

ANNUAL COMPLIANCE TRAINING

SELF-STUDY PARTICIPANT GUIDE



Warning: You are required to meet with your supervisor, manager, or designated training administrator, to review the answers to the self-check questions and to fill out the course completion and course evaluation forms.

Version Control

Date	Version	Description
11/14/2016	1.0.0	This version was released to the regions on January 2, 2017.

CONTENTS

Welcome	2
Required Meetings.....	3
A Message From the Chief Compliance and Privacy Officer	4
The <i>Principles of Responsibility</i> Attestation.....	5
Module 1: Compliance Basics	6
Module 2: Protecting Confidential Information	23
Module 3: Preventing Fraud, Waste, and Abuse.....	44
Module 4: Your Compliance Role	67
Module 5: Summary and Completion.....	82

WELCOME

Kaiser Permanente is deeply committed to a culture of compliance, ethics, and integrity; it's the way we do business. To support that commitment, this course provides a refresher of the top privacy and information security and fraud risks for 2017, and how to report compliance concerns appropriately.

All existing employees and supervisors (and physicians, students, interns, vendors, and contractors as determined by regional compliance officers) of Kaiser Foundation Hospitals and Health Plan (KFH/HP); KFH/HP's subsidiaries and affiliates; and non-physician employees of California Permanente Medical Groups may take this course to meet their 2017 annual compliance training requirement.

This self-study guide provides the required course materials and activities that meet the annual compliance training requirement for 2017. If the content in this course is difficult for you to understand, please contact your manager.

Note: If you are a new employee, you must take the *General Compliance Training for New Employees 2017* course; this annual compliance training will not fulfill your training requirement.



Warning: Do not take this training for someone else.

You must complete your own compliance training. If you complete this training for someone else or have someone do it for you, you will both be subject to disciplinary action, up to and including termination.

REQUIRED MEETINGS

There are two required meetings for using the self-study materials to meet the annual compliance training requirement.

MEETING 1 — SET EXPECTATIONS

The purpose of the first meeting is to receive the self-study materials and understand the following expectations:

- You will review all of the self-study materials.
- You will complete all of the self-check questions.
- You will fill out a course completion form.
- You will have an opportunity to provide feedback.

MEETING 2 — VALIDATE COMPLETION OF TRAINING REQUIREMENTS

The purpose of the second meeting is to validate that you, the self-study learner, have met the training requirements and that you get credit for taking the training.

To do this, meet with your supervisor, manager, or designated training administrator to review your responses to the self-check questions and fill out the course completion form. Be sure to sign both the course completion and the *Principles of Responsibility* attestations in his or her presence. You will also have the opportunity to provide feedback on the course evaluation form.



Vanessa M. Benevides
Senior Vice President
Chief Compliance and Privacy Officer

At Kaiser Permanente, our brand is our reputation and that reputation is built on trust. From the earliest days in the shipyards, to the complex, fast-paced health care world of today, it's our collective responsibility to ensure that Kaiser Permanente remains a high-trust, high-reliability, values-based organization.

This course is part of our robust compliance program and it's designed to equip you with the tools and resources you need to build and maintain trust, and to effectively deliver on our mission.

While you are taking this course, consider each scenario in the context of your day-to-day job, think about the impact of your behaviors and decisions. It's simple: Do your words and your actions build trust, or do they degrade trust?

By embracing our *Principles of Responsibility*, understanding and adhering to our policies, and reporting compliance concerns, you reflect KP's high standards of excellence and help promote a culture of trust, inclusion, and dedication.

Each of us has a responsibility to serve the best interests of our members and patients, our customers, and the communities we serve. Your participation makes living up to this responsibility achievable.

Thank you.

THE PRINCIPLES OF RESPONSIBILITY ATTESTATION

The *Principles of Responsibility* is the formal code of conduct that all KP workforce members must follow. As you have learned before, the *Principles of Responsibility* emphasizes the importance of honesty, integrity, and ethical behavior at Kaiser Permanente.

You are required to have read the *Principles of Responsibility* before you take this course. If you have not read it, find it on the National Compliance, Ethics & Integrity Office website and read it before you continue. It will take approximately 30 minutes to review. If you have questions about it, ask your supervisor for clarification.

To review the *Principles of Responsibility* and related materials, see:
<https://wiki.kp.org/wiki/display/por/Home>

THE PRINCIPLES OF RESPONSIBILITY ATTESTATION STATEMENTS

When you complete your attestation, you are agreeing that you've read and agree to be accountable for complying with all of the statements in the *Principles of Responsibility* attestation.

Because you are taking the self-study version of the course, your required attestation is included on your course completion form. If you have any questions about the attestation statements, discuss them with your supervisor during your follow-up meeting when he or she validates your completion of the training requirements.

Review the following *Principles of Responsibility* attestation statements.

- I have received and read a copy of the *Principles of Responsibility*.
- I understand that I am expected to conduct myself in an ethical and responsible manner in compliance with the *Principles of Responsibility* at all times. I also acknowledge my failure to comply with these principles can result in disciplinary action, up to and including termination.
- I understand that I am also required, in good faith, to report any suspected compliance concerns, including fraud, waste and abuse I become aware of, and that I am protected from retaliation for reporting wrongdoing.
- If I have any questions, I will seek clarification from the compliance and ethics resources listed in the “Know How to Get Help” chapter.

Yes, I attest to the above statements.

MODULE 1: COMPLIANCE BASICS

INTRODUCTION

At Kaiser Permanente, we manage risks through clearly defined policies and procedures, and through compliance services — such as audits and investigations — which help find and correct infractions.

The Federal Government requires us to have a chief compliance officer, effective training, and a code of conduct. We have a system for reporting wrongdoing and a non-retaliation policy, so it's easier for you to report anything that doesn't seem right and know that you're protected for doing so.

When something does go wrong, there are consequences. We must correct it and take appropriate action to prevent a repeat, and we may need to notify regulators or members.

Compliance is like fastening your seatbelt. Should you ever be in an accident, your seatbelt is there to help protect you.

