ForgeRock®

White Paper

10 IAM Capabilities Key to Support Digital Transformation within Federal Health IT

The need for digital transformation within the federal healthcare industry has skyrocketed due to converging trends:

- Users such as employees, citizens, and patients are demanding remote access and personalized service offerings and experiences.
- High-tech organizations and well-funded startups have entered the market, increasing competition.
- Medical IoT (MIoT) devices and things containing sensitive health data are now ubiquitous, increasing risk.
- Large-scale mergers and acquisitions (M&A) are creating complex, disparate system environments.

Unfortunately, traditional IT environments and legacy identity and access management (IAM) systems are being pushed to their limit by these trends and more. They weren't built to support today's healthcare demands. The result is a latency, frustration, friction, increased risk, and poor user experience — prompting in healthcare leaders like you to ask how to quickly and easily support digital transformation without upending operations or compromising security and user experience.

The following are 10 modern IAM capabilities that can be easily incorporated into your IAM infrastructure to support digital transformation within your federal health organization.

10 IAM Capabilities Key to Support Digital Transformation for the Federal Health Industry

1 Availability and Scale

Demand for digital healthcare access and services within Fed Health IT has exploded within the past year. To keep your organization going and make user experiences fantastic, it is important to ensure that an end user's access and session remains undisrupted should something happen, such as a server going down. Modern IAM platforms should include both service availability and session availability. Service availability ensures that users can access a site when a server goes down. Session availability preserves and keeps a session running if a server goes down.

Modern IAM should also support a variety of scale scenarios. This includes an ever-changing number (often millions) of users, devices, and things, as well as changing frequencies and lengths of simultaneous and concurrent sessions. Additionally, to help maintain healthy services and protect against breaches and distributed-denial-of-service (DDoS) attacks, you should leverage an Identity Gateway to monitor API traffic, throttle traffic volume, and detect anomalies.

Modern IAM platforms should include service availability, session availability, and support a variety of scale scenarios

2 Custom Authentication Journeys

As federal healthcare employees, citizens, patients, customers, or ecosystem partners, we all want fast, frictionless access to apps and services. At the same time, we also want our resources, assets, and sensitive data protected from fraud and cyberthreats. By customizing authentication journeys with factors such as user type, device, and geolocation, as well as using self-service features such as self-registration or password reset, you can reduce friction during the authentication process in order to provide a great user experience. On the flip side, you can also add friction, such as multi-factor authentication, when there's suspicious activity.

Support for Zero Trust/CARTA Security Models

3

It's a sad reality that fraud and cybercrime have persisted and even risen in the wake of current events. Zero Trust/Continuous Adaptive Risk and Trust Assessment (CARTA) security models are based on the idea that no network, individual, thing, or device can be trusted. Modern identity platforms should be able determine whether an entity requesting an action is authorized to do so and if they have proven they are the entity they claim to be with a sufficient level of assurance based on the risk of the specific action. Within these models, every action taken must be properly authenticated and continuously authorized. To do this, authentication and authorization decisions take into consideration a rich set of information by leveraging contextual information and become risk-based rather than binary.

> In the wake of the COVID-19 pandemic, fraud and cybercrime have persisted and even risen

Privacy, Consent, and Regulatory Support

4

To support today's healthcare trends requires that you comply with the various regional regulations (such as the California Consumer Privacy Act [CCPA] and General Data Protection Regulation [GDPR]) that apply to your employee, member, patient, consumer, and partner locations. For global and regional compliance, it's critical that modern IAM platforms enable you to meet regulation and compliance standards. This includes Privacy by Design and Consent mechanisms based on the UMA 2.0 standard, as well as integration with other software that helps meet regulatory requirements.

Equally important, to provide a great experience for your users, you also need to make it easy for them to register, consume, and manage their personal preferences or run the risk that they will leave for a better experience offered by competitors. Modern IAM platforms should include intuitive and user-friendly privacy and control mechanisms that make it easy to register and manage profile and privacy settings.

