ORACLE
Health

Oracle Health Supplier Information and Physical Security Standards

Effective Date: July 07, 2025

Contents

ORACLE Health

SCOPE

These Oracle Health Supplier Information and Physical Security Standards (the "Standards") list the minimum security controls that Oracle Health's Suppliers are required to adopt when performing Services pursuant to an agreement with Oracle Health (the "Agreement"). Capitalized terms used herein but not defined have the meaning ascribed to them in the Agreement.

SUPPLIER OBLIGATIONS

Supplier is responsible for compliance with these minimum Standards by its employees, agents, and subcontractors (Personnel), including ensuring that all Personnel are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in Supplier's agreement with Oracle, including any Oracle Health Supplier Business Associate Agreement (SBAA) or the TOMs (as defined below). These Standards supplement the SBAA with respect to Protected Health Information ("PHI" as defined by HIPAA), and the provisions of the SBAA control if they conflict with these Standards, with respect to PHI. Supplier will have policies, procedures, and technical controls in place to maintain the confidentially, integrity, and availability of Oracle Health and Oracle Health client information, including any Personal Information (as defined by applicable data protection law) or PHI. In the event that Supplier cannot comply with these Standards, it will immediately notify Oracle Health, in which case the parties will work in good faith to determine a reasonable solution.

PART A: ADMINISTRATIVE SAFEGUARDS

A.1 Security Program. Supplier will maintain a documented information security management program and risk management program that includes monitoring of Supplier's subcontractrors (collectively, the "**Security Program**") with clearly defined roles and responsibilities, policies and procedures, standards and guidelines that reflect compliance with these terms. Supplier will maintain policies that require Personnel to report security incidents and other violations of the Security Program to Supplier management for investigation and action. Supplier will engage a qualified third party to perform an assessment of its Security Program to test the effectiveness of its security controls no less than annually. Supplier will establish and maintain a security awareness training program for all Personnel, and require all Personnel to attend security awareness training at least annually. Supplier will track on-boarding and off-boarding of Personnel, with appropriate access termination for Personnel whose employment or services are terminated or whose duties are changed. Supplier will certify annually to Oracle Health to the effectiveness of its Security Program. Supplier will require all existing and new Personnel to follow and comply with these Safeguards, and Supplier will take appropriate action against Personnel who fail to comply with the Safeguards, Supplier's Security Program, applicable law, the Agreement, and otherwise determined by the Supplier or Oracle Health.

A.2. Cybersecurity. Supplier will maintain Personnel responsible for cybersecurity, including an executive level senior leader responsible for Supplier's Security Program. Supplier and its cybersecurity Personnel will, at a minimum:

a. Maintain and manage industry standard infrastructure perimeter controls;
b. Maintain a process for applying critical and high risk security patches for Supplier's computing environments within a reasonable period;
c. Update security applications and appliances frequently to enable the latest security protection packages to protect Supplier's computing environments;
d. Conduct continuous vulnerability scanning of Supplier's solution stack from the application layer to the infrastructure layer, using industry standard automated scanning tools;
e. Engage a qualified third party security service provider to conduct industry standard penetration testing for Supplier's applications and systems at least annually;

f. Maintain a process for reviewing and remediating risks and vulnerabilities identified from such scanning and testing;
g. Provide, upon Oracle Health's request, a "Penetration Testing Attestation Letter," which will describe the penetration testing that was performed, confirm that an industry standard methodology, testing tools and national vulnerability database were used, and confirm that identified vulnerabilities have been remediated or addressed in a plan for remediation and actively monitored; and
h. Maintain a continuous monitoring framework under which cybersecurity events, threats and incident management are monitored 24 hours per day, 7 days per week.

PART B: PHYSICAL SAFEGUARDS

B.1 Access Controls. Supplier will maintain physical access controls designed to protect Supplier's data centers and the Data from unauthorized access, theft, or damage. Such controls will include, at a minimum:

a. Armed security officers 24 hours per day, 7 days per week;
b. A security operations center that provides security monitoring and situational management 24 hours per day, 7 days per week;
c. Layered controls covering perimeter and internal barriers;
d. Access logging;
e. Environment controls in compliance with industry standard practices;
f. Electronic surveillance using strategically placed cameras and motion alarms; and
g. Physical access management utilizing authentication mechanisms, such as badges and documented approvals.

