KAISER PERMANENTE

KAISER PERMANENTE
DATA SECURITY REQUIREMENTS
FOR VENDORS, CONTRACTORS AND SUPPLIERS

1. **Definitions.** The following terms shall have the meaning set forth below for purposes of this Data Security Requirements document (the "***Requirements***"):

"***Kaiser***" means Kaiser Foundation Health Plan, Inc. and/or Kaiser Foundation Hospitals and their respective subsidiaries.

"***Kaiser Permanente****" or "****KP***" means the integrated health care delivery organization doing business as Kaiser Permanente, which includes Kaiser Foundation Hospitals, Kaiser Foundation Health Plan, Inc., Kaiser Permanente Insurance Company, The Permanente Federation, the Permanente Medical Groups, and the subsidiaries, partners and successors of the foregoing.

"***KP Network***" means the Kaiser Permanente electronic information systems network and related environment.

"***KP Sensitive Information****"* means certain sensitive, confidential, proprietary or other non-public information related to the business of Kaiser Permanente, including but not limited to: (a) personally identifiable information, data or records relating to or concerning any patient, member, plan participant, employee or contractor of any Kaiser Permanente entity, including, without limitation, Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA), and "Cardholder Data" under the Payment Card Industry data security standards; provided, however that not included within this definition shall be certain limited subsets of personally identifiable information, excluding Protected Health Information or Cardholder Data, that (i) only include and are limited to the one or more of the following identifiers of the individual who is the subject of the Personal Information or of relatives, employers or household members of such individual: name, postal addresses, telephone numbers, fax numbers, email addresses, URLs and IP address numbers, and (ii) are not associated with any of the categories of sensitive information referenced in clause (b) of this defined term below; and (b) other sensitive information of Kaiser Permanente, including but not limited to: business strategy information; marketing plans; price data; non-public financial, operational or facilities information or records; information relating to or lists of actual or potential vendors, customers, suppliers, employees, independent contractors, health plan subscribers or beneficiaries, and other third parties; de-identified Protected Health Information; claims data; clinical trial results; proprietary software, hardware and other information technology of Kaiser Permanente's; network and security system designs, architecture, operations and configurations; and network architecture. KP Sensitive Information shall always be Confidential Information of Kaiser Permanente.

"***Secure Services***" means services provided by Supplier, directly or indirectly, that involve accessing, generating, processing, hosting, downloading, printing, maintaining, transferring, receiving or storing, in any form or medium, KP Sensitive Information and/or accessing the KP Network, including, for example, application management, data processing, hosting, or cloud services.

*"****Secure Services Infrastructure****"* means the computer hardware, software, communications systems, network and other infrastructure used by Supplier or any Supplier Subcontractor to host and provide Secure Services.

"***Service Location***" means each facility used to provide Secure Services, including any hosting, data center, co-location or other facility operated by Supplier or a Supplier Subcontractor (also including any Kaiser-approved Offshore locations as described in Section 4 below).

"***Supplier***" means a third party services provider including but not limited to vendors, contractors, suppliers, or insurance brokers who are providing the Secure Services to Kaiser Permanente.

*"**Supplier Security Controls**"* shall have the meaning set forth in Section 6 below.

*"**Supplier Subcontractor**"* means any contractor or subcontractor of Supplier, at any tier, performing one or more Secure Services on behalf of Supplier.

"***Vulnerability Scanning and Penetration Testing***" means an assessment of systems/applications/environments involved in the Supplier's provision of the Secure Services, which may include application security vulnerability scanning (on at least a monthly basis), penetration testing (on at least an annual basis), static analysis, and/or manual code review, to identify any issues with configuration of firewalls, web services, servers and other system components that could result in access vulnerabilities.