Let's take a closer look at the role of compliance at Kaiser Permanente. We'll cover how our compliance program operates, how violations should be reported, and what happens when a concern is reported.

WHAT IS AN EFFECTIVE COMPLIANCE PROGRAM?

The Centers for Medicare & Medicaid Services (CMS) requires that we implement and maintain an effective compliance program for its Medicare Parts C and D plans.

An effective compliance program should:

- Articulate and demonstrate an organization's commitment to legal and ethical conduct.
- Provide guidance on how to handle compliance questions and concerns.
- Provide guidance on how to identify and report compliance violations.

CMS expects us to apply their training requirements and “effective lines of communication” to our FDRs. Having “effective lines of communication” means we have several avenues to report compliance concerns.

FDR

FDR stands for "First-tier, downstream, or related entity."

Each of The Permanente Medical Groups is considered an "FDR" or "First-Tier, Downstream, or Related Entity." This is a term coined by CMS used to identify entities contracted by Medicare Plan Sponsors to provide administrative or health care services for Medicare enrollees under the Medicare Part C and/or D plan.

What is an effective compliance program?

An effective compliance program fosters a culture of compliance, ethics, and integrity within an organization and, at a minimum:

- Prevents, detects, and corrects non-compliance
- Is fully implemented and is tailored to an organization's unique operations and circumstances
- Has adequate resources
- Promotes the organization's standard of conduct
- Establishes clear lines of communication for reporting non-compliance

An effective compliance program is essential to prevent, detect, and correct Medicare non-compliance as well as fraud, waste, and abuse.

OUR COMPLIANCE PROGRAM REQUIREMENTS

CMS requires that an effective compliance program must include these seven core elements.

Element	Description
<p>1. Written Policies, Procedures, and Standards of Conduct</p>	<p>These articulate our commitment to comply with all applicable federal and state standards and describe compliance expectations according to the <i>Principles of Responsibility</i>.</p>
<p>2. Compliance Officer, Compliance Committee, and High-Level Oversight</p>	<p>We must designate a compliance officer and a compliance committee that will be accountable and responsible for the activities and status of the compliance program, including issues identified, investigated, and resolved by the compliance program. Senior management must be engaged and exercise reasonable oversight of our compliance program.</p>
<p>3. Effective Training and Education</p>	<p>This covers the elements of the compliance plan as well as prevention, detection, and reporting of fraud, waste, and abuse. This training and education should be tailored to the different responsibilities and job functions of employees.</p>
<p>4. Effective Lines of Communication</p>	<p>We must have effective lines of communication that are accessible to all. In addition, these lines must ensure confidentiality, and provide methods for anonymous and good-faith reporting of compliance issues.</p>
<p>5. Well-Publicized Disciplinary Standards</p>	<p>We must enforce standards through well-publicized disciplinary guidelines.</p>
<p>6. Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks</p>	<p>We must conduct routine monitoring and auditing of KP's operations to evaluate compliance with CMS requirements as well as the overall effectiveness of the compliance program.</p> <p>Note: We also must ensure that FDRs each of the Permanente Medical Groups performing delegated administrative or health care service functions for KP's Medicare Parts C and D program comply with Medicare program requirements.</p>

<p>7. Procedures and System for Prompt Response to Compliance Issues</p>	<p>We must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.</p>
---	--

HOW DO YOU KNOW WHAT'S EXPECTED OF YOU?

How do you know what's expected of you in a specific situation? Refer to the *Principles of Responsibility*, our code of conduct. The *Principles of Responsibility* presents compliance expectations and the principles and values by which we operate.

Everyone has a responsibility to report violations and suspected non-compliance. The *Principles of Responsibility* also explains how to report suspected non-compliance.

You must conduct yourself in an ethical and legal manner. It's about doing the right thing!

- Act fairly and honestly.
- Adhere to high ethical standards in all you do.
- Comply with all applicable laws, regulations, and CMS requirements.
- Report suspected violations.

Ethics: Do the Right Thing!

THE PRINCIPLES OF RESPONSIBILITY AT A GLANCE

The *Principles of Responsibility* provides guidance over ten sections.

Section	Description
<p>1. Do the Right Thing</p>	<p>Section 1 describes the role of the <i>Principles of Responsibility</i>, who it applies to, basic compliance and ethics expectations, and the program's basic guiding principles.</p> <p>Lastly, this section provides definitions of terms used throughout the <i>Principles of Responsibility</i>.</p>
<p>2. Respect Confidentiality, Privacy, and Security</p>	<p>Section 2 focuses on complying with and meeting confidentiality, privacy, and security laws, regulations, and expectations.</p>

<p>3. Focus Resources on Member and Patient Care</p>	<p>Section 3 focuses on fraud, waste, and abuse prevention and detection. This helps us provide affordable health care and protects our members. You must not participate in fraudulent activities and you must report potential fraud if you become aware of it.</p>
<p>4. Support Community Involvement</p>	<p>Section 4 describes Kaiser Permanente’s social mission to promote the health and well-being of the communities we serve and it provides guidance about situations where disclosure is required.</p> <p>Your involvement in the community is encouraged.</p>
<p>5. Protect Our Assets and Information</p>	<p>Section 5 sets forth the standards for using Kaiser Permanente assets. This section addresses the use of physical assets and information systems, handling of confidential information and KP funds, and record management and retention practices.</p> <p>Kaiser Permanente assets are for health care and business purposes only.</p>
<p>6. Protect Our Reputation</p>	<p>Section 6 covers organizational expectations when physicians, dentists, and employees engage in external communications as representatives of Kaiser Permanente.</p> <p>Anyone who communicates to the public or professional organizations on behalf of KP must have authorization.</p>
<p>7. Treat One Another with Dignity and Respect</p>	<p>Section 7 focuses on the work environment at Kaiser Permanente: diversity, workplace safety, environmental sustainability, fostering a harassment-free environment, and non-retaliation principles.</p> <p>We do not tolerate intimidation, retaliation, or harassment. We keep our workplace safe by reporting work-related injuries and environmental hazards.</p>

