



HIPAA 101

PRIVACY AND **SECURITY** **BASICS**

This document was created as a standalone training for the Kaiser Permanente workforce. Any additional uses of this document should be cleared with Privacy, Security and Technology Compliance.

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 work at Kaiser Permanente.

TABLE OF CONTENTS

LEARNING OBJECTIVES	4
WHAT IS HIPAA?	5
UNDERSTANDING THE IMPORTANCE OF PHI	5
WHAT IS CONSIDERED PHI?	6
WHAT DOES MINIMUM NECESSARY MEAN WHEN SHARING PHI?	6
CODE OF ETHICAL CONDUCT: KP's PRINCIPLES OF RESPONSIBILITY	8
DO THE RIGHT THING	9
KAISER PERMANENTE'S SOCIAL MEDIA POLICY (NATL.COMM.001)	9
ADHERE TO KP POLICIES AND COMPLIANCE REQUIREMENTS	10
PROTECT THE PRIVACY AND SECURITY OF PHI	10
• DO NOT ACCESS PHI WITHOUT A BUSINESS NEED	10
• THINK TWICE BEFORE DISCUSSING PHI	11
• PREVENT UNAUTHORIZED ACCESS TO FACILITIES AND SECURE AREAS	11
• PROTECT THE PRIVACY OF PHI IN PRINTED OR WRITTEN DOCUMENTS	11
• PREVENT UNAUTHORIZED ACCESS TO AND DISCLOSURE OF ELECTRONIC PHI	12
• SECURE PORTABLE COMPUTING AND STORAGE DEVICES	13
• SECURE PHI IN EMAIL AND EMAIL ATTACHMENTS	13
CONSEQUENCES OF THE VIOLATION OF KP POLICY AND THE LAW	14
KNOWLEDGE CHECK	15
KAISER PERMANENTE HIPAA TRAINING ATTESTATION OF COMPLETION (OPTIONAL)	17

LEARNING OBJECTIVES

1. Define HIPAA and demonstrate a clear understanding of its importance to the integrity of the organization.
2. Identify PHI and demonstrate an understanding of when it is permitted to access and/or disclose.
3. Understand the minimum necessary rule as it applies to both written and verbal disclosures.
4. Understand why taking photos and/or videos and posting on social media is not permitted.

WHAT IS HIPAA?

HIPAA is the federal **Health Insurance Portability and Accountability Act**. It is one of the governing laws that Kaiser Permanente must comply with to manage all day-to-day activities inside and outside of hospitals, medical office buildings (MOBs), and business offices. It requires all KP workforce, regardless of job title or hours worked which includes paid and volunteer personnel, to understand the risks and safeguard the privacy and security of individually identifiable information of our members and patients.

The HIPAA Privacy Rule requires covered entities, such as Kaiser Permanente, to:

- Protect health plan members' and patients' rights to the privacy and confidentiality of their own health information.
- Comply with the limits and conditions on the uses and disclosures of patients' protected health information.
- Abide by patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

UNDERSTANDING THE IMPORTANCE OF PHI

Protected health information (PHI), which is a subset of **personally identifiable information (PII)**, is individually identifiable health information, including a members/patient's name, address and/or residential information, date of birth (DOB), social security number (SSN), medical record number (MRN), or health record number (HRN). Refer to the 18 HIPAA identifiers that are listed in [What is PHI?](#)

PHI is information that is created, received, stored, or transmitted when KP provides any form of health care service, fulfills health care operations, or processes payment for health care services.

PHI may be in oral, written, or electronic form.

Name (Full/Partial)	Address (Full/Partial)	Date of Birth (DOB)	Telephone Number	Full Face Photo Image	Email Address	
Social Security Number (SSN)	Medial Record Number (MRN)	Health Record Number (HRN)	Any unique identification number	Biometric Identifiers (Voice or fingerprint)	Dates Associated with Services Rendered	

WHAT IS CONSIDERED 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.

Health information is “individually identifiable” when it reveals a person’s identity, or if there is a reasonable basis to believe that the information could be used to determine the person’s identity.

