KPMG

Care anywhere, security everywhere

In healthcare, identity access management is the cornerstone of a seamless customer journey

read.kpmg.us/healthcarelifesciencesinstitutes

Overview

As we prepare to enter the third year of the pandemic, healthcare is at a crossroads. The long-held ideal of allowing secure access to patients' records wherever they seek care is running up against the reality that cybersecurity attacks against healthcare are at an all-time high.

On the one hand, the volume of patients seeking care due to COVID-19 has increased the need for providers to access patients' records across institutional boundaries. Consumers themselves are also demanding more seamless experiences with their providers and health plans and failing to do so could spur them to seek care elsewhere.

On the other hand, cyber-breaches put more than 40 million patient records at risk in 2021,[1] costing the industry more than $6 trillion dollars.[2] The fact that healthcare is a target isn't new news: Personal health information (PHI) is worth as much as $363 per records on the black market, compared to only $1-2 per record for credit card information.[3] However, the problem is growing: Many recent cybersecurity incidents have resulted from the sector's increasing challenges with an unpredictable, varied, and not-entirely-secure supply chain.[4]

Imagine this scenario:

James, a middle-aged man with diabetes, goes to a retail healthcare outlet to have his A1C checked. To compare the patient's current readings to his A1C over time, the onsite nurse practitioner taps into the medical records held at his endocrinologist and internist's offices. From a clinical perspective, using connected systems to foster continuity of care is clearly the key to better outcomes. However, once all these digitized records are on the move, they are ripe for the picking by cyber-criminals who can steal James's medical records to file false insurance claims, obtain medications for their own use or resale, or seek care under his name.

The fallout of such a scenario doesn't only impact patients like James, i.e., victims of identity fraud. Providers' and payers' reputations are also at risk since every breach diminishes the trust patients put in healthcare organizations to ensure their data and records don't fall into the wrong hands.

The solution: Robust identity access management

The trend toward anytime, anywhere healthcare was given a boost during the pandemic. While consumers already expected sharing of records between, for example, their cardiologist and their pulmonologist or their psychiatrist and their internist, the tremendous uptake of both virtual care and retail care has taken interoperability to a whole new level.

Ubiquitous computing requires healthcare organizations to take a new approach to identity and access management (IAM) architecture and operations. Given the many affiliations within the healthcare ecosystem, now is the time to adopt advanced IAM solutions to ensure secure access to applications through adaptive access control, centralized authentication, coarse and fine-grained authorization, and cloud applications and services.

Although hospitals and health systems have been slower to adopt these cybersecurity methods, most recognize the value of aggregating and sharing patient information across institutional boundaries. At the same time, many large payers are already ahead of the curve.

Consider this example:

One of the largest healthcare payers is instituting a cloud-based portal for consumers whose health insurance is provided through either their employers or the marketplace. The organization aims to facilitate an ecosystem where all relevant patient information can be accessed by a patient's stakeholders (i.e. providers, insurers, caregivers) and claims are digitalized so that payments get to the right provider. This payer also has a tremendous B2B client base that uses their pharmacy benefit management and coinsurance services, data-heavy interactions that require secure cross-institutional information sharing.

Advanced customer IAM solutions are enabling the payer to create a centralized platform where all B2B and B2C customers can have a unified experience comprising a simpler process for registration, the ability to see all their claims in detail, and a seamless experience around sign on, multi-factor authentication (MFA), and credential management. For the payer, this effort is part of a larger digital transformation focused on direct-to-consumer services, which will give the company a 360-degree view of each member as well as the opportunity to upsell ancillary services, e.g., wellness programs. mental health support, behavior modification tools, etc.

The company has also realized synergies between its insurance business and the pharmacy benefits management business. From a security perspective, the company can centralize its efforts to mature and improve its digital-security posture — which has been facing headwinds due to an increased threat landscape, a significant rise in data volume, and the complexity of the technology ecosystem. The combined security program will be housed under corporate information protection (CIP), eliminating the need to manage 20 different apps and related security controls. This approach will enable the company to focus on scalability, automation, and digital security.

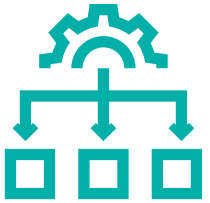
Additional considerations

1 **To orchestrate a better customer experience,** including sharing patient information and medical records across care-delivery points, healthcare organizations need a single portal backed by a robust IAM system that brings together all vertical capabilities and data sources in the background, e.g., Electronic Health Records (EHR), analytics, billing, and payment, and, thereby, streamlines the customer journey. A critical consideration here are built-in cyber controls, such as multi-factor authentication, tokens, and soft tokens so users can log in once and regain access anywhere without signing on again.