<p>8. Avoid Conflicts of Interest</p>	<p>Section 8 addresses situations in which conflicts of interest can arise at Kaiser Permanente.</p> <p>Conflicts of interest occur anytime relationships or personal financial interests influence, or might reasonably appear to influence, your ability to make an objective and fair decision based solely on what is best for KP and the members and patients we serve.</p>
<p>9. Meet Government Expectations and Cooperate with Government Inquiries</p>	<p>Section 9 speaks to Kaiser Permanente interactions with government agencies and government expectations.</p> <p>Inform your chief, supervisor, or compliance officer when a government official contacts you.</p>
<p>10. Speak Up if You Have Any Questions or Concerns</p>	<p>Section 10 re-emphasizes Kaiser Permanente’s non-retaliation policy and the ability to report anonymously to the Compliance Hotline.</p> <p>Report potential compliance issues to or discuss questions with your chief, immediate supervisor, HR, compliance officer, or union steward or representative.</p>

The *Principles of Responsibility* in Action

As we've noted, the *Principles of Responsibility* guides everything we do. When caring for our members and patients and serving our customers, we strive to act in a careful and considerate manner, with courtesy and professionalism.

Let's take a look at this in action.





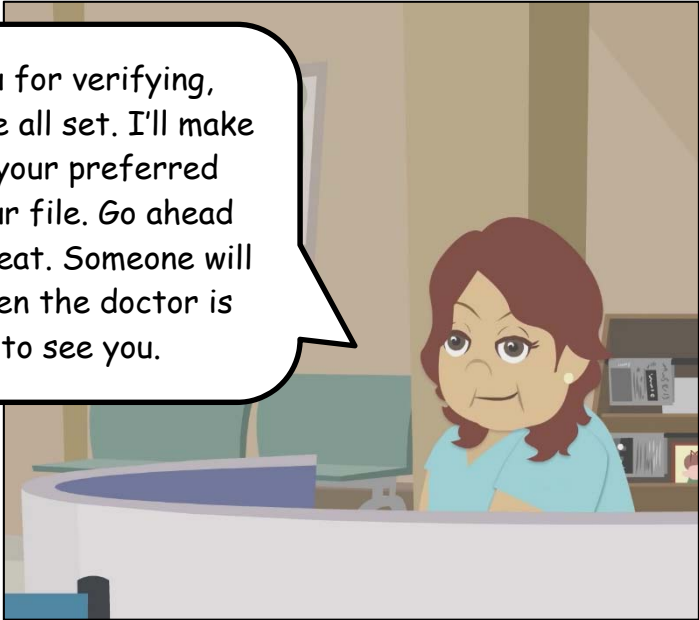
I've never seen a man come in for a Pap test before, but I'll treat him like any other member.

I'm sorry, but the medical record number is pulling up a different first name. Is Scott your preferred name?

The name I was given at birth is Sylvia Westin, but I go by Scott.



Thank you for verifying, Scott. You're all set. I'll make a note of your preferred name in your file. Go ahead and have a seat. Someone will call you when the doctor is ready to see you.





As described in section 7 of the *Principles of Responsibility*, Treat One Another with Dignity and Respect, we know that it's a privilege to serve a diverse population. We understand that we thrive when we respect one another.

A transgender person who identifies as a woman should be called "she." Likewise, a transgender person who identifies as a man should be called "he." Some people don't identify as male or female and may wish to be referred to using gender neutral pronouns like "they," "them," "xe," or "xim."

If you're not certain of someone's gender, it's appropriate to respectfully ask for a preferred name and pronoun.

Something as simple as using the preferred name and pronoun demonstrates our respect for our members and colleagues.

MORE INFORMATION

Use the *Principles of Responsibility* as a guide to ensure that compliance is integrated into the work you do every day — be it service, care, or any operational duties, such as planning, communications, and business processes.

The *Principles of Responsibility* applies to everyone. They are our rules of the road.

Refer to the *Principles of Responsibility* whenever you need guidance on what's appropriate at work or when your instincts say something's not quite right.

Section 10, Speak Up if You Have Any Questions or Concerns, provides a complete list of compliance community resources.

Access the pdf copy of the *Principles of Responsibility* and related materials:

<https://wiki.kp.org/wiki/display/por/Home>

WHAT IS NON-COMPLIANCE?

Non-compliance is conduct that doesn't conform to the law, federal health care program requirements, or an organization's ethical and business policies.

High Risk Areas for Non-Compliance

CMS identified the following as high risk areas:

- Agent/broker misrepresentation
- Appeals and grievance review (for example, coverage and organization determinations)
- Beneficiary notices
- Conflicts of interest
- Claims processing
- Credentialing and provider networks
- Documentation and timeliness requirements
- Ethics
- FDR oversight and monitoring
- Health Insurance Portability and Accountability Act (HIPAA)
- Marketing and enrollment
- Pharmacy, formulary, and benefit administration
- Quality of care

For more information, refer to the Compliance Program Guidelines in the "*Medicare Prescription Drug Benefit Manual*" and "*Medicare Managed Care Manual*" on the CMS website.

Know the Consequences of Non-Compliance

Failure to follow Medicare program requirements and CMS guidance can lead to serious consequences including:

- CMS contract termination
- Criminal penalties
- Exclusion from participation in all federal health care programs
- Civil monetary penalties

Additionally, we must have disciplinary standards for non-compliant behavior. Those who engage in non-compliant behavior may be subject to any of the following:

- Mandatory training or re-training
- Disciplinary action
- Termination
- License loss

Non-Compliance Affects Everyone

Because you provide health or administrative services for Kaiser Permanente, every action you take potentially affects you, your co-workers, our members and patients, and our reputation.

When we follow Kaiser Permanente's compliance standards, we provide better quality care. We also protect our patients, our colleagues, our jobs, and KP's name.

Without programs to prevent, detect, and correct non-compliance, we all risk harm to beneficiaries, such as:

- Delayed services
- Denial of benefits
- Difficulty in using providers of choice
- Other hurdles to care
- Less money for everyone, because of:
 - High insurance copayments
 - Higher premiums
 - Lower benefits for individuals and employers
 - Lower Star ratings
 - Lower profits

KP'S DISCIPLINARY GUIDELINES

We're all expected to abide by applicable federal, state, and local laws or regulations, to comply with Kaiser Permanente (KP) policies and procedures, and to conduct ourselves in accordance with KP's *Principles of Responsibility*.