API Security

5

APIs make today's remote world go round by linking people, systems, and services together, no matter where they are. As detailed by KuppingerCole in their API Security Leadership Compass report and Modern Identity Fabrics research paper, API security is a linchpin of modern identity and access management strategy.

With identity-enabled APIs, you can:

- Meet member, patient, partner, and consumer expectations by delivering seamless, omnichannel experiences
- Create value-added services through partnerships and third-party integrations
- Bridge legacy systems with modern applications
- Aggregate internal and third-party user data into a single view

To secure APIs requires a standards-based, modern IAM platform capable of exposing rich APIs for seamless integration, deployment agility, and continuous delivery. Modern IAM platforms also leverage a gateway to secure APIs and users by enforcing authorization for any type of traffic. You can also monitor API traffic, throttle traffic volume, and detect anomalies.

KuppingerCole names ForgeRock "Overall Leader" in all categories for API Security

Support for Bring Your Own Device (BYOD)

6

Remote healthcare employees often need to use their own devices to do their work. Supporting BYOD models requires modern access management. Just as with custom authentication discussed above, with modern access management capabilities, organizations can easily define different user journeys for access by device. This is done by capturing device-specific context such as IP address, localization, browser agent, and device characteristics. You can also store, with the user's consent, a cookie in their browser to help identify them when they return. By capturing this rich data set and then using it to make runtime access decisions, federal healthcare organizations can configure flexible yet secure journeys that prompts the user to authenticate, re-authenticate with a second factor, or completely deny access when appropriate.

A Unified Experience Through a Single View of the User

7

Within today's Federal Health IT landscape, poor user experiences can become deal breakers. From an IAM perspective, a disjointed view of a user is often to blame. Most users (patients, members, consumers, partners, employees) interact with an organization across many different channels (ie. applications and systems for things like telemedicine, HR, marketing, accounts payable, and so on). There may be user data integration between some channels, but on the whole across an organization, each channel and its data about a user are siloed. This presents difficulties in fully understanding a user from a 360-degree view. This includes knowing all their access rights, preferences, usage, potential risks, and more. Unfortunately, legacy IAM cannot bridge the siloes to help solve the puzzle.

In order to gain a complete picture of your users and how they interact with your organization, modern identity and access management (IAM) uses identity management and directory services products to synchronize, migrate, and manage identity data across your organization's system environment.

With a single view of a user, you're then able to:

- Consolidate user identities and increase their security with behavioral, contextual, and risk-based authentication and authorization policies
- Standardize and unify the user experience across any device (omnichannel)
- Continuously gather information about users in a streamlined, non-intrusive way (progressive profiling)
- Increase user acquisition and retention with easy registration (social registration) and exceptional, personalized experiences
- Conduct analytics on profiled user bases to better understand users and risks

With ForgeRock, Availity supports 12 billion transactions per year, over 800,000 daily logins, and connects two million providers to healthcare plans through the U.S.

Read the case study

AI and ML Powered Identity and Governance

8

Today, many healthcare organizations are unexpectedly supporting their entire workforce remotely. This increase is likely challenging their current employee IAM systems, as well as the IT staff, administrators, and managers who have to ensure that the right people have the right to access the right systems and applications while working from home. Additionally, the risk of breaches, hacks, fraud, and other malicious activity also increases with the sudden increase of remote employees. All of this is a problem to be solved.

Identity Governance and Administration (IGA) helps you manage and provision user access, as well as reduce the risk that comes with employees having excessive or unnecessary access to applications, systems, and data. Machine learning (ML) and artificial intelligence (AI) take IGA to the next level by automating the most common activities. This includes automatically approving access requests, performing certifications, and predicting what access should be provisioned to users. All-inclusive modern IAM platforms that offer identity and IGA powered by AI and ML increase efficiency and provide more time for IT staff and access approvers to focus on access rights that have been identified as risky or anomalous. The result is improved security and reduced administrative burden.

DevOps Friendly Architecture

9

Time is of the essence when it comes to developing and deploying capabilities that support healthcare digital transformation and innovation. One of the best ways to improve time to value is to adopt a DevOps model.

