KAISER PERMANENTE
HIPAA PRIVACY AND SECURITY TRAINING FOR REGISTRY PERSONNEL

Purpose:

The Health Insurance Portability and Accountability Act (HIPAA) requires health care professionals to obtain and complete training on both the federal HIPAA law and a health care organization's specific HIPAA policies and procedures. The purpose of this training document is to provide you with a basic understanding of HIPAA and Kaiser Permanente (KP) requirements for protecting the privacy and security of KP Member/Patient Identifiable Information (MPII) and Protected Health Information (PHI). Although you may have obtained HIPAA privacy and security training from another healthcare organization, you are responsible for reading and understanding this information about KP's privacy and security requirements and obtaining any additional information you need to comply with all laws and policies that affect the use and disclosure of MPII or PHI when you provide or coordinate health care services for a KP member or patient. If you have questions about what you must do or need additional information, consult with your supervisor, contract manager, your local Compliance Officer or your Regional Privacy and Security Officer. You can also access information at kp.org/compliance.

If you are aware of compliance, privacy or security issues or have concerns about a suspected violation of the law, you should notify your KP supervisor or call the KP Compliance Hotline: 1-888-774-9100.

Definitions:

HIPAA - (Health Insurance Portability and Accountability Act) requires all KP workforce members, regardless of job title or hours worked, to understand the risks and safeguard the privacy and security of individually identifiable information of KP members and patients.

MPII - (member patient identifiable information) is a term defined in KP policy and is any member/patient individually identifiable information that KP has received, collected, created, transmitted or maintained in connection with the individual's status as a KP member or patient. MPII includes financial data, credit card account numbers and PINs, and protected health information (PHI), but not health information in employment files. KP policy requires all KP workforce members, including contractors and vendors who work at a KP facility and act as workforce members, to protect the security of MPII in much the same way as HIPAA requires workforce members to protect PHI (see definition below).

PHI - (protected health information) is a term defined by HIPAA that covers an individual's past, present and future health care and health care payment information and includes one or more of 18 personal identifiers that individually identify a person—such as name, medical record number, address, e-mail address, telephone number, vehicle ID number, social security number, driver's license number, etc. The law and policy require you to protect all forms of PHI—written, spoken or electronic. For example, the law prohibits your accessing or discussing a member/patient's medical diagnosis unless it is required for your job and allowed by the law. PHI is a subset of MPII.

Individual Identifiers – any one or more of the following member/patient individual identifiers must be protected when used by KP: name, street or email addresses, birth date, deceased date, admission and discharge dates, telephone and fax numbers, Social Security Number, medical record or health record number, credit and banking account numbers, certificate/license number, driver's license and other vehicle identifiers, medical device numbers, URLs, biometric identifiers, full face photograph, any other unique identifying number or characteristic.

Workforce Members – according to HIPAA and KP policy, KP workforce members include all employees, volunteers, trainees or other persons who work for KP and who perform services on KP premises and are otherwise under the supervision or control of KP. For example, an individual who is a registry employee working at a KP medical center or clinic is a workforce member.

Five Privacy and Security Principles You Must Follow:

- **Never Assume**---that you have the right to use or disclose MPII/PHI just because you have easy access to the information.
- **Allowed or Required by Law**—you can only use or disclose MPII/PHI for purposes allowed or required by law.
- **Need to Know for Your Job**—you can only access, use or disclose MPII/PHI if you need it to do **your** job.
- **Minimum Necessary**—do not use, access or disclose more information than is needed to do your job—use the least amount necessary.
- **Do the Right Thing**—always treat MPII/PHI as if it were your own and a member/patient's most important possession.

Uses or Disclosures of MPII/PHI That Are Allowed or Required by Law

In general, HIPAA allows a KP workforce member to create, receive, access, use, or disclose MPII/PHI for the following purposes—but only if and when the individual's job duties includes these activities:

- **Health care treatment**—the treatment team can use MPII/PHI to provide, coordinate, or manage health care and related services. A health care professional can not use MPII/PHI for solely personal reasons—such as to check on the health care status of a colleague or friend UNLESS he/she is directly involved in the care of the patient, and therefore needs the information for treatment.
- **Health care or health plan payment** —MPII/PHI can be used for a variety of payment, billing, claims, and collection activities.
- **Health care or health plan operations**—MPII/PHI can be used for quality assessment, case management, accreditation, underwriting, legal and audit functions, and business management.

Uses or Disclosures of MPII/PHI Prohibited by Law and Policy

If a KP workforce member is not using MPII/PHI for treatment, payment, or operations, then in most cases KP must get a written authorization from the member/patient or remove all 18 personal identifiers or other information that could identify the individual. For example, if you are a health care allied professions student rotating at KP from another institution, you cannot use KP MPII/PHI for presentations or papers you prepare for your other school or educational institution. If you are a health care professional who is conducting a training session or presentation that is not directly related to the treatment provided on-site to the member/patient, then in most cases you cannot use MPII/PHI for those training purposes, including screen shots for PowerPoint presentations. You cannot use KP MPII/PHI if you are a lecturer at a conference for CME training. Always check with your manager before using any KP information in screen shots, PowerPoint presentations, or any materials that will be shared outside KP.

When you leave KP employment—as either a KP employee, vendor or contractor—you may not remove, make copies of or continue to use, access, receive, or disclose KP MPII/PHI. Doing so is a violation of the law and KP policy. If you are a contractor, you may not copy, use, or disclose KP MPII/PHI for any purpose other than specifically allowed in your Business Associate contract. If you accidentally access or disclose MPII/PHI in ways not allowed in your contract, you must immediately report the disclosure to your supervisor or contract manager. Deliberate misuse of MPII/PHI is a violation of law and policy.

Consequences for Failing to Comply with HIPAA or KP Policy

A failure to comply with the requirements of HIPAA or KP policy could result in loss of employment, termination of your contract, and legal sanctions, including fines, penalties, and imprisonment.