Frequently Asked Questions
Oracle Health Insurance Cloud Services

Top Security Features for Healthcare Payers

The purpose of this FAQ is to provide answers to common security-related questions about Oracle Health Insurance (OHI) Cloud Services.

Supporting Regulatory Compliance

Q: How does your product assist customers with their efforts to comply with regulations such as HIPAA?

A: Oracle Health Insurance Cloud Services are built for compliance and audited by third party auditors periodically. They are subject to an annual HIPAA audit. While the customer is responsible for ensuring compliance, Oracle's solution can accelerate the path to compliance by providing the infrastructure for it.

For more information on how Oracle Health Insurance Cloud Services support compliance in your region, call us at +1.800.735.6620.

Q: Is all protected health information (PHI) secured while in transit and at rest?

A: Yes, through industry-standard encryption.

Q: Where is the data stored?

A: Oracle operates both a production and secondary site within the same regional jurisdictional area.

Q: Does your solution provide role-based security and audit capabilities?

A: Role-based authorization is designed to limit the end user's access. An end user may only access the data his or her job function requires. Oracle monitoring and auditing systems are configured to log security-related activities. Those entries capture user account names and IP address, among many other details.

Ownership

Q: What are my ownership rights?

A: The customer owns any customer-specific configurations, data, and reference data.

Architecture

Q: Will my company's data be stored on servers with other customer data?

A: Oracle Health Insurance Cloud Services is a single-tenant model, where each customer has its system installed in a logically segregated environment.

Network Security Features

Q: What kind of controls has Oracle implemented to help keep my data secure?

A: Oracle safeguards access and integrity through a centralized system. Encryption features are designed to protect data-in-transit and all incoming network activity is subject to Oracle's security policies. Transparent data encryption (TDE) automatically encrypts and unencrypts data written to data files (also referred to as data at rest). Oracle protects its networks from unauthorized access through many features: penetration testing, vulnerability scanning, 24/7 Security Operations Center network monitoring through the Security Information and Event Management System (SIEM), virus detection software, firewalls, and more.

Q: How often does Oracle conduct penetration testing of your network?

A: When a service is made generally available and when a material upgrade is released.

Q: How does Oracle monitor events, detect attacks, and identify unauthorized use? Does Oracle log and monitor activity?

A: Oracle Cloud for Industry has a 24/7 Security Operations Center that monitors, logs and responds to security events including unauthorized access.

ORACLE

Q: Does Oracle maintain regular backups of the information systems and data?

A: Yes. Oracle Cloud for Industry performs regular backups. Those archival systems/disks are encrypted.

User Access Controls

Q: How does Oracle control user access to networking and computing resources?

A: Some of these safeguards are described above, including network access controls and network segregation. Other methods include network intrusion detection systems, network routing control, and system access controls.

In addition, Oracle's internal policies restrict privileged access and enforce separation of duty principles. Oracle also performs quarterly reviews of user access rights.

Other controls are built into various settings on devices and systems such as encrypted VPN for remote access. The customer's own security administrators also restrict user access by controling end user accounts.

Q: How are user passwords stored, encrypted, and transmitted?

A: Passwords are encrypted in transit and are protected when at rest. Passwords are stored in Oracle Identity Management, which uses AES 128-bit key for database encryption. The encryption is symmetric. It can be decrypted to a plain-text password using a key stored in Oracle Platform Security Service Credential Store Framework.

Encryption

Q: Does Oracle Health Insurance Cloud Services use encryption? If yes, tell me more about what gets encrypted.

A: Yes. Data in transit, data at rest, backups, and passwords are encrypted.

Data Center Security

Q: How does Oracle assess the physical and environmental controls in its data centers?

A: Oracle Health Insurance Cloud Services Data Centers undergo a third-party review of the physical and environmental controls using the standards in the SSAE 16 and ISAE 3402 annually.

Q: How do you physically protect your data centers from intruders?

A: In addition to staffing main entrances around the clock with security guards, Oracle requires authorized visitors to have electronic photo identification badges and cardholder access, and pass biometric scanning. Interior and exterior areas are under digital video surveillance, and all buildings have intrusion detection alarm systems. Visitors are prohibited from bringing in certain items such as cameras, recording devices, and any wireless communications devices.

Security as an Organization

Q: How do you train your employees on your security policies and health insurance industry best practices?

A: Oracle requires all employees who access protected health information to undergo biannual corporate privacy and security training, as well as annual HIPAA specific training. This is verified by third-party auditors during annual audits. Internally, Oracle promotes security awareness and training. Courses cover data privacy principles as well as data handling practices and corporate ethics.

Disaster Recovery and Resilience

Q: How does Oracle Health Insurance Cloud Services respond to disruptions?

A: Our cloud services were developed with business resiliency in mind. That's why Oracle has built-in protections to support customers, including fully redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases. Should there be a disaster declared by Oracle, our customers are notified immediately and provided with an estimated uptime for restoration of services.

Q: Do you have an alternative site to recover all services in case of a disaster?

A: Yes. Oracle offers separate data centers that function as primary and secondary sites for Oracle Cloud Services. In the event of a failure, customers who have chosen enhanced recovery service will have their data and services failed over to the alternate site.

Q: What are the basics of your disaster recovery plan?

A: In the event of a disaster, Oracle's first priority will always be human health and safety. Then Cloud Operations will typically manage recovery in the following stages:

Phase 1: Detect and determine the extent of the damage.

Phase 2: Recover and restore temporary IT operations at the secondary site.

Phase 3: Restore processing capabilities and resume operations at the primary site.

Q: How often do you test your disaster recovery plan?

A: Annually.

Useful Links

The FAQs here offer summarized versions of the complete answers. For more detailed information, click on the following links:

- Oracle Services Privacy Policy
- Oracle Global Customer Support Security Practices
- Oracle Cloud Services Agreements
- Oracle Cloud Hosting and Delivery Policies
- Oracle Financial Services Global Business Unit Service Descriptions and Metrics
- Oracle Financial Services Service Descriptions and Metrics – Oracle Insurance Claims Administration and Oracle Insurance Policy Administration Cloud Service

The following documents are available under NDA:

- Oracle Cloud Security Practices for Software as a Service (SaaS) Cloud Services
- Oracle Cloud Services Disaster Recovery Practices
- Oracle Cloud Services Backup Practices

CONTACT US

For more information about Oracle solutions for insurance, visit oracle.com/insurance or call +1.800.735.6620.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200