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

	You are expected to be able to: • Recognize PHI that requires protection • Determine when it is permissible to access, use, or disclose PHI • Reduce the risk of impermissible access to, use, or disclosure of PHI. Access, use, or disclose PHI only if it is required by your job.
---	--

WHAT DOES MINIMUM NECESSARY MEAN WHEN SHARING PHI?

The Minimum Necessary Rule protects the privacy and security of patients’ and members’ sensitive information. This means any PHI—oral, written, or electronic—that is shared among KP workforce members should be limited to the “need to know” details to avoid sharing it inappropriately.

HIPAA allows a KP workforce member to create, receive, access, use, or disclose PHI without patient authorization when there is a need based on a job requirement or activity related to patient health care. 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 cannot access, use, or disclose PHI for other purposes—such as to check on the health care status of a colleague, 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 KP 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, after assuring 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’s 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’s 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's or patient's health care.

- **Marketing** – PHI can be used to communicate information about a member/patient's alternative treatments, or health-related products or services that KP offers. KP may also ask for authorization in order to provide information about products and services that members or patients may be interested in purchasing or using.
- **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.

Note: There are other uses and disclosures that require prior written authorization. If you are not sure whether you can use or disclose PHI, check with your manager, local KP Compliance Officer, or Regional KP Privacy and Security Officer.

These are uses and disclosures that are prohibited by law and KP policy:

- When you stop doing work for KP—either as a KP employee, volunteer, vendor, or contractor—you may not remove, make copies of or continue to use, access, receive, or disclose PHI that belongs to KP.
- 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.

CODE OF ETHICAL CONDUCT: KP's PRINCIPLES OF RESPONSIBILITY

Kaiser Permanente is committed to providing high-quality, affordable health care services and to improving the health of our members, our patients, and the communities we serve. The [Code of Ethical Conduct: KP's Principles of Responsibility](#) supports this commitment.

The Code of Ethical Conduct: KP's Principles of Responsibility represents the following:

- It is our organization's ethical compass.
- It represents our workplace values.
- It guides our work and our interactions with others.

DO THE RIGHT THING

Whenever you need guidance on appropriate actions in your work setting or whenever your instincts tell you that something does not feel quite right you can refer to this information. If you encounter situations in your work environment that you are unsure how to address, talk to any of the following:

- Your immediate supervisor
- Another supervisor or manager in your area
- Local KP Compliance Officer
- Regional KP Compliance Officer



Note: Kaiser Permanente has a strict "non-retaliation" policy, meaning no negative actions or harm will come to an individual who reports unethical behavior. Reports made to a manager, supervisor, or through the [KP Ethics and Compliance Hotline](#) are confidential. Please speak to a manager on how to access these reporting channels.

KAISER PERMANENTE'S SOCIAL MEDIA POLICY ([NATL.COMM.001](#))



The purpose of this policy is to provide KP workforce members with clear information about the expectations of their behavior when they are using social media, including personal social media accounts, to the extent specifically stated in this policy. When employees, members, or the public raise concerns about social media content, KP reviews and responds to those concerns in accordance with the provisions of all KP policies.

Kaiser Permanente workforce who identify themselves as working at KP or who access social media through KP-owned devices will use social media in a manner that is consistent with KP policy and the [Code of Ethical Conduct: KP's Principles of Responsibility](#).

Prohibited Social Media Use

Member and Patient Confidentiality: Workforce members may not use or disclose PHI of any kind, including photographs and any other unique identifiers of any KP member or patient, on any social media without a written HIPAA-compliant authorization of the affected member or patient. Even if an individual is not identified by name, if there is a reasonable basis to believe that the member or patient could still be identified from that information, then its use or disclosure could violate HIPAA and KP policy.

ADHERE TO KP POLICIES AND COMPLIANCE REQUIREMENTS

All rules and KP policies that apply to other KP communications apply to Social Media communications. Employees are expected to comply with all KP policies, and the Code of Ethical Conduct: KP's Principles of Responsibility. Employees may not post any material about KP or KP members and patients, contractors, or suppliers, or other KP employees in a manner that reasonably could be viewed as obscene, threatening, or intimidating, or that violates KP's workplace policies against discrimination, harassment, retaliation, illegal activity, and/or threats of violence.