2. **Compliance; Service Locations.** These Requirements shall apply in all cases in which Supplier or any Supplier Subcontractor provides Secure Services, including when such provision of the Secure Services involves accessing the KP Network. These Requirements shall also apply when KP Sensitive Information is collected and transmitted to the Supplier using any method and shall apply to any form or medium of KP Sensitive Information, including KP Sensitive Information in electronic or hard copy. Each Service Location must meet or exceed the requirements set forth in these Requirements, including, without limitation, the Supplier Security Controls set forth in Section 6 below. Supplier is responsible for each Service Location's compliance with these Requirements. Prior to onboarding a new Service Location or making any change in any existing Service Location (including, e.g., any change in a hosting, data center, co-location facility or provider), Supplier will provide written notice and an opportunity for Kaiser to (a) review the proposed new facility and/or provider, or (b) conduct a Security Assessment (defined in Section 7 below).

3. **Supplier Subcontractors.** If Supplier uses any Supplier Subcontractors in the performance of Secure Services, Supplier shall be responsible for each such Supplier Subcontractor's compliance with these Requirements. Prior to providing Secure Services, Supplier shall provide to Kaiser a list of Supplier Subcontractors and their responsibilities, and Supplier shall inform Kaiser of any changes to such list of Supplier Subcontractors throughout the term of the provision of Secure Services.

4. **No Offshore.** No Service Location may be located outside the United States, United States territories, or Puerto Rico ("**Offshore**") without Kaiser's prior written approval. No KP Sensitive Information may be accessed, generated, hosted, downloaded, printed, stored, processed, transferred, or maintained Offshore by Supplier or any Supplier Subcontractor without prior written approval by a responsible Kaiser senior executive. Supplier is responsible for the compliance of such approved Offshore Service Locations with these Requirements. Such approval may be withheld by Kaiser for any reason in its sole discretion and/or approval may be subject to additional terms and conditions.

5. **No Portable Media.** KP Sensitive Information may not be stored or maintained on portable media or devices without Kaiser's prior written approval. In the event any KP Sensitive Information is stored

or maintained in a portable computer, tablet or portable endpoint device (e.g., USB flash memory or thumb drive, smart phone (such as an iPhone or Android device)) or on any other form of removable or transportable media, such KP Sensitive Information must be encrypted in accordance with all applicable legal and requirements, including use of strong cryptography in accordance with then-current industry standards, including NIST-800-53A.

6. **Supplier Security Controls.** In accordance with generally accepted industry practices and the specific requirements set forth herein, Supplier and any Supplier Subcontractor will establish and maintain, including at each Service Location, Supplier Security Controls that adhere to, at a minimum, NIST-800-53 and/or ISO 27001 industry standard controls in order to protect the security and privacy of KP Sensitive Information and the KP Network in its delivery of Secure Services, including but not limited to those controls therein: (i) against the destruction, loss, or alteration of KP Sensitive Information; and (ii) against unauthorized access to KP Sensitive Information (collectively the "***Supplier Security Controls***"). Supplier will promptly notify Kaiser of any material changes to the Supplier Security Controls that may negatively impact Supplier's or any Supplier Subcontractor's provision of Secure Services. Such Supplier Security Controls shall at a minimum cover the following types of control domains:

   i. Access Control
   ii. Asset Management
   iii. Business Continuity Management
   iv. Communications Security
   v. Compliance
   vi. Cryptography
   vii. Data Sanitization
   viii. Human Resource Security
   ix. Information Systems Acquisition, Development, and Maintenance
   x. Information Security Incident Management
   xi. Information Security Policies
   xii. Organization of Information Security
   xiii. Operations Security
   xiv. Physical and Environmental Security
   xv. Supplier Relationships

7. **Security & Compliance Assessments.** Kaiser or a reputable third-party assessor of Kaiser's choosing may perform periodic evaluations and/or inspections of Service Locations and Supplier Security Controls (each a "***Security Assessment***") (a) prior to onboarding the new Service, (b) after any material change to the Secure Services or any Service Location, or (c) during the performance of Secure Services. In the event that Supplier Subcontractor performs Secure Services, Supplier shall cooperate with Kaiser to support and/or facilitate Kaiser's ability to assess Supplier Subcontractor's performance of the Secure Services, as set forth in this Section 7.

   i. Independent Certifications.
      a. If available, Supplier will provide Kaiser, on an ongoing basis each year or after each material change, with copies of all independent, third-party certifications (each an "***Independent Certification***") of Supplier's and Supplier Subcontractor's applicable data

security controls (e.g.; ISO, SOC 1, SOC 2, HITRUST, etc.) that address all or a portion of the subject matter of these Requirements with respect to the Secure Services (e.g., information security, internal controls, privacy). For the avoidance of doubt, if Supplier Subcontractor is providing Secure Services, Supplier will facilitate the provision of such Independent Certifications to Kaiser.

b. If Supplier's or Supplier Subcontractor's provision of Secure Services have a material impact to the accuracy of Kaiser's financial statements, Supplier shall hire a third-party auditing firm on an annual basis to perform a Statement on Standards for Attestation Engagements (SSAE) No. 18 audit, or equivalent audit, and provide Kaiser with a copy of the SOC 1, Type 2 report within ten (10) business days of receipt of the report.

c. Each Independent Certification will cover a minimum period (or combined period in the case of two annual reports) of twelve (12) months. In the event that any Independent Certification or other form of independent audit results in a finding that Supplier's or Supplier Subcontractor's controls are inadequate, Supplier will promptly, at Supplier's cost and expense, (a) prepare a plan for remediation, (b) provide a copy of such plan to Kaiser, and (c) implement such plan.

d. If Kaiser determines that one or more Independent Certifications provide an adequate assessment of the Supplier Security Measures, Kaiser may accept such Independent Certifications in lieu of all or a portion of the Security Assessment described in Section 7.ii (Security Assessment) below.

ii. Security Assessment.

a. **Assessment Overview**. The specific controls evaluated in each Security Assessment will vary depending upon the nature of the Secure Services, but may include any or all of the following:

(i) Supplier's completion and return of Kaiser's security questionnaire, with supporting documentation;
(ii) Onsite visits and interviews of responsible personnel;
(iii) Supplier's provision of written security assessments of their Supplier Subcontractors and other third parties assisting in the provision of Secure Services;
(iv) In cooperation with Kaiser, Supplier's appropriate testing of user access controls prior to implementation of such access controls; or
(v) In the event that Supplier or Supplier Subcontractors do not have Vulnerability Scanning and Penetration Testing performed by an independent, reputable third-party assessor, then Kaiser or a reputable third party of its choosing, in cooperation with Supplier, may perform security testing and verification of the Service Locations and the systems/applications/environments involved in the Supplier's provision of the Secure Services, which may include Vulnerability Scanning and Penetration Testing.

b. **Assessment Frequency**. Kaiser may conduct Security Assessments prior to engaging Supplier to perform Secure Services and on an annual basis thereafter (unless a different frequency is specified in the applicable agreement between the parties). In the event of any security breach with respect to KP Sensitive Information attributable to Supplier's

performance of Secure Services, Kaiser may require more frequent Security Assessments and/or other actions or controls, including, without limitation, those set forth in the applicable agreement between the parties.

c. **Mitigation**. If a Security Assessment results in a finding that Supplier Security Controls are inadequate or are not being enforced, Supplier will, in consultation with Kaiser but at Supplier's expense, promptly implement appropriate corrective actions to remediate the gaps or security vulnerabilities identified. Alternatively, Supplier may provide supplemental information sufficient to demonstrate that any perceived security risk that may negatively impact Supplier's protection of KP Sensitive Information or performance of Secure Services has been satisfactorily addressed by Supplier.

8. Response to Security Incidents.

i. Notification to Kaiser. Supplier will notify Kaiser as soon as practicable but not longer than twenty-four (24) hours after discovering an actual breach and/or security event impacting the security of the Secure Services Infrastructure, the KP Network or the Supplier Security Controls (each a "***Security Incident***") by emailing the Privacy Incident mailbox at PrivacyIncidents@kp.org or by calling the Kaiser National Compliance Hotline at 1-888-774-9100. If Supplier sends a breach notification email to the Privacy Incident mailbox, Supplier will enable delivery request receipt of such notification email, and Supplier's foregoing notification obligation will not be considered fulfilled until Supplier has received an automated or Kaiser generated confirmation receipt email.

ii. Mitigation. Supplier will promptly implement corrective actions in response to any Security Incident, including, if requested by Kaiser, shutting down all access to any such system in which any KP Sensitive Information is hosted to address the Security Incident.