If an employee fails to comply with any of these, the employee may be subject to corrective or disciplinary action, up to and including termination.

Kaiser Permanente's disciplinary guidelines for fraudulent and non-compliant behavior are well documented in Corrective/Disciplinary Action NATLHR014. For example, if an employee backdates a document, a manager can find information to help determine the level of discipline necessary to address the incident.

Access a PDF copy of the discipline policy:

<http://npl.kp.org/pl/do/public/record?rgid=900&subcatid=5661&VIEW=M&rid=10032601>

COMPLIANCE CONCERN REPORTING OPTIONS

Compliance issues relate to laws, regulations, and policies that direct how we do our jobs or provide our services.

When issues go unresolved, they can affect your work, your relationships, and your ability to provide outstanding care; everyone can suffer. Your goal should be to resolve the issue efficiently.

Review the following ways to report compliance issues.

Local Management

Your supervisor or another local manager are usually the best resources to contact with your compliance concerns. He or she will understand the situation and be able to address it efficiently. If you're new to the organization, ask your manager or supervisor who you should contact if he or she isn't available.

Compliance Resources

Your local compliance officer or hospital compliance officer is a resource for more complex issues and concerns, such as if your concern involves your immediate supervisor. To locate your local compliance resource, you can consult the National Compliance website or ask your manager to introduce you.

KP Compliance Hotline

The KP Compliance Hotline is a resource for all employees, physicians, and dentists, and can be accessed by phone or online (call 1-888-774-9100 or click [reportlineweb/kp](#)). The hotline is operated by a third-party vendor, and you may report anonymously.

Members can call 1-800-Medicare or contact Member Services.

WHEN YOU REPORT, YOU'RE PROTECTED

If you report a regulatory compliance or fraud issue in good faith, you'll be protected. Your input is important to us, and we'll keep your concern as confidential as possible. If you wish, you can report confidentially and anonymously by using the KP Compliance Hotline (call or click).

All Kaiser Permanente employees, physicians, and dentists are covered by the whistleblower protections in the federal False Claims Act and other federal and state whistleblower laws, as well as KP's Non-Retaliation policy. KP does not tolerate any retaliation against any employee, contractor, volunteer, physician, or dentist for making a good faith report of possible wrongdoing. Workforce members who retaliate against individuals who report or refuse to participate in violations of law, regulations, policies, or the code of conduct are subject to disciplinary action, up to and including termination.

Access a pdf copy of What Happens When You Call the KP Compliance Hotline:

https://sites.sp.kp.org/teams/Ina/ProductResources/General%20Compliance%20Training/ACT2017/GC_ACT_2017_WHWYCKPH_sp.pdf

WHAT HAPPENS ONCE NON-COMPLIANCE IS DETECTED?

Once non-compliance has been detected, it must be promptly corrected. Correcting the problem saves the government money and ensures KP is in compliance with CMS requirements.

Internal monitoring and audits should continue to ensure:

- No recurrence of the same non-compliance
- KP maintains ongoing compliance
- Efficient internal controls are in place
- Members are protected

What Are Internal Monitoring and Audits?

Internal monitoring activities are regular reviews that confirm ongoing compliance and ensure that corrective actions are undertaken and effective.

Internal auditing is a formal review of compliance with a particular set of standards (for example, policies and procedures, laws, and regulations) used as base measures.

MODULE 1: SELF CHECK

Instructions: Select the best answer(s) for each question.

Question 1:

Which of the following statements about the *Principles of Responsibility* are true?

Select all that apply.

The *Principles of Responsibility*:

- A.** Applies to every employee at Kaiser Permanente.
- B.** Addresses conflicts of interest.
- C.** States that you need to know and follow the laws, regulations, and policies that apply to you and your job.
- D.** Emphasizes Kaiser Permanente's non-retaliation policy.

Question 2:

Correcting non-compliance _____.

Select all that apply.

- A.** Protects members and patients
- B.** Helps avoid recurrence of the same non-compliance
- C.** Ensures bonuses for all employees
- D.** Saves the government money
- E.** Promotes efficiency

Question 3:

True or false?

Local management is usually the best resource to address a compliance concern quickly and effectively.

Select the best answer.

- A.** True
- B.** False

Question 4:

True or false?

At a minimum, an effective compliance program includes four core elements.

Select the best answer.

- A. True
- B. False

Question 5:

What are some of the consequences for non-compliance, or fraudulent, or unethical behavior?

Select all that apply.

- A. Disciplinary action
- B. Termination of employment
- C. Exclusion from participation in all federal health care programs
- D. License loss

Question 6:

Ways to report a compliance issue or possible fraud, waste, or abuse are:

Select all that apply.

- A. Call the KP Compliance Hotline.
- B. Report online.
- C. Report to your supervisor.
- D. Report to your local compliance officer or hospital compliance officer.

SUMMARY

As you can see, our compliance program is comprehensive and can only be successful with cooperation from people like you. We've earned the trust of members, patients, and our partners by maintaining an unwavering commitment to our mission to provide high-quality, affordable health care services, and to improve the health of our members, patients, and the communities we serve.

To help ensure compliance, behave ethically and follow the *Principles of Responsibility*. Watch for common instances of non-compliance, and report suspected non-compliance.

Compliance Is Everyone's Responsibility

- Prevent: Operate within Kaiser Permanente's ethical expectations to prevent non-compliance.
- Detect & Report: If you detect potential non-compliance, report it.
- Correct: Correct non-compliance to protect members and patients and save money.

MODULE 2: PROTECTING CONFIDENTIAL INFORMATION

INTRODUCTION

Can you imagine having your credit card information stolen? The pain and embarrassment of having your protected health information hacked? Your Social Security Number lost? Data theft is a terrible experience, and one we want to prevent.