PROTECT THE PRIVACY AND SECURITY OF PHI

A breach is the unauthorized acquisition, access, use, or disclosure of PHI that compromises the privacy or security of PHI. We are all responsible for protecting our members' and patients' confidential information. **If a breach occurs or is suspected, immediately notify your supervisor, local KP Compliance Officer, or Regional KP Privacy and Security Officer.**

Understanding the importance of not disclosing a patients or members information is the first step in protecting the privacy and security of PHI. Best practices to help you remain aware and hold yourself accountable include:

- **DO NOT ACCESS PHI WITHOUT A BUSINESS NEED**
 - No matter how curious you might be regarding the health of an incoming patient, a peer, a friend, a celebrity, or a family member, do not access a medical record unless you are authorized to do so and it is required by your job.
 - Never access or discuss a fellow employee's PHI unless it is for purposes allowed by law and required by your job.

- **THINK TWICE BEFORE DISCUSSING 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.
 - If a private area is not available and you must use a public space, remember to lower your voice when discussing PHI to avoid other people from overhearing the conversation.
 - Always ask the patient in advance if it is acceptable to speak with his or her family members.
 - If possible, close the door or move to a private area when observing or participating in discussions with patients and/or family members.
- **PREVENT UNAUTHORIZED ACCESS TO FACILITIES AND SECURE AREAS**
 - When you are at work, wear your KP identification badge at all times and ensure that it is prominently displayed.
 - Notify Security if you notice someone without an ID/card badge in a restricted access area. Politely ask the individual, "How may I help you?", 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 security access codes.
 - Shield the key strokes when entering an access code to protect from code theft via shoulder surfing.
 - Follow the same guidelines for facility access as you would for password maintenance. Change codes periodically, use complex codes that are not obvious, do not share your access code or access badge, and do not allow other 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 their own 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 Human Resources when you leave KP or are transferred to another KP job where your current ID badge will not be reused.
- **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 (AVS), 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 individuals with assigned 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 paper work with PHI.
- Use cabinets with locks to store printed or written documents containing PHI.
- Use a confidential destruction bin when disposing PHI.
- When creating training and presentation materials, including screenshots, remove patient identifiers.

Employees should only take KP work files and printed documents home if the process has been approved by the employee's manager and the employee understands and has agreed to the accountability and required safeguarding of the files with or without protected health information. Employees must also follow documented processes to ensure appropriate security of the data at all times in addition to retention and destruction requirements.

Printing PHI to a personal printer while working remotely is **prohibited** unless an exception has been granted through the Information Security policy exception process. A policy exception may be obtained from Technology Risk Office by submitting a [TRO Engagement Request](#). You may print to a personal printer without an exception as long as the document does not contain PHI.

For more security measures while working remotely, refer to [Security at Work](#).

- PREVENT UNAUTHORIZED ACCESS TO AND DISCLOSURE OF ELECTRONIC PHI

- Create a complex password with a minimum of twelve characters—at least one number, one upper case letter, one lower case letter, and one special character is recommended. Do not use consecutive identical characters.
- Use passphrases because they are longer, more complex, and more difficult to crack and less vulnerable to compromise.

- Do not use your individual identifiers (e.g., name, driver's license number, social security number)
- If you suspect your password has been compromised or misused, report the incident immediately to your supervisor.
- Do not share or post passwords or user IDs on your computer. If someone asks to use your password, report the incident to your supervisor.
- Secure or lock your workstation before stepping away. Do not leave your workstation unattended for any period of time without first securing or locking it.
- If you share a workstation, only use your own password and user 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 credentials to access or disclose PHI.
- Turn your computer screen away from viewing visitors if you work in an open area. If PHI is frequently displayed on your screen, install a privacy screen to protect the display.
- **SECURE PORTABLE COMPUTING AND STORAGE DEVICES**
 - Store confidential information, such as PHI, in KP secure network servers. **Never store PHI in a laptop or other portable, endpoint devices 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, endpoint computing device (e.g., laptop, PDA, cell phone, hand-held device, MP3 player, USB drive, CD, DVD), you should take the [HIPAA Privacy and Security Rules Training](#) in KP Learn.
 - Know where your portable devices 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 is otherwise securely locked.
 - If you are leaving for the day, take your laptop and other portable devices with you, or lock them in a desk drawer or cabinet.
 - If your portable device is stolen or lost, immediately report the incident to your supervisor. If the lost or stolen device contains PHI—encrypted or not—you must immediately report the loss of the data to your supervisor, local KP Compliance Officer, or Regional KP Privacy and Security Officer.
- **SECURE PHI IN EMAIL AND EMAIL ATTACHMENTS**
 - Encrypt all emails containing PHI that are sent to an external non-KP address. Include one of the following at the end of the Subject line separated with a