PART C: TECHNICAL SAFEGUARDS

C.1 Technical Safeguards. Supplier will maintain an identity and access management system and controls that include the following, at a minimum:

a. Policies, procedures, and/or technical controls to provide timely modification or revocation of Personnel's access, privileges are authorized and appropriate for their job responsibilities, and follow the least privileged access model;
b. A compliance program which shall be designed to ensure compliance with these Standards (i.e., Data encryption, Username and password, two-factor authentication, file permission control, version control, backups) to protect the confidentiality, integrity and availability (the CIA Triad) of the Oracle Health data;
c. Restriction of logical access to Supplier systems to Personnel and non-Supplier personnel with approved active work agreements, with access being permitted as appropriate to their respective functions;
d. Controls to prevent unauthorized access to its or Oracle Health's application, program, or object source code and ensure that access is restricted to authorized Personnel only;
e. Restriction on use of any Oracle Health confidential information from production systems for development, testing, or staging purposes. Any use of confidential information for artificial intelligence models or training purposes is strictly prohibited unless expressly authorized by Oracle Health in a separate agreement.
f. Identification of Personnel by a unique user identifier and password as a condition to gaining access to Supplier systems;
g. Authentication of users by individual corporate applications using the assigned unique identifiers for access, depending on the nature of the application and user requirements;
h. Use of industry standard password complexity rules (as required by the National Institute of Standards and Technology (NIST) security standards), password change and re-use rules. National identifiers or Social Security Numbers must not be utilized as User IDs for logon to applications.

i. Restriction of any Personnel from using generic account logins;
j. A process to approve (i) requests for, (ii) monitoring of, and (iii) modifying system access which includes eligibility criteria for access, formal request and approval for access, proper segregation of duties analysis, account verification and regular review of access privileges;
k. Timely de-provision (revoke, suspend or modify) Personnel access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, which shall be implemented as per established policies and procedures;
l. An authorized user list identifying individuals, including third parties, authorized to access Oracle Health's system, data or solution which may be provided to Oracle Health upon written request.
    i. Such approved access shall be reviewed by management at least annually or sooner if the parties agree dependent on scope of Services;
    ii. Access will be suspended, revoked, denied or terminated immediately without proper authorizations;
    iii. Access shall be reviewed when Personnel change roles and shall be removed when role requires no access; and
    iv. Access shall be removed immediately, but no later than within 24 hours of termination of employment. Upon termination, Personnel must return all company-owned devices, which shall securely wiped.
m. Document exceptions for any Personnel or third party to bypass Supplier's policies and procedures and demonstrate approval by Supplier's executive level approver;
n. Oracle Health may deny access to Supplier in its sole discretion;
o. The parties responsible for the installation, maintenance, and change control of the various hardware and software assets shall be established, documented and shared with Oracle Health and relevant parties as applicable;
p. Document defined roles and responsibilities regarding hardware, software installation and maintenance;
q. Implement a change management process with appropriate segregation of duties and validation of the results;
r. Encryption of Data, in transit or at rest, using VPN, Secure FTP, PGP, Windows Bit Locker, whole disk encryption, or another Supplier-approved encryption method consistent with industry standards and applicable law. Secure Sockets Layer (SSL) with a cipher strength of 128-bit is, at a minimum, required for data across public networks in transit and Advanced Encryption Standard (AES) with cipher strength of 256-bit is, at a minimum, required for data at rest on internal or external networks and devices used to perform Services;
s. Encryption of all back-up media, laptops, mobile devices, jump/USB and similar drives, and on other devices that interact with or store Data;
t. Enable monitoring of key assets and revoke access upon request by Oracle Health in response to any suspicious activity related to assets being used to host or process Oracle Health or Oracle Health Client Data;
u. Monitor assets and networks under the Supplier's control to identify compromised hardware and software that process, store, or otherwise transfer Oracle Health or Oracle Health Client information;
v. Maintenance of audit logs of all devices that interact with or store Data so that if a device is lost or stolen, Supplier can verify that the device was encrypted;
w. Requirement that the only desktops/laptops that can be used for the provision of any Services under the Agreement or Task Order are Supplier-approved desktops/laptops;
x. Maintenance of policies and procedures governing remote work areas and printer usage to address risks of unauthorized disclosures;
y. Configuration of all Supplier systems and devices with industry standard malware prevention and anti-virus controls;