At Kaiser Permanente, we safeguard a large amount of confidential data, including protected health information (PHI), financial information, and other sensitive data. We work hard at it because we want to keep our members, patients, and colleagues safe.

Some of the risks to our data are everyday challenges. Others are potentially headline worthy situations. This module will help you identify the different categories of confidential information and prepare you to minimize compliance risks. By developing good habits, we can reduce our data risk.

HIPAA AND KP'S NOTICE OF PRIVACY PRACTICES

HIPAA is a federal law that protects and enhances the rights of consumers by providing access to their health information and preventing inappropriate use of that information. HIPAA privacy regulations require every KP region to provide its members and patients with a Notice of Privacy Practices (NPP).

The NPP describes how health plan and medical (and dental) health information may be used and disclosed, and how members and patients can get access to their own information.

KP's responsibilities include:

- Protect the privacy of PHI.
- Tell members and patients about their rights and our legal duties with respect to their PHI.
- Notify members and patients if there is a breach of their PHI.

Access your region's NPP online:

https://healthy.kaiserpermanente.org/health/care/consumer/center/lut/p/a1/dU3BCoJAFPwaj_Fe iqbdNEh2pSyK0r3EJost6LrYw_DvM6NjAwMzzDADAgOQRg66lqQ7I5uPF8Fty095kixjzP3cR7bz04gHex c3K7gCB1E33X0ulw8iu3bQwZe1VWdIGaomqt5BEF9lZKugsL0eZDUuniRJtVMwLYn5DD12nM_SQ4DI wuycXaLMQ3R_hT-IEWwbjh7q-A3Yi_F2/dl5/d5/L2dBISEvZ0FBIS9nQSEh/

SAFEGUARDING CONFIDENTIAL INFORMATION

You can safeguard confidential information by paying attention to your surroundings and concentrating on the task at hand.

Secure Area

Secure areas contain medical records or other confidential information. They can include entire floors with restricted access or secured rooms within a public area.

To minimize risk:

- If you don't have a job-related reason to enter a secure area, don't enter.
- If you see the door open to a secure area, close it and report it to your supervisor.
- If an unauthorized person is in a secure area, approach them and offer help.
- If you unlock something, lock it when you're finished with your task.

PCs and Laptops

Workstations are high-risk areas when it comes to confidential information. Others shouldn't be able to see the information on your monitor while you're working.

To minimize risk:

- Lock your computer screen when you're away from your workstation.
- Use a privacy screen on your computer if it's in view of other people.
- Secure documents and approved electronic media (DVDs, CDs, thumb drives, etc.) in a locked drawer when not in use.
- Don't let anyone use your user ID and password.

KP Portable Devices

Do you use a camera, phone, tablet, or other portable device? Lock it in a drawer. A lost device can expose confidential information.

You must get approval before you can store confidential information on any portable device. Failure to get approval can lead to disciplinary action, up to and including termination.

To minimize risk:

- Never leave portable devices that contain confidential information unattended.
- Use a cable to secure your laptop.

- Don't share KP portable devices such as tablets and smartphones with co-workers, friends, or family.

Shared Resources

Fax machines, printers, filing cabinets, and photocopiers pose a risk to confidential information. In these busy environments, it's easy for someone to pick up a document they are not intended to see.

To minimize risk:

- When you fax patient information, double-check the recipient's number.
- Use a cover sheet that contains a confidentiality statement.
- Take your master copies with you after copying them.
- Promptly pick up faxes and copies from the tray.

Shared Confidential Information

HIPAA minimum necessary requirements state that when you access, use, or disclose PHI, only access, use, or disclose the minimum necessary information to accomplish the intended purpose.

To minimize risk:

When working with confidential information, determine the least amount you need, and work with that. If you're unsure, check with your supervisor or manager.

Also, purge copies of unneeded sensitive information when done.

Information Disposal

Be sure to dispose of confidential information properly.

To minimize risk:

- Follow national, regional, and local policies to dispose of both paper and electronic confidential information.
- Use designated document destruction bins to dispose of PHI in paper form and other confidential information.
- If you discover confidential information where it shouldn't be, report the incident to your supervisor immediately.
- Don't use paper from the workplace, printed PHI, or confidential information to make scrap paper or confetti.

