KAISER PERMANENTE®

SECTION 16

HIPAA AND PRIVACY RULES

16.0 INTRODUCTION

Contracted providers may have signed a document that creates a business associate relationship with Kaiser Permanente, as such relationship is defined by federal regulations commonly known as “HIPAA” (defined below).

Once a provider signs an Agreement, they are a "covered entity" as that term is defined under HIPAA, and the Privacy Rule issued by the Department of Health and Human Services. As a covered entity, they have specific responsibilities to limit the uses and disclosures of personal health information (PHI), as that term is defined by the Privacy Rule (45 CFR Section 164.501).

Certain data which may be exchanged as a consequence of their relationship with Kaiser Permanente is subject to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-91) and its regulations (collectively, "HIPAA”). To the full extent applicable by the provisions of HIPAA, a provider must comply with HIPAA, including but not limited to the HIPAA standards for the following:

- Privacy
- Code Set
- Date Transmission Standards
- Security regarding physical storage, maintenance, transmission of and access to individual health info

A provider must use and disclose PHI only as permitted by HIPAA and the Privacy Rule, subject to any additional limitations, if any, on the use and disclosure of that information as imposed by the Agreement signed with Kaiser Permanente. Providers must maintain and distribute a Notice of Privacy Practices to members using their services. Providers must distribute their Notice of Privacy Practices (45 CFR Section 164.520) to and obtain acknowledgements from members receiving services from them, in a manner consistent with their practices for other members. Providers must give Kaiser Permanente a copy of their Notice of Privacy Practices and give Kaiser Permanente a copy of each subsequent version of their Notice of Privacy Practices whenever a material change has been made to the original Notice.

Providers are required by HIPAA to provide a member with access to his or her PHI, to allow that member to amend his or her PHI, and to provide an accounting of those disclosures identified under the Privacy Rule as reportable disclosures. Providers must extend these same rights to Health Plan members who are members. If a provider amends, allows a member to amend, or includes in records any statement of a member pursuant to HIPAA requirements, a copy of such item must be given to Kaiser Permanente.

16.1 ELECTRONIC COMMUNICATION OF PHI

As a “Covered Entity” or “Business Associate” as defined under HIPAA, Kaiser Permanente providers are responsible for limiting the use and disclosure of PHI.

PHI may be used for purposes of treatment, payment and health care operations, directly with the individual, and/or for a specified purpose with the member’s authorization.

A Kaiser Permanente provider’s violation of the use of Kaiser Permanente member’s PHI could undermine member trust in Kaiser Permanente and place the violator at risk for penalties under HIPPA as well as other laws. Suggestions for electronic communication of PHI are:

- Use a confidentiality statement when transmitting faxes or e-mail messages with PHI
- Presume any message sent over the internet is not secure and may be available to the public
- Double check the address line(s) before sending an e-mail message to make sure it’s going to the right party
- Don’t send messages containing ePHI to a distribution list unless it’s essential that all persons on the list require access to the information
- Password-protect attachments containing PHI and send the password in a separate email
- Always double check the fax number before sending a fax
- Check fax machines, printers and copiers frequently for paper PHI