ForgeRock

CIAM

How to Compare Digital Identity Management Platforms for CIAM Within the Healthcare Payer Industry

A Workbook

Healthcare is being rapidly reshaped by the six digital transformation trends described below. Though this reshaping is happening worldwide, it is seen most dramatically in the US where healthcare impacts 17.9% of GDP[1] and is the nation's largest employer[2].

- **The Disruptive Economy:** Digital transformation, consumerism and healthcare reform have created a high-stakes game to capture and retain patient relationships. Patients also now demand new channels of digital care delivery that surprise and delight in order to keep their loyalty. Additionally, the shift to Cloud technology is enabling the rapid creation and delivery of innovative new services.

1 https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/nationalhealthaccountshistorical.html
2 https://www.beckershospitalreview.com/workforce/healthcare-becomes-largest-us-employer-6-takeaways.html

- **Cybercrime Targets Patient Data:** Attack sophistication and the number of data breaches, hacks, and ransomware threats have skyrocketed —with no sign of relenting.
- **Changing Regulatory Environment:** Regulators have raised the bar on HIPAA while additional privacy regulations are set to sweep through healthcare. Compliance is now a continual challenge.
- **Patient Trust and Consent:** Patients, as consumers, now demand consent and control over their personal health data, and a voice in where and how it can be shared.
- **Connected Medical Devices and IoT:** By 2020 there will be 25 billion connected 'things'. Unfortunately, many are not secure — a direct threat to patient safety.
- **New Delivery Models and Players:** Care has shifted from 'episodic' towards 'managing population health' — demanding new integrated business relationships. Cooperation between providers, payers, and patients is the new norm while massive new players like Apple, Google, and Amazon are set to jump in.

Within the industry, technology innovation largely determines new market winners. Because of this, health plan business leaders must carefully evaluate digital identity management platforms for customer identity and access management (CIAM) to meet both today and tomorrow's requirements.

How to Use This Workbook

As part of the ForgeRock Ultimate Guide to Digital Identity Management for Customer Identity and Access Management Use Cases, this workbook follows two papers detailing the six digital transformation trends and the components needed for CIAM, as well as future-forecasted use cases.

Use this workbook to compare digital identity management providers specifically for the healthcare payer industry by copying the RFP question tables and filling in the blank answer boxes provided. ForgeRock answers are included within this workbook.

CIAM Questions to Ask Digital Identity Management Providers for the Healthcare Payer Industry

Provider:

Question	Reason This Is Important To Ask	Answer
Does your solution enable the management of rights and data between dependent patients and responsible parties? Adults and children? Power of Attorney (POA) holders?	Family relationships are colliding with privacy regulations, and we need granular capabilities to address the complexities we see with cases such as children aging out of the default of someone having rights to their data, or elderly people signing over POA and responsibility.	
How does your solution solve consent management needs of applications integrated with the solution?	Centrally managing consent is essential to meeting HIPAA standards, providing ease-of-use and securing the identities of each patient and family member accessing sensitive information.	
How does your solution propose to solve identity proofing?	Identity fraud is a particular challenge in the healthcare industry. Also, many patients have been through the registration process multiple times, as a guest, shopping for a specialist, or as a registered patient booking an appointment or getting information on their own EMR. Getting a single-view of an identity, while securing each identity is paramount to a frictionless patient experience.	
Is your product compliant with healthcare regulations (e.g. HIPAA, etc)?	Knowing you are pursuing a solution which meets the regulatory compliance requirements of today and will be committed to be ahead of the curve for tomorrow is important.	
Does the solution enable consumers or active members to opt in for additional security, such as a multi-factor authentication (MFA) method?	Users should have the flexibility in accessing accounts under different situations and add security according to each account holder's needs and device type availability (wearables, digital mobile cards, etc).	
Does the system support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, facial recognition, etc.? Please elaborate.	On-premises and cloud deployment options are essential to any best of breed solution. One size does not fit all and governments need options to support all of their legacy systems and environments, as well as those currently in the cloud and planned to be in the cloud.	
Does the system support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, facial recognition, etc.? Please elaborate.	Members and patients should be able to use passwordless login methods to quickly engage with services or applications.	
Does your solution support usage analytics?	Usage analytics enables admins to monitor and track performance in order to improve services.	