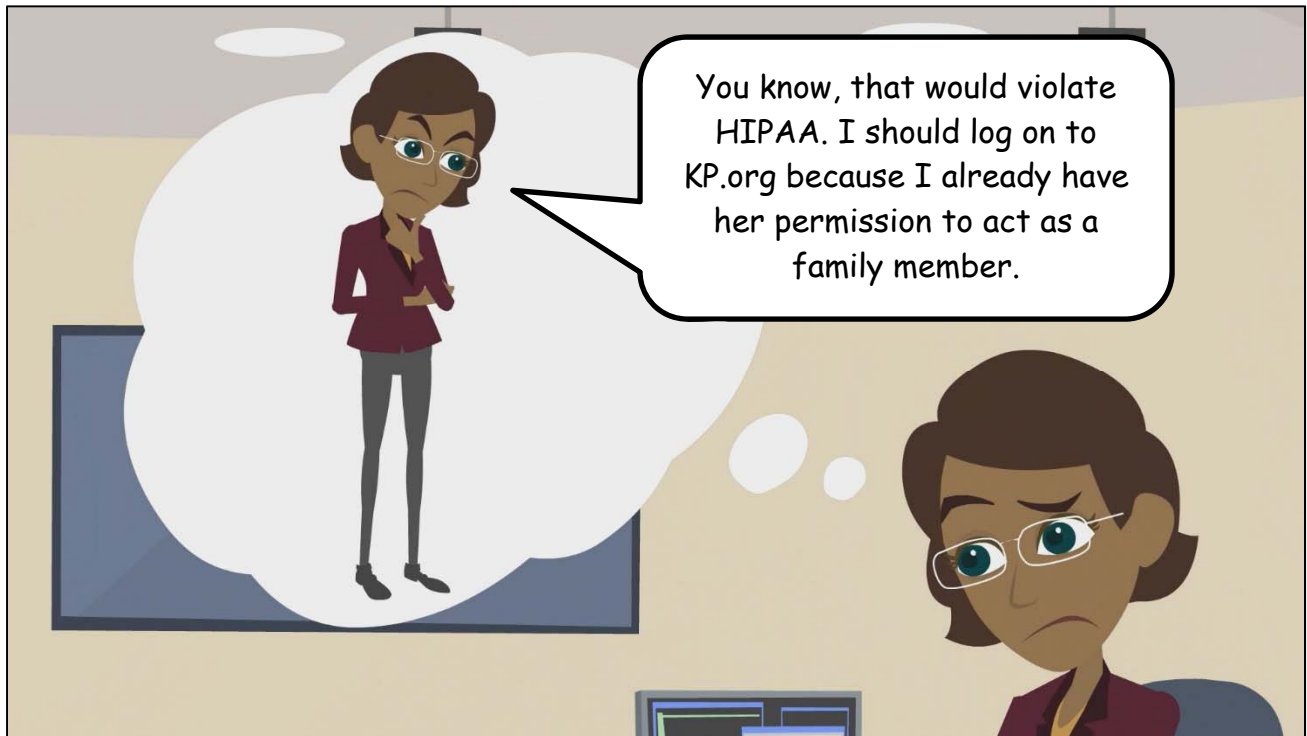
MANAGING RISK IN THE REAL WORLD

In your job, you may be faced with ethical and practical challenges when dealing with data. It's vital that our members' privacy and security is your first priority.

Remember, you're not alone – we face the same challenges, and we're stronger when we face them together.

Scenario





Question

Which system should Margaret use to get information?

Select the best answer.

- A.** KP HealthConnect
- B.** KP.org with her daughter's permission.

Feedback

The best response is B.

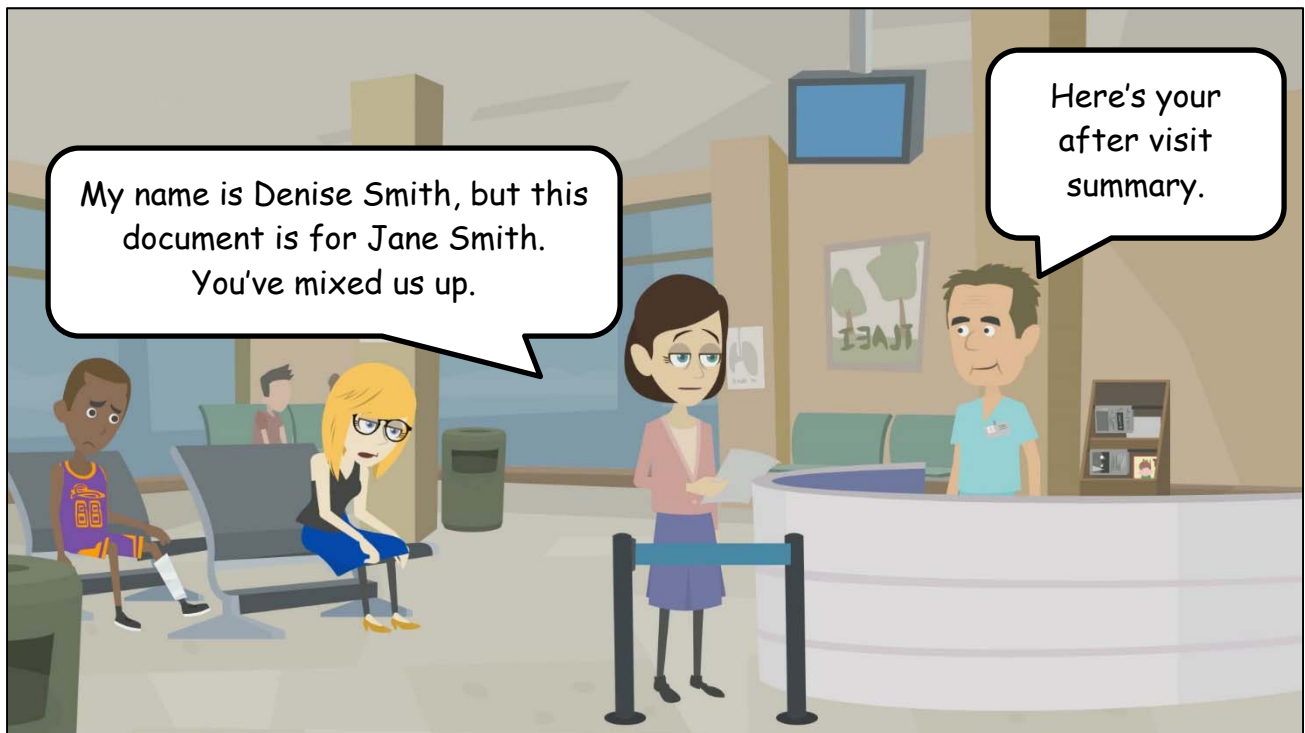
Margaret shouldn't use KP HealthConnect® for personal reasons; it's a business tool for job-related purposes only.

If you need to help a family member, use kp.org, once you've set up Act for a Family Member with the member's permission.

KP.org is a tool that members use to access their medical information – you can use it to manage your own care online, or, with proper authorization, the care of another person.

Accessing, using, or disclosing confidential information you don't need to do your job may have severe consequences. You could lose your job, your license, and your ability to practice your profession. You could even face penalties and jail time.

Scenario



Question

Which of the following steps would ensure that the AVS is in the right member's hands?

Select all that apply.

- A.** Use more than one type of information about a person to verify identity.
- B.** Ask the patient to state his or her name, and then check the name and MRN against the document before handing it over.
- C.** Call the member's name and look for recognition.

Feedback

The best responses are A and B.

Always use more than one identifier to avoid a distribution error. AVSs and hospital discharge instructions include member PHI — handing out the wrong document can hurt our members. It can also hurt Kaiser Permanente, because it could be a HIPAA violation. It may need to be reported to state and federal agencies and we could face penalties and damage to our reputation.

Scenario



Question

Alejandra has accidentally acted in a way that is non-compliant with HIPAA. What should she do?

