KAISER PERMANENTE®

PAYMENT CARD INDUSTRY REQUIREMENTS
FOR VENDORS, CONTRACTORS AND SUPPLIERS

Supplier will comply with the payment card industry requirements described below, if applicable.

A. Definitions:

"*Cardholder Data*" refers to the account number assigned by a payment card issuer that identifies the cardholder's account, plus any of the following, cardholder name, expiration date and/or service code or any other card verification value code ("*CVV*").

"*Confirmed Data Breach*" means a breach that is confirmed via a forensic audit conducted by an independent third party engaged and paid for by Supplier, and the results of such audit (which promptly shall be communicated to Kaiser) confirm that such breach has resulted from a breach of Supplier's systems.

"*Kaiser*" means Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, Kaiser Permanente Insurance Company, and the subsidiaries and successors of the foregoing.

"PCI DSS" means the Payment Card Industry Data Security Standards.

"*Supplier*" means a vendor, contractor or supplier who is providing goods or services to Kaiser.

B. Requirements:

If Supplier's services include processing, storing, using or transmitting payment Cardholder Data (other than CVVs or other security related information pertaining to a cardholder which may never be stored), then Supplier acknowledges and agrees that, in accordance with the rules of the payment card networks, and Supplier's acquiring bank and processor, Supplier will comply at all times with the requirements prescribed by the PCI DSS Council, which can be found at https://www.pcisecuritystandards.org/index.php.

Supplier is liable to Kaiser and to any third party claiming damages through Kaiser for all fees, costs, penalties and fines should a Confirmed Data Breach or incident occur involving Cardholder Data on the POS system, technology systems and/or broadband internet connectivity provided by Supplier.

C. Attestation:

If Supplier is required to meet the PCI DSS requirements (as described in Section B above), then it must provide Kaiser, on an annual basis, with an Attestation of Compliance* by a qualified PCI security assessor confirming Supplier's compliance with the PCI DSS requirements. Upon execution of the agreement between Kaiser and Supplier or attachment of this document to the agreement, Supplier shall immediately provide to Kaiser the most recent valid Attestation of Compliance.

*PCI-DSS v.3 Requirement 12.9 (and any later PCI-DSS version updating or amending such requirement) requires service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes or transmits on behalf of the customer, or to the extent they could impact the

security of the customer's cardholder data environment. On an annual basis, any third party service provider will provide a declaration of the service provider's compliance status with each of the PCI DSS requirements and security assessment procedures that apply to the services being provided. Supplier shall immediately notify Kaiser if it is not in compliance with any of the PCI-DSS requirements or security assessment procedures that apply to the services being provided.