Question	Reason This Is Important To Ask	Answer
Does your solution enable admins to configure multi-factor authentication (MFA) settings based on pre-defined high-risk behavior?	In the event of a high-risk behavior, admins should be able to challenge the login with additional authentication without compromising the member online experience.	
Does your solution have the ability to enforce multifactor authentication (MFA) based on the context of the authentication request, such as source IP address?	Contextual factors, such as a user's IP address or location can change throughout the day. MFA, or step-authentication, adds friction to the user journey only when a risk is posed.	
Does the system have the ability to trigger different workflows based on the role a user selects during registration?	Different types of users may need to go through different workflow processes during authentication and authorization, such as an existing member that has already provided certain types of information versus a new member or guest that would follow a different workflow as a "new enrollee" or as a "guest".	
Does the solution support registration of new accounts, or associate existing accounts to other social networks? Please describe the features that the system provides by such linking, such as authentication.	Users should be able to use other forms of identification to log in other than their username and password, as well as knowledge-based authentication (KBA) to reduce help desk requests.	
Does your solution have the ability to progressively collect user information as users interact with your system over multiple interactions, such as collecting email, name, and password during registration, and then later requesting subscription interests? For example, "Would you be interested in more information?"	Users should be able to quickly onboard without going through lengthy forms and only be asked relevant questions at appropriate stages in their journey.	
Does the solution have the ability to progressively collect user information as users interact with your system over multiple interactions, such as collecting email, name, and password during registration, and later requesting subscription interests (such as "Would you be interested in more information?")	Users should be able to quickly onboard without going through lengthy forms and should be asked relevant questions at appropriate stages in their journey. Progressive profiling allows organizations to collect more information from users based on configurable triggers, by using simple, automated forms that progressively gather information over time.	
Does the solution support a consent framework? To what degree is the consent control fine grained?	Health plan members should have fine-grained control over who has access to which parts of their personal data, along with the ability to immediately revoke any access, review the history of how their data was shared, and manage communication preferences.	
Does the system have the ability to store complex relationships that include many to many mappings?	Health plans manage complex health relationships between family members and their various providers — who are often in care teams with different roles. These various roles, such as member, dependant member, provider, and even employer, have significant implications for the way Identity is managed and how access to information is granted.	

Question	Reason This Is Important To Ask	Answer
Does the solution support identity-enabling legacy applications that do not support current Identity/Federation standards without modifying the underlying application?	Healthcare organizations typically have many legacy applications that have no knowledge of current Identity and Federation standards and protocols. Many health plans have legacy applications; such as for enrollment, eligibility, claims, and many others. These applications are typically very difficult if not impossible to upgrade, but they still need to be supported for an extended period of time. The Identity solution should allow for supporting current Identity Standards for access to these legacy applications.	
How is your organization contributing to thought leadership in the healthcare space?	A digital identity vendor who is invested in the healthcare space will continue to innovate and support such organizations now and going forward.	

Provider: ForgeRock

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution enable the management of rights and data between dependent members and responsible parties? Delegated access? Adults and children? Power of Attorney (POA) holders	Family relationships are colliding with privacy regulations, and we need granular capabilities to address the complexities we see with cases such as children aging out of the default of someone having rights to their data or elderly people signing over POA and responsibility.	Yes, the ForgeRock Platform is designed to model relationships and apply privacy and security choices based upon them. Whether someone is a legally entitled parent or POA, a dependent, or an aging person who needs care, ForgeRock's solution provides for secure and yet frictionless consent to POA's and other family members indefinitely or for a finite amount of time. This allows such persons to address a specific medical decision on behalf of a dependent member -- or for any member or their covered family providing consent to have their health or other data attributes reviewed. ForgeRock also recognizes the identity of devices and can inject patient identity into a data stream, ensuring clinicians are aware of the actual device from which a reading was taken. This helps to connect a patient to a device(s) for data transparency and clarity.
How does the solution solve consent management needs of applications inte-grated with the solution?	Centrally managing consent is essential to meeting HIPAA standards, providing ease-of-use, and securing the identities of each member and dependant family member accessing sensitive information.	The ForgeRock Identity Platform is the first identity management platform available to support User-Managed Access (UMA) for member consent and data sharing. The ForgeRock out-of-the-box user interface for the central sharing management console offers value-add features such as: 1) share buttons so that end-users can choose to delegate selective access to IoT devices, online identity data, and other digital resources, and 2) pending-request pages so that end-users can selectively approve access requests made to those resources.