Select the best answer.

- A.** She should talk to her supervisor immediately.
- B.** Wait and see if anyone notices.

Feedback

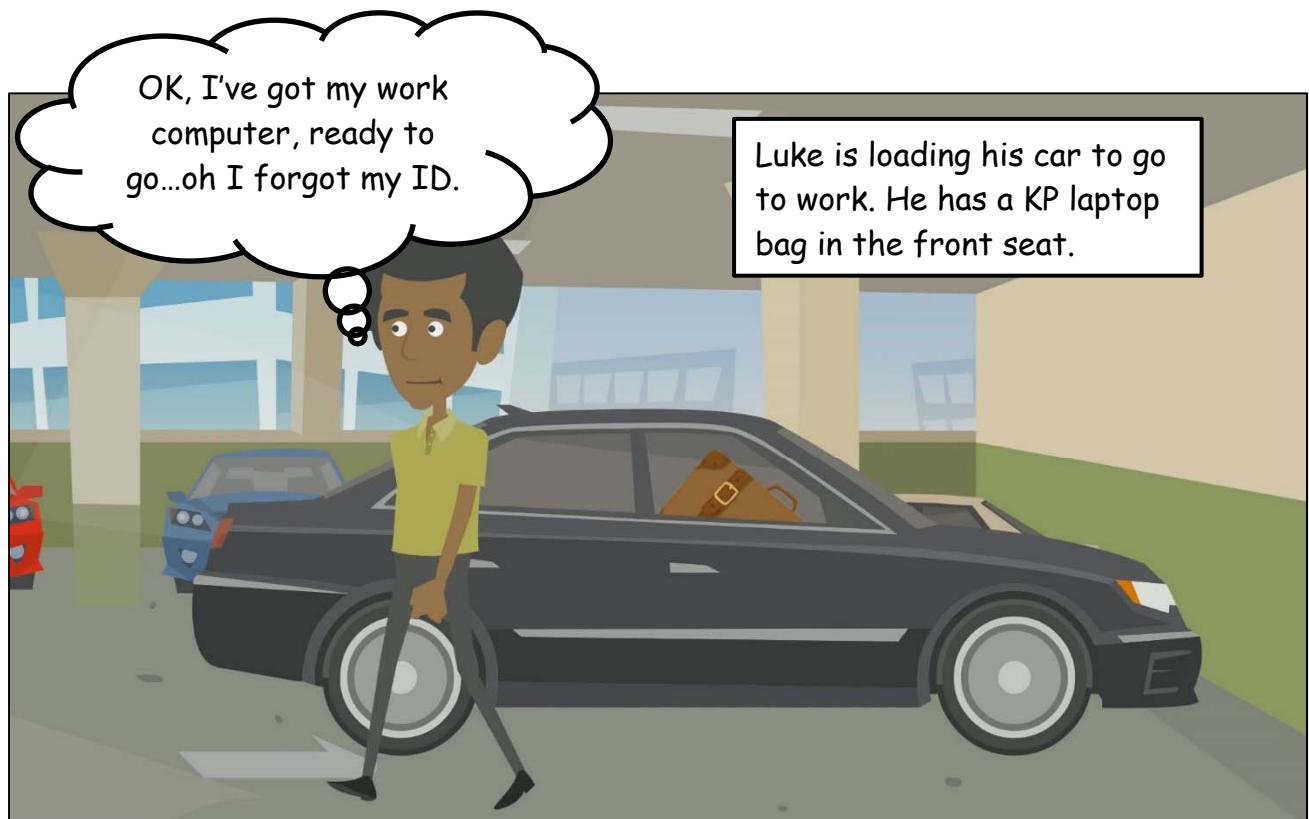
The best response is A.

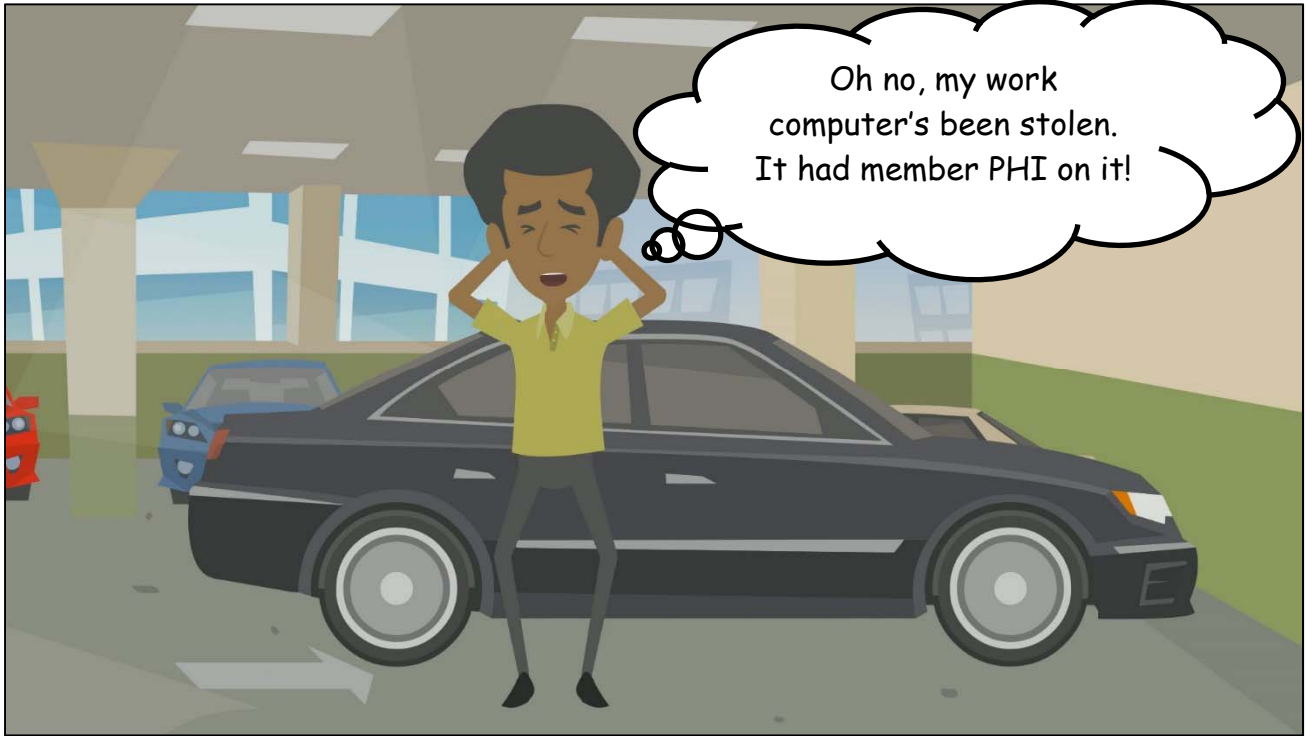
Alejandra should talk to her supervisor as soon as possible about this accidental disclosure of PHI.

