

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:

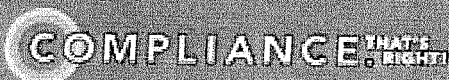
HIPAA - (Health Insurance Portability and Accountability Act) requires all KP workforce members, regardless of job title or hours worked, to understand the risks and safeguard the privacy and security of individually identifiable information of KP members and patients.

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.



Compliance Hotline 1-888-774-9100 • Compliance Online kp.org/compliance



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.



Privacy and Security Requirements

The following is a list of some of the safeguards you must implement to protect the privacy and security of MII/PHI:

► Think Twice When You Talk About MII/PHI

- Never tell others about MII/PHI unless allowed by law and required for your job. For example, never tell a friend, family member, or other employees about a KP member/patient's diagnosis or treatment unless it is for purposes allowed by law and required for your job.
- Lower your voice in public or avoid discussing MII/PHI in public areas, including when you use a cell phone where others may overhear.
- Close the door when consulting with patients and/or family members or when dictating your charts.
- Be sure to ask the patient in advance if it is acceptable to provide or discuss health care information with the member/patient's family members.

► Protect the Privacy of MII/PHI in Printed or Written Documents (e.g. the Medical Record)

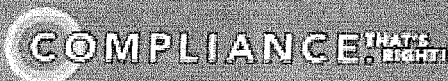
- Never access, use or disclose MII/PHI in a written document or file—e.g., a medical record—unless allowed by law and required by your job. For example, you cannot access a medical record of a friend, family member, or celebrity because you are simply curious about his/her health status.
- Never remove medical records from a KP facility without express approval from your supervisor. If you are permitted to transport copies of the medical record by car or other means, make certain the records are secure and protected in transit.
- Always double check the fax number before sending a fax. Use a coversheet with a confidentiality statement when transmitting faxes containing MII/PHI. Don't send faxes containing MII/PHI to a list of numbers unless you are certain that all recipients need to receive the information.
- Place machines that process MII/PHI in secure areas. Check fax machines, printers, copiers, and mailboxes frequently to retrieve MII/PHI.
- Cover, put away, or turn over paperwork with MII/PHI so that is not easily read by passersby.
- Use cabinets with locks to store medical records or other printed or written documents containing MII/PHI. Access to these areas should be limited to those individuals with designated rights of access.
- Use a confidential destruction bin or shredder when disposing of MII/PHI in documents, on labels, etc.

► Prevent Illegal Access to and Disclosure of Electronic MII/PHI with Strong Passwords

- Create complex passwords with a minimum of eight characters—at least one number and one letter. Use a mixture of capital and lower case letters. Do not use consecutive identical characters or all alphabetical groups or consecutive characters on the keyboard (e.g., aaaaaa, 111111, qwerty).
- Do not use actual words (e.g., Kaiser, password) or your individual identifiers as a password (names, driver's license number, social security number). Use clues, a phrase or a code to remind you of your password. For example, use your grandmother's middle initials and number of grandchildren.
- If you suspect your password has been compromised or misused, you should immediately change the password, and report the incident to your supervisor.
- If you share a workstation, only use your own password and logon ID to access data. Always log off when you are finished and at the end of the day. Never share your unique logon information with other users, or you could be held responsible if someone using your logon illegally accesses or discloses MII/PHI.

► Secure MII/PHI on Your Computer, Biomedical Equipment, Laptop, or Other Portable Devices

- Store and save MII/PHI on a secure drive so in the event the information is lost or stolen, you have



secured and backed up critical care or business data.

- Turn your computer screen away from viewing by visitors if you work in an open area. If MPII/PHI is frequently displayed on your screen, install a “privacy screen” to protect the display.
- You must obtain your supervisor’s approval to store MPII/PHI on any portable device, including laptops, PDAs, cell phones, jump drives, CDs, DVDs, etc. You can only store KP MPII/PHI on a portable device if it is for a purpose allowed or required by law and a part of your job function. If approval is granted, the mobile device must have encryption software installed prior to storing MPII/PHI. See National Policy: *NATLNCO PS 024, Secure Electronic Storage of Member/Patient Data* for more information.

► Provide Physical Security for Portable Computing and Storage Devices

- Know where your laptop and PDA are at all times. Never check them as baggage or leave unsecured.
- Make sure your laptop is secured by a locking cable, or securely locked in the docking station. If you’re leaving for the day, take the device with you or lock it in a desk or cabinet.
- Carry tokens and removable media separately from the laptop (don’t put them in the same case).
- If your device is stolen or lost, you must report the loss immediately to your supervisor. If the lost or stolen device contained MPII/PHI—encrypted or unencrypted—you must report the loss of the data immediately to your regional Privacy and Security Officer or Compliance Officer.

► Secure MPII/PHI in Email and Email Attachments

- Encrypt all e-mails containing MPII/PHI that are sent from an internal KP address (e.g., kp.org) to a non-KP.org external address (e.g., earthlink.net). If you use the “Email Your Doctor” secure messaging function or other similar provider to patient email functions, you do not need to encrypt because those functions employ other security controls.
- To encrypt an email, include any one of three “keywords” in the subject line. Put either parentheses or brackets around the word. A keyword can be capitalized or lower case:
 - PHI (phi), {PHI}, [phi]
 - MPII (MPII), [mpii], {MPII}
 - Encrypt (encrypt), {encrypt}, [ENCRYPT]
- Never open email messages or attachments from people you don’t know or can’t identify.
- Always double-check the address line(s) before sending an email message to make sure it’s going to the right party. If you send an email containing MPII/PHI to the wrong addressee, report the mis-mailing immediately to your supervisor and Privacy and Security Officer.
- Do NOT rely on the Lotus Notes functionality to accurately auto fill or auto-populate the address lines. Instead, use the Lotus Notes address book and select the name of each intended recipient.
- If you must use a distribution list to send MPII/PHI, verify the names on the list. Each individual must be allowed or required by law to receive an email containing MPII/PHI. Double-check any email address that is not within Kaiser Permanente’s email system.

► Prevent Illegal Access to Facilities and Secure Areas

- If you notice someone without a ID/card badge in a restricted access area, immediately notify Security. If you feel comfortable and safe doing so, direct the person to Security to get a temporary badge.
- Obtain an ID badge before entering a KP facility to begin your work.
- When you leave KP or are transferred to a job where your current ID badge will not be re-used, you are responsible for turning in your badge to your supervisor or HR.
- Do not post keypad access codes near doors, offices and workstations.

