DATASHEET

HIPAA Compliance

ForgeRock Identity Cloud

The Health Insurance Portability and Accountability Act (HIPAA) is the U.S. national standard for health information security and privacy. HIPAA governs the use and disclosure of sensitive electronic Protected Health Information (e-PHI).

HIPAA requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.[1]

[1] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

How ForgeRock Supports HIPAA Compliance

ForgeRock's security foundation is based on three core principles of information security:

Confidentiality

Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity

The accuracy and completeness of information and related assets is safeguarded.

Availability

Information is accessible and usable upon demand by authorized entities only.

These principles underlay a cohesive framework to deliver ForgeRock Identity Cloud that allows healthcare organizations to simply and securely access the digital world.

In addition to supporting HIPAA requirements, the ForgeRock Identity Cloud helps your organization focus on elevating customer experiences and security instead of running IAM solutions and infrastructure. As the only SaaS-delivered identity platform purpose-built for the enterprise, it delivers the industry's most comprehensive set of IAM capabilities. With unparalleled security and flexibility, ForgeRock Identity Cloud provides solutions for today's hybrid enterprise through patented data isolation technology and options to augment SaaS with the most flexible IAM software deployment options available today.

To support healthcare organizations, ForgeRock Identity Cloud implements a HIPAA-compliant architecture that delivers these benefits.

Full Tenant Isolation

ForgeRock's cloud-native security architecture, with application containerization and Kubernetes cluster orchestration, delivers complete tenant isolation in a modern, multi-tenant cloud environment. There is no commingling of one customer's data with another. This ensures that each healthcare organization has complete control over their own data. With no central database of tenant data that can be compromised, you can keep your customers' information safe and secure.

Access Control

All users accessing ForgeRock systems, services, and applications are uniquely authenticated with strong credentials. Access rights, including accompanying privileges, are authorized by senior management according to business role and function. All access is granted on a "need to know" basis, and regulated according to role.

Access Monitoring

ForgeRock Identity Cloud is continuously monitored by highly trained ForgeRock experts using NIST 800-137 standards. To comply with HIPAA requirements, ForgeRock logs all searches run by any ForgeRock account to any customer environment. These access logs are stored in a long-term archive with a locked six-year retention policy to prevent tampering. Each HIPAA customer data set is also configured with safeguards to prevent accidental data deletion.

Incident Response

ForgeRock's incident management service is founded on the principles of detection, containment, eradication, and recovery. As soon as a potential incident is detected and the threat is identified, it is contained so that it does not spread to further systems or assets. Next, all compromised systems are cleaned or rebuilt to eradicate the threat. Finally, all operations are fully brought back online, and the system is recovered to its original state. If the security incident involved compromise or access to customer or supplier data, an incident notification process is initiated with all potentially affected parties. The incident notifications continue until the incident is resolved.

Disaster Recovery

ForgeRock Identity Cloud provides a high-availability architecture with transparent failover to meet strict service level agreement (SLA) requirements. ForgeRock includes an additional layer of capabilities with tenant-specific backup and restore. This feature, unique

to ForgeRock Identity Cloud, enables healthcare organizations to recover quickly and efficiently from any accidental or malicious data corruption issues.

Physical and Network Security

The cloud service provider maintains the physical security of the infrastructure itself, along with network security to prevent common threats like distributed denial-of-service (DDoS) attacks. ForgeRock implements an additional layer of physical safeguards for all workstations that access e-PHI.

Operational Security

The ForgeRock Enterprise Security team, under the leadership of the CISO, periodically reviews all operational procedures, including security policies, to ensure compliance with changing environmental and operational needs.

Encryption

The ForgeRock Security architecture extends tenant isolation with Federal Information Processing Standard (FIPS) 140-2 compliant encryption and hashing ciphers for in-flight messaging, protocol tunnels, and credential storage. The data is chunked and stored with different encryption keys to limit the "blast radius" of any potential encryption key compromise.

Secure Development

All development projects at ForgeRock follow secure development lifecycle principles. All new products, tools, and services undergo a design review to ensure that security requirements are incorporated into the proposed development. Major changes to existing products, tools, and services undergo the same design review. All ForgeRock system developers also participate in annual training in secure development principles and related disciplines.

Secure Testing

ForgeRock deploys automated vulnerability scanning of all production and internet-facing systems on a regular basis. This includes static and dynamic software application security testing of all code, including open source libraries, as part of our software development process. Regular penetration testing both by internal security engineers and external penetration testing companies is also conducted to ensure a comprehensive, real-world view of our products.

ForgeRock is regularly audited by an independent third party, to ensure compliance with HIPAA security regulations and breach notification requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act. The auditor verifies that all appropriate controls, procedures, and information security are in place for compliance.

In addition to HIPAA compliance, ForgeRock is also compliant with the following:

SOC 2 Type 2 | ISO 27001 | CSA STAR Level 2

For more information on how ForgeRock helps healthcare organizations, click here.