DevOps enables software development and deployment cycles to run continuously, so you can roll out new apps, services, and capabilities faster by reducing time to production. Because of the efficacy and rapid adoption of DevOps, future-minded IAM platforms support DevOps deployment with containerisation and orchestration technologies such as Docker and Kubernetes.

DevOps-friendly IAM platforms help you roll out new apps, services, and capabilities faster

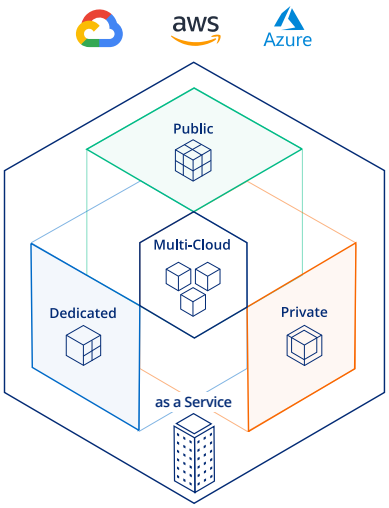
Flexible Cloud Options to Consume or Deploy

10

Today, getting modern IAM capabilities that securely and quickly support federal healthcare digital transformation is important. Traditional, legacy IAM deployment and maintenance is often lengthy, costly, and complex, requiring numerous resource hours and slowing time-to-market. Further, legacy IAM solutions can be very difficult to modify in order to meet new needs, trends, and demands. On the flip side, consuming or deploying modern IAM in the cloud accelerates time-to-market, increases flexibility, availability, and scalability, and saves resource time.

By deploying modern IAM platform in a cloud environment (private, public, hybrid cloud, multi-cloud) or consuming it as a service (IDaaS), you can easily move your existing workloads and and get up and running within minutes without sacrificing rich features and extensibility. Further, with a full-suite identity platform as a service, you also get the benefit of offloading maintenance to the provider, as well as the big advantage of always being on the latest version.

Importantly, IAM providers that offer a comprehensive identity cloud platform with feature parity to their software platform give you the invaluable flexibility to easily shift your IAM environments according to your business needs with minimal disruption.



The ForgeRock Identity Platform: Deploy in the Cloud or Consume as a Service

Connect Everyone, Anywhere With ForgeRock

Identified as an Access Management and Federation Overall Leader and the Overall Leader in all categories for Identity API Platforms by KuppingerCole, as well as one of the most visionary access management providers by Gartner, the ForgeRock Identity Platform easily connects everyone, anywhere by supporting today's federal healthcare industry requirements at scale without sacrificing experience and security.

> "Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations."
>
> – KuppingerCole

ForgeRock helps people safely and simply access the connected world by enabling exceptional digital experiences, no-compromise security, and comprehensive functionality at any scale. The ForgeRock Identity Platform consists of Identity Management, Identity Governance and Administration, Autonomous Identity, Access Management, User-Managed Access, Directory Services, Edge Security, and an Identity Gateway. The platform is delivered as-a-service and with push-button deployments to any cloud or any data center.

Meet Modern Identity Requirements Without Ripping and Replacing Legacy IAM

Today, time is of the essence. Unlike most IAM providers, with ForgeRock you don't need to suffer the pain, risk, and expense of ripping out existing legacy identity solutions to get the features and benefits of IAM modernization needed to support your Health IT operations at scale.

ForgeRock provides a flexible approach that enables you to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems like CA Single Sign-On (SiteMinder), Oracle, IBM and even homegrown identity systems.

ForgeRock provides a flexible approach that enables you to augment first, then coexist to later consolidate or retire disparate, legacy identity management systems

We're Here and Ready To Help. Contact Us to Get Started

Federal Healthcare digital transformation leaders use ForgeRock to improve outcomes, grow their business and competitive advantage, increase productivity, and improve security, privacy, and compliance while reducing costs. Contact us to learn more about how ForgeRock can help you.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit www.forgerock.com or follow ForgeRock on social media.

Follow Us

ForgeRock