ForgeRock®

WHITEPAPER

A Better Identity Cloud for Healthcare

Do IAM SaaS Better with a Patented Security Architecture, HIPAA Compliance, and Enterprise-Grade Capabilities

Table of Contents

Over the past decade, technological advances have drastically improved healthcare. The healthcare ecosystem is no longer confined to the doctor's office, clinic, or hospital. Today, digital health technologies power **connected healthcare ecosystems** that have transformed care and served as a lifeline during the global pandemic lockdowns.

Healthcare is now delivered through ecosystems based on a network of front- and back-office systems, internet of medical things (IoMT), independent healthcare software, third-party application programming interfaces (APIs), and identity and access management (IAM) and identity governance and administration (IGA) systems. Digital health ecosystems have also formed that extend beyond a single organization's perimeters. These ecosystems support dynamic partnerships between providers, payers, life sciences, pharmaceutical, medical device, and retail organizations.

> "In the health ecosystem of the future, touchpoints, technologies, and capabilities would be interconnected via open platforms/application programming interfaces (APIs) and seamlessly packaged and delivered to consumers in their preferred manner of engagement."[1]
>
> Deloitte

Through digital healthcare ecosystems, quality healthcare can be integrated into the consumer's (patient's, member's) daily life. They provide digital options for first-line care and enable a constantly accessible touchpoint between patients and their providers and payers. Digital health ecosystems also facilitate the transition from episodic care to a continuum of care that drives preventative action and helps people use fewer care services by encouraging them to have healthier lifestyles. All of this helps to reduce the cost of services.

To participate in digital healthcare ecosystems, internal and external users, IoMT, devices, sessions, and services must be seamlessly connected and secured. Privacy and consent regulations – such as the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA) – in addition to the 21st Century Cures Act must also be supported and followed.

Security is non-negotiable for healthcare organizations and their digital ecosystems. According to the **ForgeRock 2021 Breach Report**, healthcare was the biggest target for the third year in a row, accounting for 34% of the total number of breaches. It was also the most costly at $474 per record.

Meeting the requirements above is no easy task. Many healthcare organizations are blocked from accomplishing them due to the shortfalls of their homegrown and legacy identity and access management (IAM) solutions. These solutions are unable to address the needs of a modern digital ecosystem simply due to the fact that they were not built to do so.

Healthcare Turns to the Cloud

From innovation and care outcomes, to security and cost efficiency, the success of a digital health ecosystem relies on the robustness and readiness of digital identity systems. To help to speed their ecosystem innovation, increase scalability and flexibility, and reduce costs and the burdens on their already strapped IT resources, healthcare organizations are now looking at SaaS options for IAM.

> Managing infrastructure and data centers have become responsibilities these [healthcare] CIOs wish to shed in favor of choosing and integrating cloud software that solves business problems and expands new business.
>
> Gartner[2]

[1] https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-the-digital-imperative.pdf
[2] https://www.gartner.com/en/documents/3980260/best-practices-for-building-healthcare-solutions-with-hy

The market for cloud services within the healthcare sector is steadily increasing. According to Mordor Intelligence[3], "The healthcare cloud computing market was valued at USD $23,749.33 million in 2020, and it is expected to reach USD $52,303.35 million by 2026, registering a CAGR of 14.12% during the forecast period of 2021-2026."

With all of the benefits of the cloud, it's no surprise that healthcare organizations are making the transition. Yet while cloud-based solutions help modernize and bring agility to the healthcare IT landscape, not all of them are alike.

The Shortcomings of Many Identity SaaS Solutions

Many early cloud-only IAM solutions focused primarily on simplicity at the expense of functionality and configurability. This narrow focus allowed them to quickly gain market share within a narrow band of organizations that had simple needs.

Today's healthcare organizations are demanding more capabilities than simple cloud-only IAM solutions can deliver. These include enterprise-grade security and configurability.

In a 2021 Forrester study, nearly all (98%) of the early adopters of cloud-only IAM solutions cited challenges that include:

- Failure to integrate with existing business processes
- Inability to manage identities across current applications and systems
- Lack of visibility into on-premises systems, which results in an incomplete picture of risk and security posture

The most consistent hurdle respondents face is the inability to map or integrate to existing processes or legacy solutions. In healthcare, business processes and identity integrations vary widely across applications. Each supports different standards and protocols. And this introduces complexity for any solution that does not support the required standards or does not offer flexibility and extensibility to adapt to business needs.

98%

of cloud-only IAM solution early adopters cited challenges.

Forrester[4]

As mentioned, some IAM providers simplify their offerings by omitting the extensibility needed by many large organizations. This results in solutions that cannot integrate seamlessly with legacy and modern applications or adapt to the business processes of large healthcare organizations.

