



# 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.

This document provides important information about Kaiser Permanente 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 ability to work at Kaiser Permanente.

## TABLE OF CONTENTS

<b>LEARNING OBJECTIVES</b> .....	4
<b>ADDITIONAL RESOURCES</b> .....	4
<b>WHAT IS HIPAA?</b> .....	5
<b>UNDERSTANDING THE IMPORTANCE OF PHI AND PII</b> .....	5
WHAT IS CONSIDERED PHI/PII?.....	6
WHAT DOES MINIMUM NECESSARY MEAN WHEN SHARING PHI/PII?.....	6
<b>KAISER PERMANENTE’S PRINCIPLES OF RESPONSIBILITY (POR)</b> .....	7
DO THE RIGHT THING.....	7
KAISER PERMANENTE’S 5 GUIDING PRINCIPLES.....	7
<b>KAISER PERMANENTE’S SOCIAL MEDIA POLICY (NATL.COMM.001)</b> .....	9
ADHERE TO KP POLICIES AND COMPLIANCE REQUIREMENTS.....	9
<b>PROTECTING THE PRIVACY OF KP PATIENTS AND MEMBERS</b> .....	10
• DO NOT PEEK; “CURIOSITY KILLED THE CAT”.....	10
• THINK TWICE BEFORE DISCUSSING PHI/PII.....	10
• PREVENT UNAUTHORIZED ACCESS TO WORKSPACES.....	11
• PROTECT THE PRIVACY OF PHI IN PRINTED OR WRITTEN DOCUMENTS.....	11
<b>KNOWLEDGE CHECK</b> .....	12
<b>KAISER PERMANENTE HIPAA TRAINING ATTESTATION OF COMPLETION</b> .....	14

## LEARNING OBJECTIVES

1. Define HIPAA and demonstrate a clear understanding of its importance to the integrity of the organization.
2. Identify PHI/PII 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.

## ADDITIONAL RESOURCES


1. <https://www.cdc.gov/phlp/publications/topic/hipaa.html>
2. <https://www.youtube.com/watch?v=gmu86igu93w>
3. <https://www.thejobnetwork.com/using-social-media-as-a-health-care-professional/>
4. <https://careertrend.com/facts-7289412-professionalism-health-care.html>

## WHAT IS HIPAA?

**HIPAA** is the federal **Health Insurance Portability and Accountability Act**. It is one of the governing laws that Kaiser Permanente uses to manage all day-to-day activities inside and outside of hospitals, medical office buildings (MOBs), and business offices. Regardless of job title or hours worked, is important to understand the risks of not following this law. Therefore, it is a priority to 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.

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	

## UNDERSTANDING THE IMPORTANCE OF PHI AND PII


**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). This information 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 verbal, written, or electronic format.

## WHAT IS CONSIDERED PHI/PII?

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

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

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. 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.

	<p>Individually identifiable information, even if not PHI, may still be subject to other state and federal privacy protections. You are expected to:</p> <ul style="list-style-type: none"> <li><b>Recognize</b> PHI that requires protection</li> <li><b>Determine</b> when it is permitted to access, use, or disclose PHI</li> <li><b>Reduce</b> the risk of accidental or improper access to use or disclose PHI.</li> </ul>
---	--

## WHAT DOES MINIMUM NECESSARY MEAN WHEN SHARING PHI/PII?

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

By law, 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.**

**Note:** Other uses and disclosures require prior written authorization. If you are not sure whether to disclose PHI, speak immediately with your supervisor or manager before discussing or releasing information.

## KAISER PERMANENTE'S PRINCIPLES OF RESPONSIBILITY (POR)

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 Principles of Responsibility supports this commitment.

The Principles of Responsibility is Kaiser Permanente's code of conduct:

- 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 doesn't feel quite right you can refer to this information. If you encounter situations in your work environment that aren't addressed by the Principles of Responsibility, talk to any of the following:

- Your immediate supervisor
- Another supervisor or manager in your area



## KAISER PERMANENTE'S 5 GUIDING PRINCIPLES

These guiding principles are intended to make it easier for you to do the right thing at work. They are at the heart of who we are and what we stand for. Keeping these guiding principles in mind when you do your job should make it easier for you to follow the standards of conduct in the Principles of Responsibility and help us continue to make Kaiser Permanente an organization of which we are proud to be a part.

1. Improve Our Members' and Patients' Health and Wellness and the Nation's Health Care
  - Our cause is health. Our passion is service. We work to make lives better
  - We deliver compassionate, personalized, and proactive care to our members and patients.
  - We act to improve the access, delivery, and funding of health care for the communities we serve.

