HIPAA 101: Privacy and Security Basics

Purpose

This document provides important information about Kaiser Permanente (KP) policies and state and federal laws for protecting the privacy and security of individually identifiable member and patient information. You are responsible for understanding this information and any additional information you need to comply with all laws and policies that affect your job.

In most cases, you have received this information because you are a "limited time workforce member"—you work or volunteer at KP less than 160 hours/year. However, if your job description or contract requires you to routinely receive, access, create, use or disclose member and patient information, you must take additional privacy and security training. Contact your contract manager or supervisor immediately to enroll in KP General Compliance Training for New Employees web-based or instructor-led training for new employees.

What is HIPAA?

HIPAA – is the Health Insurance Portability and Accountability Act and 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 our members and patients.

What is PHI?

For information to be considered PHI, it must meet all of the following three conditions:

1. The information is created, received, or maintained by a health provider or health plan.
2. The information is related to past, present or future health care or payment for that health care.
3. The information identifies a member or patient, or there is enough information to be able to identify the individual.

Only health information about an individual that is linked to that individual by an identifier is protected health information.

Health information that is not linked to an individual by one or more of 18 HIPAA identifiers and for which there is no reasonable basis to believe that the information can be used to identify the individual is not protected health information.

Removal of all 18 HIPAA identifiers means the information is de-identified and no longer protected health.

Individually identifiable health information ceases to be PHI 50 years after death.

Individually identifiable information, even if not PHI, may still be subject to other state and federal privacy protections.

What Does This Mean to Me?

You are expected to be able to:

1. Recognize PHI that requires protection.
2. Determine when it is permissible to access, use or disclose PHI.
3. Reduce the risk of impermissible access to, use or disclosure of PHI.

When it is permissible to access or use PHI?

Only access, use or disclose PHI if your job allows you access and that access is required for your job.

What Uses or Disclosures of PHI Are Permitted by Law?

HIPAA allows a KP workforce member to create, receive, access, use, or disclose PHI without patient authorization when the workforce member's job duties involve certain activities. These activities include, but are not limited to:

- **Health care treatment**—the treatment team can use PHI to provide, coordinate, or manage health care and related services, including consultation between health care providers of an individual, and referral of a patient for health care from one provider to another provider for treatment. However, UNLESS the provider is directly involved in the care of the patient, and needs the information for treatment, a health care provider can not access, use, or disclose PHI for other purposes—such as to check on the health care status of a colleague or friend or family member, without the patient's specific authorization.
- **Health care or health plan payment** —PHI can be used for premium payment, billing, claims management, utilization review, coordination of benefits, eligibility and/or coverage determinations, and collection activities.
- **Health care or health plan operations**—PHI can be used for quality assessment, case management, population-based activities such as disease management, accreditation, underwriting, legal and audit functions, fraud and abuse protection and compliance, and business management.

There are other uses and disclosures where patient authorization is not required, including:

- **Appointment reminders** – PHI may be used to contact members and patients about appointments for health care and treatment.
- **Business Associates** – PHI may be used by KP's contracted business associates of a Kaiser Permanente regional Health Plan, hospital or of one of the regional Permanente Medical Groups to perform certain functions on KP's behalf. Business associates must sign a business associate agreement with the regional Health Plan or the regional Permanente Medical Group and agree to safeguard KP member and patient PHI.
- **Communications with family and others when the member or patient is present** - PHI may be discussed in the presence of a family member or other person involved in the member's or patient's care, but make sure the member or patient does not object.
- **Communications with family and others when the member or patient is not present -** PHI may be disclosed to a family member or other person involved in the member or patient's care when there is an emergency, the member or patient is not present, or the member or patient lacks the decision making capacity to agree or object to the disclosure. Use professional judgment to determine if it is in the member or patient's best interest to disclose their PHI to a family member, and limit the disclosure to the PHI that is directly relevant to the person's involvement with the member or patient's health care.
- **Marketing** - PHI can be used to contact members about KP benefits, and certain health-related products or services that add value to, but are not a part of, the plan of benefits offered to a KP member.