Question	Reason This Is Important To Ask	ForgeRock Answer
How does the solution propose to solve identity proofing?	Identity fraud is a particular challenge in the healthcare industry. Also, many members have been through the registration process multiple times — as a guest, shopping for a provider or specialist, or as a registered patient booking an appointment or getting information on their own health history, payments, or claims. Getting a single-view of an identity while securing each identity is paramount to a frictionless member experience.	ForgeRock easily facilitates identity proofing to ensure member identity right from initial enrollment. For example, the solution can prompt the customer to enter details about an existing insurance policy (policy number, approximate renewal date, postcode) and validate those details against an existing policy database before continuing the registration flow. ForgeRock can also integrate with third-party identity proofing services during registration or sign on via open standards. Identity proofing can be implemented in a fashion unique to the organization and may involve multiple stages, such as an automated call out to external proofing services followed by manual tasks to allow the user to present physical documentation (such as a photograph of a driver's license) to be examined by a member of staff. Daon and Callsign are among the strong authentication vendors that have developed authentication modules for use with the ForgeRock Identity Platform which can be utilized for identity proofing purposes.
Is the product compliant with healthcare regulations such as HIPAA, etc?	Knowing you are pursuing a solution which meets the regulatory compliance requirements of today and will be committed to be ahead of the curve for tomorrow is important.	Yes, ForgeRock provides several capabilities that help protect Personally Identifiable Information (PII) and other sensitive data per both PCI and HIPAA, including data isolation across geographies, strong encryption, and privacy protection through access control.
Does the solution enable consumers or active members to opt in for additional security, such as a multi-factor authentication (MFA) method?	Members should have flexibility in accessing accounts under different situations and add security according to diverse needs and device type availability (wearables, digital mobile cards, etc).	Yes. ForgeRock's philosophy has always been that static, monolithic (multi-factor authentication) MFA was never enough to meet both the security and agility needs of an organization. We have gone above and beyond to future proof for new factors or biometrics that have yet to be created. We do this through Intelligent Access which provides improved end user choices. For example, members want much more control over how they are identified, which device they use, which MFA option they want to use, and when they want to use it. If one MFA factor is compromised, an organization can simply pivot to a new MFA method with Intelligent Access by switching nodes in the tree-like decisioning structure.
Does the system support biometric authentication or biometric-involved authentication, such as fingerprint readers, TouchID, facial recognition, etc.? Please elaborate.	Members and patients should be able to use passwordless login methods to quickly engage with services or applications.	The ForgeRock Identity Platform supports Touch ID using the fingerprint scanner on a phone in combination with push authentication. The ForgeRock Identity Platform architecture allows for integration of biometrics-based authenticators through open standards and APIs, leveraging standard protocols such as OpenID Connect and SAML, or leveraging API-based integration via a scriptable authentication node. By providing an extensibility framework, the ForgeRock Identity Platform can integrate with various biometric authenticators, including FIDO compliant authenticators. Integration of third-party authentication technologies, such as biometric readers, can be achieved through documented integration points. For light-touch integration, a scripted authentication node might be suitable, whereas for close integration, a full authentication node may be more appropriate.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the solution support usage analytics?	Usages analytics enable admins to monitor and track performance in order to improve services.	The ForgeRock Identity Platform provides a variety of standard mechanisms for monitoring and alerting in its products. ForgeRock monitoring is designed to allow alerting on the availability and system characteristics of the various platform components, and also on the performance and events that occur for specific functions. Examples could be high CPU, low memory, and failed critical transactions. The ForgeRock Identity Platform uses Dropwizard's Metrics as its common metrics framework for adding monitoring capabilities to an application. Additionally, third-party monitoring frameworks such as Prometheus can be used to monitor published metrics over REST, and can then be extended further by using tools such as Graphite for data storage and Grafana for visualization. All products in the ForgeRock Identity Platform also share a common audit log service and are commonly consumed by third-party SIEM and analytics solutions, such as FireEye®, Guardian Analytics®, Logstash and Splunk.
Does your solution enable admins to configure multi-factor authentication (MFA) settings based on pre-defined high-risk behavior?	In the event of a high-risk behavior, admins should be able to challenge the login with additional authentication without compromising the member online experience.	Yes. By leveraging adaptive security intelligence, administrators can strike the right balance between security and choice to deliver a more secure and meaningful experience across all digital touch-points. ForgeRock Intelligent Access is based on a powerful decision tree framework that enables you to: › Easily configure, measure, and adjust login journeys using device, contextual, behavioral, patient choice, analytics, and risk-based factors. › Integrate with cyber security solutions with an intuitive drag-and-drop interface. › Leverage user login analytics to increase user adoption rates, and improve the patient experience. › Automatically redirect suspicious users for further monitoring.
Does your solution have the ability to enforce multifactor authentication (MFA) based on the context of the authentication request, such as source IP address?	Contextual factors, such as a user's IP address or location can change throughout the day. MFA, or step-authentication, adds friction to the user journey only when a risk is posed.	Yes. ForgeRock has introduced ForgeRock Intelligent Access, an intelligent tree-like decisioning framework to authenticate users. It is no longer sufficient to use one or two-factors for authentication, additional signals such as context (IP Address, operating system, browser, device, time of day), behavior (does the member or provider normally log in at this hour, is the location familiar), and risk-based factors (is the user accessing sensitive data) must also be considered. Authentication trees provide a powerful platform for modelling the authentication journey using authentication nodes to detect these digital signals. Intelligence can be built into the tree to direct the journey, gathering information along the way. This information is not only used to determine risk, but to inform downstream apps of the accumulated knowledge gained during the authentication journey.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the system have the ability to trigger different workflows based on the role a user selects during registration?	Different types of users may need to go through different workflow processes during authentication and authorization, such as an existing member that has already provided certain types of information versus a new member or guest that would follow a different workflow as a "new patient" or as a "guest".	Yes. The ForgeRock Identity Platform allows the capability to call to different registration workflows based upon details such as user type and what data already exists for a user, if any.
Does the solution support registration of new accounts, or associate existing accounts to other social networks? Please describe the features that the system provides by such linking, such as authentication.	Users should be able to use other forms of identification to log in other than their username and password, as well as knowledge-based authentication (KBA) to reduce help desk requests.	Yes. The ForgeRock Identity Platform includes a comprehensive user self-service capability which includes self-registration. This allows users to easily and securely sign up to the service. Additional security features can also be added to the process, including email verification, knowledge-based authentication (KBA), Google reCAPTCHA, social registration, and custom plugin. Once a new user has registered, an account is normally created in a user data store, allowing them to immediately log in. In addition, ForgeRock Identity Management can trigger the provision of accounts in any other related data stores, trigger workflows for more complex tasks, or even initiate an approval process.
Does the solution have the ability to progressively collect user information as users interact with your system over multiple interactions, such as collecting email, name, and password during registration, and later requesting subscription interests (such as "Would you be interested in more information?")	Users should be able to quickly onboard without going through lengthy forms and should be asked relevant questions at appropriate stages in their journey. Progressive profiling allows organizations to collect more information from users based on configurable triggers, by using simple, automated forms that progressively gather information over time.	The ForgeRock Identity Platform includes a progressive profiling capability with configurable triggers, such as 'Time since user creation', 'Number of logins for the user', and 'Value of a profile property'. The number of progressive profiling triggers is unlimited and the data collected at each trigger point is completely configurable. Progressive profiling triggers are typically fired when a user attempts to log in. The ForgeRock Identity Platform checks the criteria for existing progressive profiling forms. If the user meets the criteria defined, the user is directed to one or more forms. When each of the displayed forms has been submitted with the required information the user is authorized to access the self-service UI.
Does the solution support a consent framework? To what degree is the consent control fine grained?	Health plan members should have fine-grained control over who has access to which parts of their personal data, along with the ability to immediately revoke any access, review the history of how their data was shared, and manage communication preferences.	Yes. ForgeRock User-Managed Access (UMA) is a privacy and consent solution based on UMA 2.0 that helps address compliance with consent requirements of privacy laws. Through UMA capabilities, the ForgeRock Platform allows users to manage -- grant and withdraw -- consents and permissions in a fine-grained fashion over time from a convenient central console across multiple data services. UMA capabilities are available in ForgeRock Access Management (authorization server), ForgeRock Identity Gateway (resource server), and through the Profile and Privacy Management dashboard in ForgeRock Identity Management. This user-centric approach addresses GDPR concepts of consent and data minimization. UMA capabilities also enable user control of access to APIs. The approach of protecting APIs that directly deliver data to processors without central aggregation addresses the GDPR concept of data accuracy. The ForgeRock Platform can also capture user consent to Terms and Conditions (T&Cs) and privacy notices, at both account registration time and at authentication time, and enables users to manage account information over time.

