHI or PII).

Medical providers are also challenged with how to manage the user lifecycle for partner users. Onboarding new users, provisioning apps to them, regularly updating profile information, recovering passwords, and offboarding are critical and regularly occurring events. If performed manually, they are also very time consuming for IT. B2B partner networks can be large and often have high turnover rates. It can be difficult for medical providers to keep track of and manage all these changes. It's also difficult for IT to know which partner users should have access to what medical information.

Medical providers and their partner organizations also have very diverse needs. No organization is identical. Each likely has different security requirements, access policies, multi-factor authentication solutions, etc. Some providers are small and have no existing identity infrastructure in place, while others have a single sign-on solution and want to federate directly with a medical provider. To be successful, it's critical that medical providers be able to adapt to these different alternatives.

Cloud identity enables medical providers to securely and easily share information with B2B partners.

Cloud identity is a service; it's secure, on-demand, and available everywhere. With cloud identity, medical providers have a centralized view of all users in their partner network, regardless of where they're actually mastered. Cloud identity also gives IT full visibility into the user lifecycle and the ability to quickly and easily make updates or changes to it. With cloud identity, each user has just one account. This enables IT to easily onboard and offboard users, update user profile information, automate provisioning of new apps and control access policies from a single, centralized point. Cloud identity also prevents lingering user access to PHI or PII by immediately deprovisioning users to cut off their access when they leave a partner provider.

Cloud identity eliminates many of the manual processes associated with building out a partner network. Some cloud identity providers offer self-service registration. With this, medical providers can create validation rules that determine who will be allowed to register in their partner network. Partner users can then fill out a templated registration form, register themselves and be granted immediate access to the apps and data they need. Cloud identity also allows medical providers to delegate administration of users to a partner organization. This is critical because, in most cases, partners know their own users best. Delegated administration allows partner IT organizations to set up their own access policies, rules and registration rights for their users. Cloud identity can also allow partners who already have an identity management system in place to use that existing infrastructure and single sign-on into partner applications via federation. In doing so, partner users can have access to the appropriate resources with their own username and password.

Finally, cloud identity provides the flexibility partner organizations require. One size certainly does not fit all with medical providers or their B2B partners. Cloud identity enables partner organizations to use various authentication options. In some instances, users may not have smartphone access and will require SMS codes as second factor authentication. A medical provider needs the flexibility to accommodate this. Cloud identity also provides flexible administration options. Some partners may want to manage their own users, while others may want to federate to the app or portal with their existing identity management solution. And finally, cloud identity provides flexible access policies so that medical providers can tailor user access based on the type of partner they are working with.

Okta uniquely provides the foundation that medical providers need as healthcare moves toward population health. Okta is the foundation for secure connections between people and technology. Okta's Universal Directory (UD) equips medical providers with a centralized repository for all people– be it a partner user or their own. With UD, medical providers can manage access policies, store profile information and manage passwords. With Okta, medical providers can connect to an unlimited number of federated providers, quickly enabling partner end user access to the data and medical information they need. Okta also automates the user lifecycle and allows medical providers to automatically create partner user accounts for new applications and immediately deprovision users when an account is canceled. Okta enables IT to implement strong authentication policies without inhibiting end users by offering a comprehensive set of authentication factors including voice, one-time push, SMS, and the ability to integrate with third-party factors. And, not all users have to use the same factor. Okta is agile and scalable. As information sharing increases in healthcare, Okta can scale to handle it.

Fee-for-service is simply not sustainable for US medical providers in the long term. The shift toward population health and strong B2B collaboration poses significant identity challenges for the medical industry today. Cloud identity solves those challenges by providing a unified view of all users, whether B2B or internal. Cloud identity also eliminates the manual processes of setting up and managing a partner portal, enabling medical providers to offer flexible options to partner organizations.

okta IDENTITY CLOUD
Single Sign-On
Universal Directory
Lifecycle Management
API Access Management
Adaptive Multi-Factor Authentication
Mobility Management
Developer SDKs

The Industry's Most Reliable and Secure Platform, Period.

okta