- **Facility Directories** – PHI can be used to create directories that include patient names, room locations, general medical conditions, and religious affiliation. Room location, and general medical condition may be disclosed to any person who asks for the patient by name. All of this information, including religious affiliation, may be disclosed to members of the clergy, if the patient has not restricted this disclosure. Patients have the right to object to the use and disclosure of some or all of this information; if so, KP will not disclose the information to visitors or other members of the public.

Other uses and disclosures require prior written authorization. If you are not sure about whether or not you can use or disclose PHI, check with your manager/supervisor, compliance officer, or privacy and security officer.

What Uses or Disclosures of PHI are Prohibited by Law and KP Policy?

- When you stop doing work for KP — either as a KP employee, vendor or contractor— you may not remove, make copies of or continue to use, access, receive, or disclose KP 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 PHI for any purpose other than specifically allowed in your Business Associate contract. If you inadvertently access or disclose PHI in ways not allowed in your contract, the law requires you to immediately report the disclosure to your supervisor or contract manager, and your company to report the breach to KP.

How Can I Help Prevent Breaches of PHI?

A breach is the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of the PHI. We are all responsible for protecting our members' and patients' confidential information. If a breach occurs, immediately notify your manager/supervisor, compliance officer, or privacy and security officer.

Do Not Peek

- No matter how curious you might be regarding the health of a coworker, a friend, a celebrity, or a family member, do not access a medical record unless you are authorized to do so.
- Never access or discuss a fellow employee's PHI unless it is for purposes allowed by law and required for your job

Think Twice When You Talk About PHI

- Do not discuss patient information at home or outside of work, including who you saw as a patient.
- Avoid discussing PHI in public areas, including talking on a cell phone where others may overhear.
- Lower your voice when you must share PHI in areas where others might overhear.
- If possible, close the door when consulting with patients and/or family members or when dictating.
- Be sure to ask the patient in advance if it is acceptable to speak with his or her family members.

Prevent Unauthorized Access to Facilities and Secure Areas

- When you are at work, wear your KP ID badge and be sure it is prominently displayed.
- Notify Security if you notice someone without an ID/card badge in a restricted access area. Ask the individual, "May I help you?" or "You seem to be lost", and then direct them to Security to obtain a temporary badge.
- Keep doors locked and restrict access to areas where sensitive information or equipment is kept.
- Do not post keypad access codes.
- Shield the key strokes when entering an access code to prevent others from seeing the code.
- Follow the same guidelines for facility access as you would for password, including changing codes periodically; using complex codes that are not obvious; not sharing your access code or access badge; and, not allowing others to use your access rights to enter a facility or secure area.
- Do not allow others to "tailgate", or follow you into a restricted area. Each employee must have a badge to enter restricted areas, or otherwise be directed to Security to obtain a badge.
- Turn in your badge and keys to your supervisor or HR when you leave KP, or are transferred to another KP job where your current ID badge will not be re-used.

Protect the Privacy of PHI in Printed or Written Documents

- Check to make sure that you are giving the correct paperwork to the right member or patient. Examples include after-visit summaries, discharge instructions, medication bottles or packages, and pharmacy inserts. Many incidents are paper related and preventable.
- Keep paper medical records out-of-sight, and in locked storage areas. Access to these areas should be limited to those individuals with designated rights of access.
- Always double check the fax number before sending a fax. Use a cover sheet with a confidentiality statement when transmitting faxes containing PHI.
- Place machines that process PHI in secure areas.
- Check fax machines, printers, copiers, and mailboxes frequently to retrieve PHI.
- Cover, put away, or turn over paperwork with PHI.
- Use cabinets with locks to store cameras, and printed or written documents containing PHI.
- Use a shredder or confidential destruction bin when disposing of PHI.
- When creating training and presentation materials, including screen shots, remove patient identifiers so the materials do not display PHI.