2 **To improve outcomes,** hospitals can use an IAM platform and application program interfaces (APIs) to integrate identity into every part of a patient's journey. For example, if a patient enters a hospital for a simple appointment that later escalates into multiple tests, scans, medications, surgery, and post-care appointments, all data will be available to the care teams in an integrated manner instead of in different, disconnected data silos.

3 **To protect patient privacy,** it is critical to use IAM solutions during controlled data-sharing between patients and healthcare providers, particularly when patients use Internet of Things (IoT) devices and wearables to share sensitive health data. Sharing minute-to-minute health data in this way will empower patients to take a more active role in improving their own health outcomes. At the same time, to protect against unauthorized access to patient data, IAM solutions can be used to log and audit user activity, enforce complex passwords, and help the organization transition from shared accounts to individual accounts. It is important to note that healthcare organizations need to transition from pure role-based access control (RBAC) models, which are usually not scalable given the many roles and specializations that need access, to policy-based access control (PBAC), which assigns permissions on a more granular level by defining exactly which actions are allowed for staff members or resources depending on their roles and the context.

4 **To streamline clinical workflows** as value-based care models and digital transformation enable anytime, anywhere care – and an increasingly decentralized workforce erodes a well-defined network perimeter – it is imperative that trusted identities manage processes and systems. Further, in addition to on-prem applications, there is an ever-expanding number of cloud applications, a diverse set of edge devices, and ever-more connected medical services (MIoT) devices, all of which must communicate with each other to provide continuous care.



Getting started

Healthcare organizations interested in upgrading their IAM capabilities need to account for not only technical considerations, but cultural ones as well. That means:

— **A Front-Office** integrated to customer experience and digitally-enabled initiatives led by a digital enablement officer.

— **CISO and Cybersecurity teams** that ensure all solutions incorporate best-of-breed cloud and on-premise software.

— **A Marketing team led by the CMO** that drives digital identity/Customer Identity and Access Management (CIAM) transformation centered around a digital channel for seamlessly up-selling or cross-selling company and third-party services.

— **And a People and Change team** that evangelizes the change so that staff at all levels of the organization understand the value of CIAM when it comes to a streamlined customer journey.

References

1. Kat Jercich, The biggest healthcare data breaches of 2021, Healthcare IT News, November 16, 2021.
2. Recent Healthcare Data Breaches as of September 6, 2021, Chief Healthcare Executive, September 26, 2021.
3. Data Breaches: In the Healthcare Sector, Center for Internet Security.
4. Jessica Davis, 10 biggest healthcare data breaches of 2021 impact over 22.6M patients, SC Media, December 21, 2021.

Why KPMG

KPMG brings extensive delivery experience and well-established success in the payer and provider space with a wide spectrum of value realization to implement a secure, enterprise-wide approach to manage the member, patient, provider, and broker digital identities, improve their experience and develop a more intimate relationship with customers.

This covers the following CIAM areas:

— Strategy

— Vendor evaluation & selection assistance

— Requirements, Architecture and Design

— Implementation and Adoption support

— Sustained Engineering and Operations

Our cross-functional professionals are in sync with the current privacy and regulatory requirements around access to healthcare information which helps in making sure that CIAM solutions being proposed and implemented are aligned with the same.

Further, we are able to support CIAM integration with with leading platforms to include privacy as a complementary service which is very impactful in the customer space.

Companies are collecting all sorts of data on our online activities, whether we are making a purchase, using points from our loyalty program, updating our profile, or just searching areas of interest. Together, this record of data makes up a digital identity.

To instill trust in customers (and to help meet regulatory demands), it is critical that companies thoughtfully and strategically engage customers on consent. KPMG brings together the power of leading privacy platforms to help companies deepen trust with their customers by supporting enhanced transparency, visibility, and customer control of their personal information.

KPMG has a strong track record of helping companies to implement, configure, and redesign supporting processes and operating models leveraging the OneTrust and Okta platforms. As privacy technology evolves into an ecosystem rather than single tool model, KPMG is well poised to help bring together leading industry technologies to help customers elevate trust and impact with their customers.

Contact us

Anurag Rai
Principal, Advisory,
Cyber Security Services
T: 312-665-2563
E: anurag.rai@kpmg.com

Lav Kapoor
Director, Advisory,
Cyber Security Services
T: 973-912-6461
E: lkapoor@kpmg.com

To learn more, please visit:
read.kpmg.us/healthcarelifesciencesinstitutes

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia