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 "***Data Security Requirements***"):

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

"***Kaiser Permanente***" 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.

"***Personal Information***" or "***Patient/Personal Data***" means 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 ("PHI") under HIPAA and "Cardholder Data" under the Payment Card Industry ("PCI") data security standards. Personal 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 Personal Information, including, for example, application management, data processing, hosting, or cloud 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 at which any Secure Services are provided.

"Supplier Security Measures" means appropriate safeguards and controls which conform to the requirements set forth herein and are used by Supplier and each Supplier Subcontractor to protect the security and privacy of Personal Information, including: (i) safeguards and controls against the destruction, loss, or alteration of Personal Information; and (ii) safeguards and controls against unauthorized access to Personal Information.

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

"***Supplier***" means a vendor, contractor or supplier who is providing the Secure Services to Kaiser Permanente.

2. Compliance at Each Service Location. Each Service Location must meet or exceed the requirements set forth in this Data Security Requirements document, including, without limitation, the Supplier Security Measures set forth in Section 6 below. Supplier is responsible for compliance with these Data Security Requirements at each Service Location. Prior to any change in any Service Location (including, e.g., any change in a hosting, data center, or co-location facility or provider), Supplier will provide written notice and an opportunity for Kaiser to review the proposed new facility and/or provider. No Service Location may be located outside the United States without Kaiser's prior written approval.

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 Data Security Requirements.

4. No Offshore Access to Personal Information. No Personal Information may be accessed, generated, hosted, downloaded, printed, stored, processed, transferred, or maintained outside of the United States by Supplier or any Supplier Subcontractor without Kaiser's prior written approval. 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. Personal Information may not be stored or maintained on portable media or devices without Kaiser's prior written approval. In the event any Personal Information is stored or maintained in a portable computer, tablet or portable endpoint device (e.g., a zip drive, USB flash memory or thumb drive, mp3 player, smart phone (such as an iPhone, Android, Windows or Blackberry device)) or on any other form of removable or transportable media (e.g., tape, diskette or CD-ROM), the Personal Information must be encrypted in accordance with all applicable legal and regulatory requirements, including use of strong cryptography.

6. Supplier Security Measures. In accordance with generally accepted industry practices and the specific requirements set forth herein, Supplier (and Supplier Subcontractors) will establish and maintain at each Service Location Supplier Security Measures sufficient to meet or exceed these Data Security Requirements. Supplier will promptly notify Kaiser of any material changes to the Supplier Security Measures that may impact Supplier's provision of Secure Services. Without limitation of the foregoing, Supplier Security Measures will, at a minimum, include the following:

i. Information Security Policies: Supplier will establish and maintain information security policies and controls for the facilities, network, and systems at each Service Location that support the delivery of the Secure Services. Such information security policies will describe Supplier's information security requirements, responsibilities, roles, controls, and risk management practices pertaining to information protection, privacy, and site and internal security. Supplier will comply with such information security policies and will enforce compliance by all Supplier employees, agents and Supplier Subcontractors that support the delivery of the Secure Services.

ii. Physical Security: At each Service Location, the systems used to access, process and store Personal Information shall be operated in an environment equipped with 24-hour onsite security and monitoring, security alarm systems, and other reasonable measures designed to protect the security and integrity thereof. Supplier will have onsite staff on duty capable of identifying, categorizing, and responding to a physical security event.

iii. Access Controls: Supplier shall maintain access controls that prevent the unauthorized access, disclosure or use of Personal Information including, without limitation, the following access controls: (a) limiting access to systems supporting the delivery of Secure Services to authorized personnel who have a need for such access for purposes of providing the Secure Services; (b) limiting access to any Personal Information stored or processed on such systems only for such access as necessary in order to provide the Secure Services; (c) identifying and associating each action taken with respect to any Personal Information with the individual who performed such action and maintaining logs documenting such actions; (d) revoking all access privileges of any Supplier, employee, agent or Supplier Subcontractor that no longer has reason to access the systems supporting the Secure Services; and (e) tracing any action performed with a surrogate user account such as Root, Administrator or Service Account to Supplier personnel who have approved the use of such an account.

iv. Firewalls: Supplier will utilize hardware and software firewalls configured in accordance with industry standard practices to minimize the risk of unauthorized access to Personal Information.

v. Communication Protocols: The transfer, exchange or other communication of Personal Information requires Secure File Transfer Protocol (SFTP) or Secure Socket Layer (SSL) or similar secure mechanism. Strong authentication is required for any access initiated from outside the Kaiser network and may rely on devices, such as a VPN token or a certificate. All login streams (user ID and password) to systems on which Personal Information is stored must be encrypted, regardless of source or destination. All files sent by electronic transmission must be encrypted.

vi. Protection against Malicious Code: Supplier will not knowingly introduce any viruses, worms, Trojan horses, logic bombs, disabling code, or other malicious code into Supplier systems or data ("Malicious Code"). Supplier will implement reputable and industry standard virus detection/scanning program(s) to scan all files transmitted to Kaiser and all information systems used to provide the Secure Services. Supplier shall continuously update such virus detection/scanning program(s) for the detection, prevention, and recovery to protect against Malicious Code and will also implement appropriate user awareness procedures.

vii. Intrusion Detection: Supplier will deploy a monitoring system or service intended to detect and prevent against abnormal network traffic that would indicate a potential intrusion by unauthorized users for purposes of interrupting services or accessing data. The intrusion detection and prevention service along with other security systems (e.g., firewalls, anti-virus programs and the like) that generate security logs and events will be monitored 7x24 by knowledgeable Supplier security personnel. Appropriate procedures for dealing with an intrusion will be maintained and followed. System logs will be maintained for a minimum of one year.

viii. Data Encryption: Personal Information transferred from servers/systems that are vulnerable to outside sources are to be encrypted in transit and at rest (i.e., when stored) by Supplier. Users will only be permitted to connect to the systems that process or store Personal Information using secure web browsers supporting strong encryption.

ix. Back-Up Storage and Security: Supplier will have and maintain policies, processes, and for back-up of data containing Personal Information, image repositories and provisioned environments. The back-up storage infrastructure will be Supplier-owned or Supplier Subcontractor-owned equipment and media and will meet these Data Security Requirements. The back-up storage infrastructure will be located in physically protected, limited access facilities located within the United States and be governed by the access controls and other security measures as set forth herein.

x. Business Continuity Management: Supplier will have and maintain a documented disaster recovery plan. This disaster recovery plan should include detailed recovery procedures for all reasonably foreseeable disasters and other disruptions that may impact Supplier's performance of the Secure Services. In the event of a disaster, Supplier will endeavor to promptly restore such Secure Services and to comply with any work and/or data restoration deadlines included in any agreements between the parties. Supplier will periodically test its disaster recovery plan and procedures.

xi. 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 Data Security Requirements.

7. Security & Compliance Assessments. Prior to and during the performance of Secure Services, Kaiser may perform periodic evaluations and/or inspections of Service Locations and Supplier Security Measures to assess whether Supplier and Supplier Subcontractor(s) maintain information security controls appropriate to protect Personal Information and to identify, prevent, and mitigate any security breach in connection with the performance of Secure Services (each a "***Security Assessment***").

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

   a) Review of Supplier's and Supplier Subcontractor's control environment;
   b) Interviews of Supplier and Supplier Subcontractor personnel;
   c) If requested, Supplier's completion and return of Kaiser's security screening Questionnaire for Kaiser's review and approval. Supplier will also provide documentation to support its assertion of the security controls and measures in place. Thereafter, Supplier shall maintain the Supplier Security Measures as described in Supplier's response to Kaiser's Questionnaire during the performance of Secure Services or provide advance written notification to Kaiser of any material change thereto;
   d) On at least an annual basis, Supplier will engage a reputable third party assessor to perform a vulnerability assessment to identify any issues with configuration of firewalls, web services, servers and other system components that could result in access vulnerabilities. Supplier will provide reports and other results of such assessments to Kaiser upon receipt. Vulnerabilities within a Service Location that cannot be remediated in a timely fashion or for which remediation may have an adverse impact on Kaiser or the Secure Services must be promptly communicated to Kaiser's security personnel together with an identification of probable risks;
   e) In cooperation with Kaiser, Supplier will conduct appropriate testing of user access controls prior to implementation of such access controls;
   f) In cooperation with Supplier, Kaiser may perform security testing and verification of the Service Locations and Secure Services which may include application security vulnerability scanning, application penetration testing, static analysis, and/or manual code review.

ii. 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 Personal Information attributable to Supplier's performance of Secure Services, Kaiser may require more frequent Security Assessments and/or other actions or measures, including, without limitation, those set forth in the applicable agreement between the parties.

iii. Mitigation. If a Security Assessment results in a finding that Supplier Security Measures 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 or provide supplemental information sufficient to demonstrate that any perceived security risk that may negatively impact Supplier's protection of Personal Information or performance of Secure Services has been satisfactorily addressed by Supplier.

8. Independent Certification of Supplier's Controls.

i. Independent Certifications. If available, Supplier will provide Kaiser, on an ongoing basis each year, with copies of all independent, third-party certifications (each an "***Independent Certification***") of Supplier's applicable data security controls (e.g.; SSAE16, ISO, SOC 1, SOC 2,

etc.) that address all or a portion of the subject matter of these Data Security Requirements (e.g., information security, internal controls, privacy). 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 above.

ii. Frequency. 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 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.

9. Response to Security Incidents.

i. Notification to Kaiser. Supplier will notify Kaiser as soon as practicable but not longer than four (4) hours after discovering an actual breach or compromise of the security of Supplier's systems or Supplier Security Measures or any other unauthorized access that may have occurred with respect to Personal Information (each a "***Security Incident***") by calling the Kaiser National Compliance Hotline at 1-888-774-9100.

ii. Mitigation. Supplier will promptly conduct corrective actions in response to any Security Incident, including, if requested by Kaiser, shutting down all access to the systems in which any Personal Information is hosted or stored, and remediation to fully address the Security Incident.

iii. Investigation/Consumer Remedies. Supplier will promptly conduct an investigation of any Security Incident and submit an oral report of its findings to Kaiser immediately, to be followed by a written report as soon as practicable. Supplier will respond to reasonable requests from Kaiser for information regarding the Security Incident and will cooperate with Kaiser in connection with any incident management, including with respect to external and media relations, law enforcement activities, and notification to affected individuals. With respect to any Security Incident that arises in a Services Location, 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 s 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.