Prevent Unauthorized Access to and Disclosure of Electronic PHI

- Create complex passwords with a minimum of eight characters--at least one number, symbol and/or 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).
- Do not use your individual identifiers (names, driver's license number, Social Security number).
- If you suspect your password has been compromised or misused, you should immediately change the password, and report the incident to your supervisor.
- Do not share or post passwords or user IDs on your computer. If someone asks to use your password, report it to your supervisor.
- Use a password, and secure or lock your workstation, before stepping away and leaving it unattended for any period of time
- If you share a workstation, only use your own password and logon ID to access data. Log-off when you are finished. Never share your passwords with other users; you could be held responsible if an unauthorized person uses your logon or password to access or disclose PHI.
- Turn your computer screen away from viewing by visitors if you work in an open area. If PHI is frequently displayed on your screen, install a "privacy screen" to protect the display.

Provide Physical Security for Portable Computing and Storage Devices

- Store confidential information such as PHI on KP's secured network severs. **Never store PHI on a laptop or other portable, endpoint device unless you have specific approval from your supervisor and Regional Leadership.** If granted, the mobile device must have encryption software installed. If you have been approved to use and store PHI on a portable, end-point computing device— e.g., a laptop, PDA, cell phone, hand-held device, mp3 player, flash or jump drive, CD or DVD, etc.—you should obtain the Privacy and Security training that is required for all workforce members. See your supervisor or contract manager immediately about the training.
- Know where your portable devices (laptop, PDA, cell phone, hand-held device, mp3 player, flash or jump drive, CD or DVD, etc.) are at all times. Never check them as baggage or leave them unattended or unsecured at home, work, or in transit.
- Whenever you leave your work area, make sure your laptop is secured by a locking cable, or securely locked in the docking station.
- If you are leaving for the day, take the laptop or other device with you or lock it in a desk or cabinet.
- If your device is stolen or lost, immediately report the loss to your manager/supervisor.
- If the lost or stolen device contained PHI—encrypted or unencrypted—you must report the loss of the data immediately to your regional privacy and security officer or compliance officer.

Secure PHI in email and email Attachments

- Encrypt all emails containing PHI that are sent from an internal KP.org address to a non-kp.org external address (e.g., yahoo.net). Lotus Notes users can use the "Send Secure" function, which automatically encrypts the email message.
- If your Lotus Notes does not have the "Send Secure" button, you can encrypt an email by including any of the two "keywords" in the subject line, with either parentheses or brackets around the word. A keyword can be capitalized or lower case:
  - PHI (phi), {PHI}, [phi]
  - Encrypt (encrypt), {encrypt}, [ENCRYPT]
- Use Secure File Transfer to send large files securely to both internal and external addresses.
- Never open attachments in email messages from people you don't know or can't identify.
- Always double-check the address line(s) before sending an email message to ensure it's going to the right party. If you send an email containing PHI to the wrong addressee, report the mis-mailing immediately to your manager/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 PHI, verify the names on the list as each having a need to receive the email. Take a critical view of any email address that is not within Kaiser Permanente's email system.

Violating KP policies, federal regulations, and state laws and regulations can lead to disciplinary action – up to and including termination, personal fines, civil and criminal penalties and suspension of professional licenses

You are responsible for understanding this information and any additional information necessary to comply with all laws and policies that affect your job.

If you have questions about what you must do, consult with your supervisor, contract manager, local KP compliance officer or KP regional privacy and security officer. You can also access KP privacy and security information at kp.org/compliance.

Appendix – HIPAA Identifiers

"HIPAA identifiers" means any of the following identifiers, either of the individual or of his/her relatives, employers or household members:

- Names.
- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

- All date elements (except year) for dates directly related to an individual, including of birth date, an admission or discharge date, date of death; and all ages over 89 and any date (including year) indicative of such age, however such ages and elements may be aggregated into a single category of age 90 or older.
- Telephone numbers.
- Fax numbers.
- Email addresses.
- Social Security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- URLs.
- Internet protocol address numbers.
- Biometric identifiers including finger and voice prints.
- Full face photographic images and any comparable images.
- Any other unique identifying number, characteristic, or code (provided that (a) the code or other record identifier is not derived from or related to other information (for example scramble MRNs and SSNs are not permitted) and not otherwise translatable to identify the individual; (b) the covered entity does not use or disclose the code or other record identifier for any other purpose; (c) and the covered entity does not disclose the mechanism for re-identification.