Cloud Without Compromise

Today's healthcare IAM requirements exceed the capabilities provided by many cloud-based IAM offerings – especially those that focus on limited use cases with unpredictable costs. A modern identity solution is foundational to providing secure, simple, and innovative healthcare solutions in a complex digital ecosystem. Modern IAM should support a secure, unified digital ecosystem that streamlines care, lowers costs, and enables better outcomes.

The ideal IAM SaaS platform has extensible integration with systems and support for APIs, microservices, and IoMT devices. It delivers advanced capabilities to support innovation; no-code and low-code orchestration for onboarding; self-service and passwordless authentication; and advanced authorization policies. To reduce costs and align with budgetary constraints, the identity provider should offer simple and flexible subscriptions with predictable pricing.

[3] https://www.mordorintelligence.com/industry-reports/global-healthcare-cloud-computing-market-industry
[4] https://www.forgerock.com/resources/analyst-reports/forrester-study-hybrid-cloud-iam

Do Cloud Better with ForgeRock

ForgeRock Identity Cloud offers cloud-based IAM without compromise. With one subscription, your healthcare organization can have complete freedom to fulfill all your digital ecosystem needs.

ForgeRock Identity Cloud is a **HIPAA-compliant**, comprehensive identity platform delivered as a service. It addresses the challenges of today and tomorrow with essential tools to secure your organization and your workforce, support digital health ecosystems, and innovate personalized customer experiences that will differentiate your business.

With ForgeRock Identity Cloud, your healthcare organization can:

1. **Deliver superior experiences,** mitigate risk, and reduce costs with a comprehensive identity platform.
2. **Gain cutting-edge identity capabilities** without worrying about maintenance, patching, and upgrading.
3. **Increase productivity** by leveraging a single platform for all identity and access needs: users, devices, things, APIs, services, and more.
4. **Leverage a patented security architecture** with data isolation that gives you total control.
5. **Quickly innovate and grow the business** now and into the future without costly overage charges.
6. **Rely on predictable pricing** with overage protection.

Cloud Security Built for Enterprise Healthcare Organizations

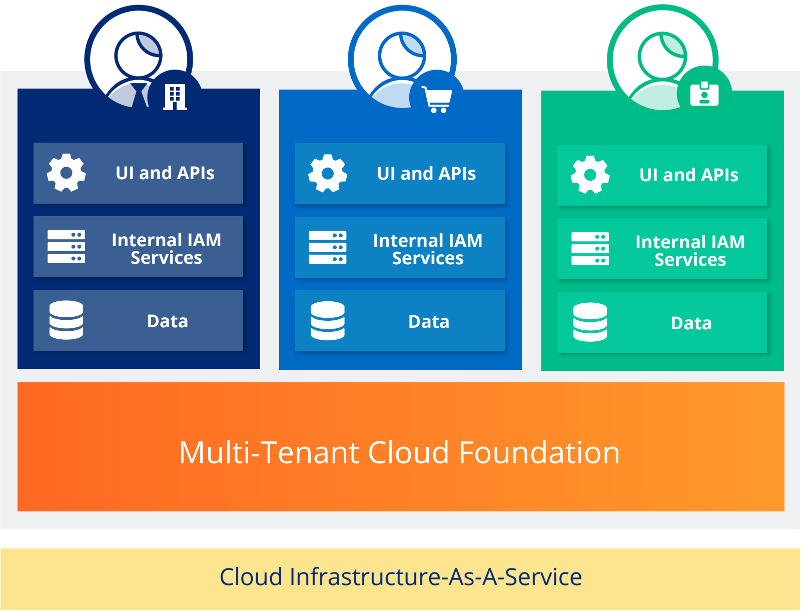
Security concerns – including data sharing and data sovereignty – are among the major reasons many large healthcare organizations have shied away from moving to a complete cloud IAM platform. ForgeRock Identity Cloud allays those concerns by providing maximum security with complete customer isolation in a modern, multi-tenant cloud architecture.

ForgeRock Identity Cloud is the only identity platform delivered as a service that offers full tenant isolation. This means your data and workloads are never commingled with others. ForgeRock eliminates common challenges related to scaling and storing sensitive and regulated identity data in the cloud.

ForgeRock Identity Cloud provides you with:

- Total control with data isolation
- Data sovereignty and compliance
- Maximum availability with individual backups

The Cloud Architecture That Gives You More



Give Your Security Teams Peace of Mind

Many SaaS vendors combine multiple customers (tenants) into a single instance. This outmoded approach to multi-tenancy results in elevated risk because one customer's activities could impact other customers. ForgeRock does cloud differently. ForgeRock's cloud-native architecture with application containerization and Kubernetes cluster orchestration delivers next-generation, high-availability SaaS without impacting performance.