z. Prohibition on downloading Data to local disk, servers, or other personal or mobile media devices (including personal USB thumb drives);
aa. Requirement of all non-Supplier owned/supplied equipment (e.g., subcontractors connecting to the Supplier network) to desktop vulnerability scans to validate the strength of security controls (e.g., anti-virus, firewalls, anti-spam);
bb. Industry standards such as BSIMM, NIST, OWASP, etc. to build in security for Supplier's Systems Development Lifecycle (SDLC);
cc. Practice secure design and coding techniques;
dd. Use both an automated and manual source code analysis tool to detect and remediate security defects in code prior to production deployment;
ee. Maintain policies and procedures to triage and remedy reported bugs and security vulnerabilities for the products and Services it provides to Oracle Health;
ff. Include security control validation in their test planning and execution; and
gg. Include server configuration security reviews in the deployment phase.

PART D: SECURITY INCIDENT MANAGEMENT AND REPORTING

D.1 Security Incident. Supplier will, within twenty-four (24) hours of becoming aware of an actual or threatened security breach which compromises or may lead to the compromise of the confidentiality or security of the Oracle Health Data ("Security Incident"), notify Oracle Health in writing of such Security Incident. For any Security Incident, Supplier will: (i) promptly furnish to Oracle Health full details of the Security Incident; (ii) reasonably assist and cooperate fully with Oracle Health in Oracle Health's investigation of Supplier, Personnel, or third parties related to the Security Incident, including, but not limited to, providing Oracle Health with reasonable physical access to Supplier's premises and facilities, books, records and procedures and divisions of the facilities and operations affected, facilitating interviews with employees and others involved in the matter, and making available all relevant records, logs, files, and data; (iii) cooperate with Oracle Health in any litigation or other formal action against third parties deemed reasonably necessary by Oracle Health to protect its rights and rights of its clients and customers; and (iv) promptly use its reasonable efforts to prevent a recurrence of any such Security Incident. Supplier will perform such actions at its own cost and expense.

D.2. Security Incident, Breach Notification and Continual Update Process. Supplier will develop a schedule for ongoing updates to Oracle Health throughout investigation and remediation of the Security Incident. Supplier will name a contact who will be responsible for scheduling and maintaining communication for the updates. The updates will be progressive in nature. Frequency of the updates will be determined by mutual agreement between Supplier and Oracle Health, depending upon the severity of the issue.

D.3 Notification. Unless otherwise required by applicable law, Supplier agrees that in the event of a Security Incident, as between the parties, Oracle Health has the sole right to determine, (a) whether notice or disclosure is to be provided to any customers, individuals, regulators, law enforcement agencies, or consumer reporting agencies, as required by law or regulation or in Oracle Health's discretion, and (b) the contents of such notice or disclosure, whether any type of remediation may be offered to affected individuals and the nature and extent of any such remediation. In addition to any remedies available to Oracle Health under the Agreement, at law or in equity, upon occurrence of a Security Incident, Supplier will be liable for any and all costs and expenses incurred by Oracle Health or Oracle Health's clients or customers arising from remedying any such Security Incident.

PART E: IT SECURITY CONTROLS

E.1 Remote Access and Location of Supplier Operations. Supplier may only access Oracle Health networks or systems or Oracle Health customer network and systems upon prior written approval by Oracle Health and in accordance with and subject to all applicable network and system access policies provided by Oracle Health

or Oracle Health customer to Supplier. Unless otherwise specified in the Agreement or a Supplier Data Processing Agreement, the Supplier will ensure that all Oracle Health Data resides in, and may be accessed only from within, the United States of America.