- We share our knowledge and innovations through research, our support of education for community health professionals and consumers, and by helping to inform public policy.
2. Excel and Innovate in Our Professions
    - We always strive to learn. We are dedicated to raising our own standards and the standards of our professions through continuous learning, performance improvement, research, training, adoption of new technology, and investment in state-of-the-art facilities.
    - We deliver care and services through teamwork because it is through collaboration with others that we can be most effective.
    - We strive to be responsible stewards of the environment and provide health care services in a manner that protects the environment now and for future generations.
  3. Respect Members, Patients, Customers, and One Another
    - When caring for our members and patients and serving our customers, we strive to act with courtesy, in a careful and considerate manner, and with professionalism.
    - We protect the privacy of our members and patients and respect their autonomy, customs, and beliefs. We involve them in decisions regarding their treatment and care according to their preferences.
    - We understand that we thrive when we respect one another. We are proud of our collegial environment, which honors diversity and inclusion
    - We listen to and respect the opinions of others, even when our views differ.
  4. Be Fair and Honest
    - We know that we must earn our distinguished reputation every day and understand that each health care and business decision is an opportunity to demonstrate our commitment to ethics and integrity.
    - We recognize the trust others place in us and recognize the responsibility of upholding that trust by being truthful and honest—always.
  5. Demonstrate a Commitment to Compliance and Ethics
    - Compliance means we fully adhere to federal, state, and local laws and regulations; federal health care program requirements; licensing requirements; accreditation standards; and requirements of the Centers



for Medicare & Medicaid Services and federal, state, and customer contracts.

- We never retaliate against those who, in good faith, report suspected violations of laws, accreditation standards, and Kaiser Permanente policies.
- Acting with ethics and integrity in our work means that we always try to do the right thing and make the best decisions, and that we seek help when the right thing or the best decision is not clear.

**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 can be confidential. Please speak to a manager or additional information 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 employees with clear information about KP’s 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 employees 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 *Principles of Responsibility (POR)*, KP’s Code of Conduct.

## 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 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.

### **Prohibited Social Media Use**

**Member and Patient Confidentiality:** Employees 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 the Health Insurance Portability and Accountability Act (HIPAA) and KP policy.

## **PROTECTING THE PRIVACY OF KP PATIENTS AND MEMBERS**

Understanding the importance of not disclosing a patients or members information is the first step. Additional best practices to help you remain aware and hold yourself accountable include:

- **DO NOT PEEK; "CURIOSITY KILLED THE CAT"**

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, or it is required for your job. Doing so may result in immediate termination and/or additional legal action.

- **THINK TWICE BEFORE DISCUSSING PHI/PII**

The action of discussing private and/or sensitive patient information is not allowed during your time of employment with Kaiser Permanente as well as once your term and/or job duties have ended.

- Never discuss patient information at home or outside of work, including who you may have seen as a patient.
- Do not discuss PHI in public areas, including talking on a cell phone where others may overhear.
- Always ask the patient in advance if it is acceptable to speak with his or her family members.

- Close the door or move to a private area when observing or participating in discussions with patients and/or family members.
- 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 overhearing the conversation.

- **PREVENT UNAUTHORIZED ACCESS TO WORKSPACES**

It is important to keep the KP form of identification that is given to you on hand and for it to be always visible while you are at the facility. If you are serving in restricted areas do not open doors or allow access to anyone. KP Personnel have badges that will provide them access to secured spaces. This helps keep KP equipment and member and patient information secure.

- Do not allow others to “tailgate”, or follow you into a restricted area
- Keep doors locked and restrict access to areas where sensitive information or equipment is kept.
- 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.

- **PROTECT THE PRIVACY OF PHI IN PRINTED OR WRITTEN DOCUMENTS**

In the event you are working in a space that has printed or written material or you are required to take notes, remember to keep sensitive material locked up. If you must throw anything away, be sure to use the proper disposal options such as a locked shred bin. Always double check to make sure that you are giving the correct paperwork to the right member or patient. Examples of written material may include after-visit summaries (AVS), discharge instructions, medication bottles or packages, and pharmacy inserts.

- Keep paper medical records out-of-sight, and in locked storage areas. Access to these areas is limited to individuals or personnel who have the proper credentials for restricted and/or employee only areas.
- When sending information outside of KP, double check that it’s the correct information and that the email, fax, or mail label is for the right person.
- Always check printers to confirm PHI/PII isn’t left out by mistake or mixed in with other documents.

**Note:** It is **never acceptable** to take printed or written PHI/PII material home. PHI in any form must always remain in a designated KP location. If printed material containing PHI/PII leaves a KP facility, you must **report it immediately to your manager or supervisor**.

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

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?

This means any PHI that is shared amongst KP workforce members should be limited to the "need to know" details only. This is regardless of it being in written or verbal format.

6. What is Kaiser Permanente's 5 guiding principles?

1. Improve Our Members' and Patients' Health and Wellness and the Nation's Health Care
2. Excel and Innovate in Our Professions
3. Respect Members, Patients, Customers, and One Another
4. Be Fair and Honest
5. Demonstrate a Commitment to Compliance and Ethics

7. You 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 four actions that you can take to protect the privacy of patients and members?
  1. Do not peek; "curiosity killed the cat"
  2. Think twice before discussing PHI/PII
  3. Prevent unauthorized access to workspaces
  4. Protect the privacy of phi in printed or written documents

## KAISER PERMANENTE HIPAA TRAINING ATTESTATION OF COMPLETION (OPTIONAL)

If you are reviewing 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: \_\_\_\_\_

Supervisor of KP Department: \_\_\_\_\_