iii. Investigation. Supplier will promptly conduct an investigation of any Security Incident and submit an initial report of its findings to Kaiser within three (3) business days, to be followed by a written report approved by a senior member of Supplier's security team as soon as practicable, but no later than one (1) business week following the occurrence of such Security Incident. Supplier will respond to reasonable requests from Kaiser for information regarding the Security Incident and will cooperate reasonably with Kaiser in connection with any incident management, including with respect to external and media relations, law enforcement activities, and notification to affected individuals.

iv. KP Investigation and Evidence Request. Upon the occurrence of a global or material security event, Supplier will cooperate with Kaiser's due diligence requests with respect to Supplier's posture regarding such global or material event, and will respond to such due diligence requests in a timely fashion. For any Security Incident involving the KP Network, KP systems, members, employees, and/or respective KP Sensitive Information or content, Supplier agrees to cooperate with Kaiser with respect to Kaiser's investigation of such Security Incident, including providing, as applicable, the following evidence or other artifacts requested within three (3) business days of such request provided by Kaiser, as follows:

a. Evidence files: Supplier will provide forensic evidence files collected from compromised and/or affected computers and devices within the scope of the investigation.

b. Logs: Supplier will provide all logs from all computers and devices affected by or containing a record of the Security Incident, or the response to it, for the entire time frame surrounding the Security Incident and corresponding response activity. Logs include, but are not limited to: 1) All host logs (operating system logs, application logs, security event logs, user event logs), 2) Network and security device or software logs (network firewalls, application firewalls, intrusion detection/prevention system logs, antivirus), and 3) Log aggregation software or devices (SIEMs, syslog servers, or any software or device used for collecting, parsing, or aggregating logs).

c. Change management and security patching: Supplier will provide a change management/security patching historical record for all changes requested and/or completed to all computers, applications, devices, networks, and environments in the scope of or related to the investigation.

d. Network and security infrastructure diagram: Supplier will provide a detailed diagram and data flow of the network, security, and computing infrastructure (servers, workstations, and other protected devices) at the time of the Security Incident and changes that have occurred following the Security Incident.

e. Communications: Supplier will provide all communications regarding the security, configuration, change management, detection of the Security Incident in question, and/or response the Security Incident in question for computers, applications, devices, networks, and environments in the scope of or related to the investigation.

f. Vulnerability scans and penetration tests: Supplier must provide all results from vulnerability scans and penetration tests to all computers, applications, devices, networks, and environments in the scope of or related to the investigation.

g. Attestations: Supplier and/or its reputable third party incident response firm (1) shall have performed a comprehensive analysis of any Security Incident that involves an intrusion or breach, (2) affirmatively determined that the relevant networks, resources and data were not affected, (3) have validated that such networks are secure in accordance with industry standards and are ready to resume the performance of Secure Services to Kaiser, and (4) shall deliver to Kaiser a written attestation of (1) – (3) above, signed by either an officer of Supplier, legal counsel to Supplier, a Supplier compliance officer, or a reputable third party incident response firm that was materially involved in the performance of such analysis.

v. Consumer Remedies. With respect to any Security Incident that arises in a Services Location and/or within the KP Network, or is otherwise associated with Supplier's (or a Supplier subcontractor's) systems or network or the Secure Services, and was caused by: (a) Supplier's failure to perform its obligations under this Agreement or an applicable Business Associate Agreement, including violation of any data security or privacy law; (b) Supplier's, Supplier Subcontractor's or any of their employees or agents' negligent acts

or omissions or intentional wrongdoing, Supplier shall be responsible for the costs associated with notification of affected individuals and the provision of any required consumer remedies, such as credit monitoring or ID theft insurance.

9. **Indemnification.** Supplier will defend, indemnify and hold Kaiser, Kaiser Permanente, and their respective officers, directors, employees and agents harmless from and against all liabilities, claims, actions, losses, damages, judgments, orders (judicial or administrative), penalties, fines, settlements and other costs and expenses (including reasonable attorneys' fees and costs) arising from or relating to any breach of these Requirements.