ForgeRock Identity Cloud provides:

- Geographic redundancy of components for maximum availability
- Dedicated customer backups for quick recovery
- Limited incident impact with all data-at-rest encrypted with distinct keys
- Regional isolation of customer data to comply with sovereignty mandates

Share Security, Not Data

Security starts with the fundamentals: secure coding practices, dependency management, least privilege access, and continuous vulnerability and penetration testing. ForgeRock Identity Cloud is built with these fundamentals in mind. And it is constantly updated and refreshed to keep pace with the evolving threat landscape and your demands as a healthcare organization.

With ForgeRock Identity Cloud, you get:

- Physical and network security to prevent common threats like distributed denial-of-service (DDoS) attacks
- Dedicated trust zones to prevent any accidental or malicious commingling of data
- Continuous monitoring by highly trained ForgeRock experts using NIST 800-137 as a guide
- Continuous vulnerability and penetration testing to stay ahead of bad actors
- A layered security approach to mitigate a single point of failure

Leverage the Combined Power of ForgeRock and Google Cloud

Built on the Google Cloud Platform (GCP), the ForgeRock Identity Cloud uses GCP-native network security features to prevent denial-of-service (DoS) attacks against customer environments or services, blocking traffic from specific geographic locations. Network communications are strictly controlled using Kubernetes network policies. At the service level, customer data is stored within a customer environment comprising a dedicated trust zone that shares no code, data, or identities with other customers' environments. At the physical level, GCP provides encryption of data at rest, so all data is encrypted when written to a hard drive and decrypted when read.

Eliminate Accidental or Malicious Data Access

ForgeRock Identity Cloud delivers enterprise-grade security. Its architecture leverages application containerization and Kubernetes cluster orchestration to run a dedicated copy of the service code. Along with other cloud-native features, you benefit from next-generation high availability without compromising performance. With no central database of tenant data that can be compromised, you can keep your healthcare customers' information safe and secure.

Prevent Unintended Loss of Data

ForgeRock Identity Cloud provides a high-availability architecture with transparent failover to meet strict service level agreement (SLA) requirements. It includes an additional layer of capabilities with tenant-specific backup and restore. This feature, unique to ForgeRock Identity Cloud, enables your healthcare organization to recover quickly and efficiently from any accidental or malicious data corruption issues.

Never Be Out of Date

The ForgeRock Identity Cloud makes it much easier to stay current with patches and versioning. With our Continuous Integration/Continuous Deployment (CI/CD), you can be assured that you are always protected with the latest, patched version. In keeping with the 'assumed breach mindset', technologies and processes for quickly detecting, mitigating, and recovering from attacks are integrated into the service design and operation. ForgeRock also operates a continuous monitoring program that detects potential security issues and alerts when appropriate.

Achieve Regulatory Compliance

With ForgeRock, all your identity data and configurations, including backups, are always under your control and in the region of your choice. Each customer environment is separate and self-sufficient, so users cannot access data or resources in any other environment. This helps you satisfy regulatory and compliance requirements quickly and efficiently.

ForgeRock Identity Cloud is **HIPAA compliant**. ForgeRock also supports numerous standards, including the FHIR standard to meet data portability requirements under the 21st Century Cures Act.

Partner with a Healthcare Identity Leader

ForgeRock invests significantly in the healthcare sector to drive innovation. Key ForgeRock leadership roles and contributions include:

- Founder of the OpenID Foundation Health Relationship Trust (HEART) Working Group
- Founder and leadership of the User-Managed Access (UMA) standard
- Technical expert for U.S. Office of the National Coordinator (ONC) of Health IT, commenting on matters such as health IT priorities and API security and privacy

Recognized as a Leader by All Top Analysts

ForgeRock is a global digital identity leader. We support today's demands and are defining the future of identity.

ForgeRock is a "Leader" in:

- **Forrester Wave™** for Customer Identity and Access Management
- **Gartner Magic Quadrant** for Access Management

ForgeRock scored highest for external identities, and second for all other use cases in:

- **Gartner Critical Capabilities** for Access Management

ForgeRock is also the "Overall Leader" in the following KuppingerCole Leadership Compass reports:

- Access Management and Federation
- Customer Identity and Access Management
- Identity Fabrics
- API Identity Platforms
- Adaptive Authentication

Learn More About How ForgeRock Can Help Your Organization

Digital health ecosystems require a flexible, comprehensive identity SaaS solution.
Contact us to learn how ForgeRock can help you achieve your digital healthcare goals.

About ForgeRock

Follow Us

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that 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 1300 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 headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com**.

ForgeRock