Question	Reason This Is Important To Ask	ForgeRock Answer
Does the system have the ability to store complex relationships that include many to many mappings?	Health plans manage complex health relationships between the Plan, family members and their various providers — who are often in care teams with different roles. These various roles, such as patient, covered member, provider, and even employer, have significant implications for the way Identity is managed and how access to information is granted.	Yes. The ForgeRock Identity Platform can manage relationships between identities. This can be used, for example, to manage relationships between a parent and a child, a physician and their patients, or an employee and their manager. Identities can also be created to represent any other thing or entity, such as between a user and their devices, connected medical devices, cars, organizations, companies, and services.
Does the solution support identity-enabling legacy applications that do not support current Identity/ Federation standards without modifying the underlying application?	Healthcare organizations typically have many legacy applications that have no knowledge of current Identity and Federation standards and protocols. Many health plans have legacy applications; such as for enrollment, eligibility, claims, and many others. These applications are typically very difficult if not impossible to upgrade, but they still need to be supported for an extended period of time. The Identity solution should allow for supporting current Identity Standards for access to these legacy applications.	Yes. The ForgeRock Identity Gateway allows customers to add SAML 2.0, OpenID Connect 1.0, and UMA 2.0 support, as well as fine grained access control to legacy applications without requiring any changes to the underlying application.
How is your organization contributing to thought leadership in the healthcare space?	A digital identity vendor who is invested in the healthcare space will continue to innovate and support such organizations now and going forward.	ForgeRock is investing significantly in the healthcare vertical and helping to drive innovation in this space. With the rising costs of face-to-face doctor visits driving the adoption of Telehealth and remote monitoring solutions, prescribing and gathering data from wearable medical devices is becoming common practice. Unfortunately, frameworks to perform chip-to-cloud medical device data and consent security are lacking. ForgeRock is a key member of the OpenMedReady alliance, a collaborative effort between technology and health leaders Arm, Philips, Qualcomm Life and ForgeRock, along with innovative healthcare startups Sparsa and US TrustedCare. Together we are focused on enhancing Patient Generated Health Data (PGHD) from medical devices to enable more trustworthy data sourcing and consented patient-information sharing. More information about this effort can be found at www. openmedready.org, and is one example of how ForgeRock is a leader in healthcare.