E.2 Audit. Supplier will maintain complete, auditable records relating to its obligations under these Standards. Oracle Health and its authorized third parties and representatives (including internal and external auditors and regulators) will have the right to perform an audit, during reasonable business hours, and upon reasonable notice to review Supplier's security, confidentiality, privacy practices and standards and overall compliance with these Standards. Such audit shall not compromise the confidentiality of Supplier's other customers' information. In addition, on an annual basis, the Supplier will complete an Oracle Health written assessment or questionnaire which Oracle Health may share with any relevent clients or regulatory authorities subject to appropriate confidentiality restrictions.

PART F: CERTIFICATIONS

F.1 Certifications and Required Artifacts. Supplier is required to maintain the below, as applicable, for the relevant Services. Supplier will promptly provide the following to Oracle Health upon Oracle Health's request or as otherwise set forth below, to demonstrate that the Services are in scope of the following audits, certifications, assessments or reports (as applicable):

a. SOC 2 Type 2. On an annual basis, Supplier, at its sole cost and expense, will retain a qualified, third party assessor to perform an annual audit of its security controls with respect to the Services provided under the Agreement, and provide a SOC 2 Type II report (or industry equivalent) to Oracle Health.

b. HITRUST. Supplier will retain a qualified, third party assessor to perform a Health Information Trust Alliance ("HITRUST") framework certification. The resulting certification and Corrective Action Plan reports will be provided to Oracle Health upon Oracle Health's request.

c. PCI - DSS Assessment. If applicable, where the provision of Services involves Personnel receiving Oracle Health cardholder data, Supplier agrees and will at its own cost and expense, engage a qualified auditor to perform a PCI DSS assessment promptly upon request by Oracle Health. On an annual basis, Supplier will provide Oracle Health evidence demonstrating its ongoing compliance with the PCI DSS requirements.

d. Penetration Test Attestation. Supplier will, upon Oracle Health's request but no less than once yearly, provide a Penetration Testing Attestation Letter. The letter will describe, at a minimum, the penetration and vulnerability testing that was performed, confirm that an industry standard methodology, testing tools and national vulnerability database were used, and that identified vulnerabilities have been remediated or are being addressed in a plan for remediation and actively monitored.

e. Right to Disclose. Supplier understands that Oracle Health may share the relevant certifications or reports with clients and regulatory authorities subject to appropriate confidentiality restrictions.

PART G: OTHER ORACLE HEALTH REQUIREMENTS

G.1. Oracle Health Technical and Organizational Measures. Where a Supplier (i) Processes Personal Data of residents of the European Economic Area, the United Kingdom or Switzerland; or (ii) is located or provides Services outside of the United States of America, the Supplier shall comply with the Oracle Health Technical and Organization Measures (TOMs). For purposes of these Standards, all references in the TOMs to "Cerner" shall mean Oracle Health.

G.2. Oracle Health Restricted Transfers under the Final Rule. Where a Supplier or a Supplier Affiliate will have Access to Oracle Health or Oracle Health Affiliates' Covered Data to perform the Services, Supplier represents, warrants, and covenants that: (i) neither Supplier nor any Supplier Affiliate who has Access to Covered Data (nor any Personnel or subcontractor of Supplier or any Supplier Affiliate who has Access to

Covered Data) is a Covered Person; (ii) Supplier and Supplier Affiliates will not engage in any Covered Data Transaction; and (iii) Supplier will immediately notify Oracle Health in writing if any representation in this Section changes or is no longer true. For purposes of this Section, "Access", "Country of Concern", "Covered Data", "Covered Data Transaction", and "Covered Person" have the meanings set out under the Final Rule. "Final Rule" means the rule implementing Executive Order 14117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, along with any additional guidance, advisory opinions, or licensing decisions, issued by the U.S. Department of Justice.

G.3 EU Data Act Requirements. If applicable, the Transfer of any Non-Personal Information, including Metadata (both as defined under the EU Data Act), is subject to safeguards as set out in Section 6 of the Oracle Health SDPA.