space between the Subject text and one of these encryption tags: (phi) (PHI) [phi] [PHI] (encrypt) (ENCRYPT) [encrypt] [ENCRYPT]. For example, do this "Subject text (PHI)" instead of "Subject text(PHI)".

- Place the encryption tag at the end of the Subject line to activate the encryption function. This ensures that a Reply or Forward email will continue to retain the encryption tag **at the end of the Subject line.**
- **Do not use the Encrypt function in Outlook.**
- Use Secure File Transfer (SFT) to transmit files containing sensitive information even when the data exceeds the 25MB limit in the standard Outlook encrypted email. SFT works exactly like email. Simply visit <https://sft-kw.kp.org/> and click "Compose" to create your message.
- Never open attachments in an email message from people you do not know or cannot identify.
- Always double-check the address line(s) before sending an email message to ensure it is going to the right party. If you send an email containing PHI to the wrong addressee, immediately report the mistake to your supervisor, local KP Compliance Officer, or Regional KP Privacy and Security Officer.
- Do not rely on the functionality of the Outlook email system to accurately auto-populate address lines. Instead use the 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 to ensure each recipient has a need to receive the email. Take a critical view of any external non-KP email address.
- **Do not send confidential business information, PHI, or PII to a personal email address,** even if the email is encrypted during transmission.

CONSEQUENCES OF THE VIOLATION OF KP POLICY AND THE LAW

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 all 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 your Regional KP Privacy and Security Officer at <https://pstc.kp.org/privacy-and-security/officers/>.

KNOWLEDGE CHECK

1. What does HIPAA stand for?

Health Insurance Portability and Accountability Act

2. What is the definition of PHI?

Protected health information (PHI) is personally identifiable health information, including demographic information that is created, received, stored, or transmitted in relation to the provision of health care, fulfillment of health care operations, or processing of payment for health care services. PHI may be in oral, written, or electronic form.

3. What are the three conditions that must be met to be considered PHI?

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

4. Give 5 examples of HIPAA identifiers.

- a. Name
- b. Medical Record Number
- c. Social Security Number
- d. Date of Birth
- e. Address (full/partial)

5. What is the Minimum Necessary Rule?

Any PHI that is shared among KP workforce members should be limited to the “need to know” details, regardless of form—oral, written, or electronic.

6. What does the Code of Ethical Conduct: KP’s Principles of Responsibility represent?

1. It is our organization's ethical compass.
2. It represents our workplace values.
3. It guides our work and our interactions with others.

7. You are allowed to make a social media post that shares details of a patient interaction that you were a part of or observed as long as you exclude the patients name.

True/False

8. What are 7 actions that you can take to protect the privacy of PHI?
1. Do not access PHI without a business need
 2. Think twice before discussing PHI
 3. Prevent unauthorized access to facilities and secure areas
 4. Protect the privacy of PHI in printed or written documents
 5. Prevent unauthorized access to and disclosure of electronic PHI
 6. Secure portable computing and storage devices
 7. Secure PHI in email and email attachments

KAISER PERMANENTE HIPAA TRAINING ATTESTATION OF COMPLETION (OPTIONAL)

If you are reviewing this HIPAA training material on your own, you must complete the following information and submit this document to the person in charge of your assignment no later than _____

(To be filled in by supervisor)

I have received and read a copy of Kaiser Permanente HIPAA 101 Privacy and Security Basics document.

I understand that I am responsible for reading this packet and asking questions if I do not understand the content.

Name (Printed): _____

Signature: _____

Date: _____

Month/Day/Year

Circle one: **student** **agency worker** **volunteer** **contractor**

School or Agency: _____

City and State: _____

School Instructor or Agency Contact Person: _____

KP Department: _____

Facility: _____

KP Department Supervisor: _____