For additional RFP questions to ask digital identity management providers for CIAM, as well as an in-depth review of the components providers should offer, read *Comparing Digital Identity Management Providers for Customer Identity and Access Management*.

Notes:

ForgeRock: Defining Digital Identity Management

Identified as an customer identity and access management (CIAM) platform Overall Leader by KuppingerCole and one of the most visionary access management providers by Gartner, the ForgeRock Identity Platform is shaping the future of digital identity management.

The ForgeRock Identity Platform is a simple yet comprehensive digital identity management solution that can be implemented across an organization for all use cases — employees, customers, devices, and 'things'. The ForgeRock Identity Platform consists of access management, user-managed access, identity management, governance, automated identity, directory services, edge security, and an identity gateway. The full platform can be consumed as a service (PaaS) or deployed in minutes within any cloud environment, including multi-cloud and hybrid-cloud, for millions of identities. Importantly, the ForgeRock Identity Platform is the only solution on the market able to address all components of the six global trends and beyond. Read why in *Evaluating Digital Identity Providers for Customer Identity and Access Management: Top Criteria, Differentiators, and Questions to Ask CIAM Providers.*

Learn More About ForgeRock for Your Organization

ForgeRock is an overall leader and visionary digital identity management provider. Contact us to learn how ForgeRock can help your organization.