Take care to share only the least amount of PHI that is necessary to accomplish the specific task or intended purpose.

Some email systems have a function to recall messages. If you mistakenly send an email to internal recipients, check to see if you can recall the email.

Scenario





Question

What could have prevented this from happening?

Select all that apply.

- A.** Never leave a KP computer unattended.
- B.** Place the computer in the trunk and out of sight.

Feedback

The best responses are A and B.

Either of these actions can help prevent laptop theft.

When commuting with a laptop:

Store it out of sight, keep your badge and token in a separate location, and encrypt files with PHI.

CONFIDENTIAL INFORMATION AT KP

Another component of our successful compliance program is how we handle confidential information. Confidential information (oral, written, or electronic) includes protected health information (PHI), personal information, KP business information in any format, and payment card information.

Protected Health Information (PHI)

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

1. The information is created, received, or maintained by a health provider or health plan.
2. The information is related to 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.

Personal Information

Personal information is any information about an individual maintained by an organization, including any information that can be used to distinguish or trace an individual's identity. Personal information can include PHI but is also more broadly defined.

Employment-related personal information is personal information when used for any employer human resources purpose such as recruitment, compensation, benefit management, or performance management.

Some states, including California, require notification to regulators and affected individuals when their sensitive personal (non-PHI) information is compromised.

KP Business Information

KP business information includes Kaiser Permanente's financial figures, strategies, initiatives, research, and intellectual property (ideas, patents, copyrights, inventions, and trademarked programs).

KP business information should not be shared with anyone outside of the organization unless approval has been given by management.

Payment Card Information

The Payment Card Industry Data Security Standard applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers — as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data.

Protecting cardholder data is crucial to an organization's success.

You can find more information on the Payment Card Industry's Wiki site, available on the Course Resources page.

Does This Information Need Protection?

Instructions: Determine which items require protection.

Question 1 of 2



Does this information need protection?

- A. Yes
- B. No

The best response is A.

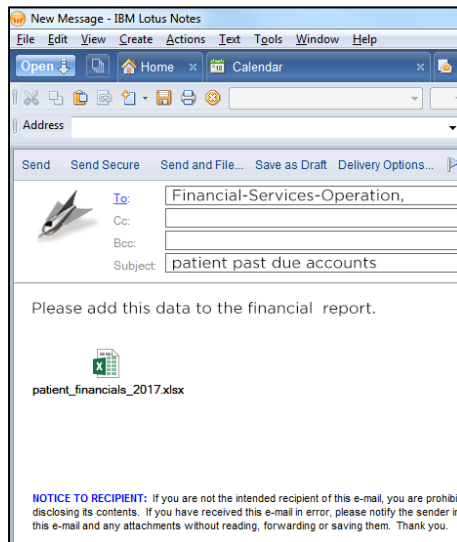
The medical wrist band requires protection because it meets all of the following conditions:

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

The patient's name and medical record number on the wrist band are PHI. Always dispose of

wristbands in a shredder or other confidential waste bin.

Question 2 of 2



Does this information need protection?

- A. Yes
- B. No

The best response is A.

The document attached to the email contains financial information, names, member numbers, addresses and dates of birth.

If you receive an email message with confidential information by mistake, notify the sender immediately (Do NOT reply all). Notify your manager or compliance officer and take no further action until you are instructed by your manager or compliance officer. Do NOT delete, forward, print, or save.

Never include PHI or other confidential information in the subject line of an email message.

Recognizing Potentially Dangerous Email

Cyber-attacks against health care organizations are on the rise. The most commonly used attack, with the highest degree of success, is masked as a well-constructed email.

This technique is called "phishing" and is intended to bait a person into clicking on a malicious link or attachment and providing personal and financial information. Clicking a link can also download "ransomware" that locks information from access. A successful attack can lead to network breaches, loss of sensitive data or even a halt to online operations.

Activity

Let's look at some real-life phishing email.

Dawn Bennett just sent you a personal message...

From: **Dawn Bennett** (Bennett1975@echo.ptwebserver.com)
Sent: Sat 12/08/12 1:26 AM
To: [Redacted]

LinkedIn

Dawn Bennett just sent you a message

Date: 12/08/2012

<https://www.linkedin.com/trk?act=viewProfile&eg=profile&message=3332515>

[View/reply to this message](#)

Don't want to receive e-mail notifications?
© 2012, LinkedIn Corporation

Annotations:

- But look at the email address – it's not from LinkedIn at all. The email is a fake.
- This email is designed to look like it came from LinkedIn. As you can see, the logo and content are exactly what you'd expect from a LinkedIn email.

Annotations:

- This is a phishing email designed to resemble official email from Apple, and it looks authentic.
- Look at the email address – it's not from apple.com, it's from the domain palpay.com, which has nothing to do with Apple.

Apple <account@palpay.com>
TO: [Redacted] 8:12 PM
Your Apple Account Is Temporarily Blocked Until Update

Dear User,

This is an automated email, please do not reply .

You have to confirm your account information within 48 hours.
Your account has been frozen temporarily in order to protect it.

The account will continue to be frozen until it is approved And Validate Your Account Information.
Once you have updated your account records, your information will be confirmed and your account will start to work as normal once again.

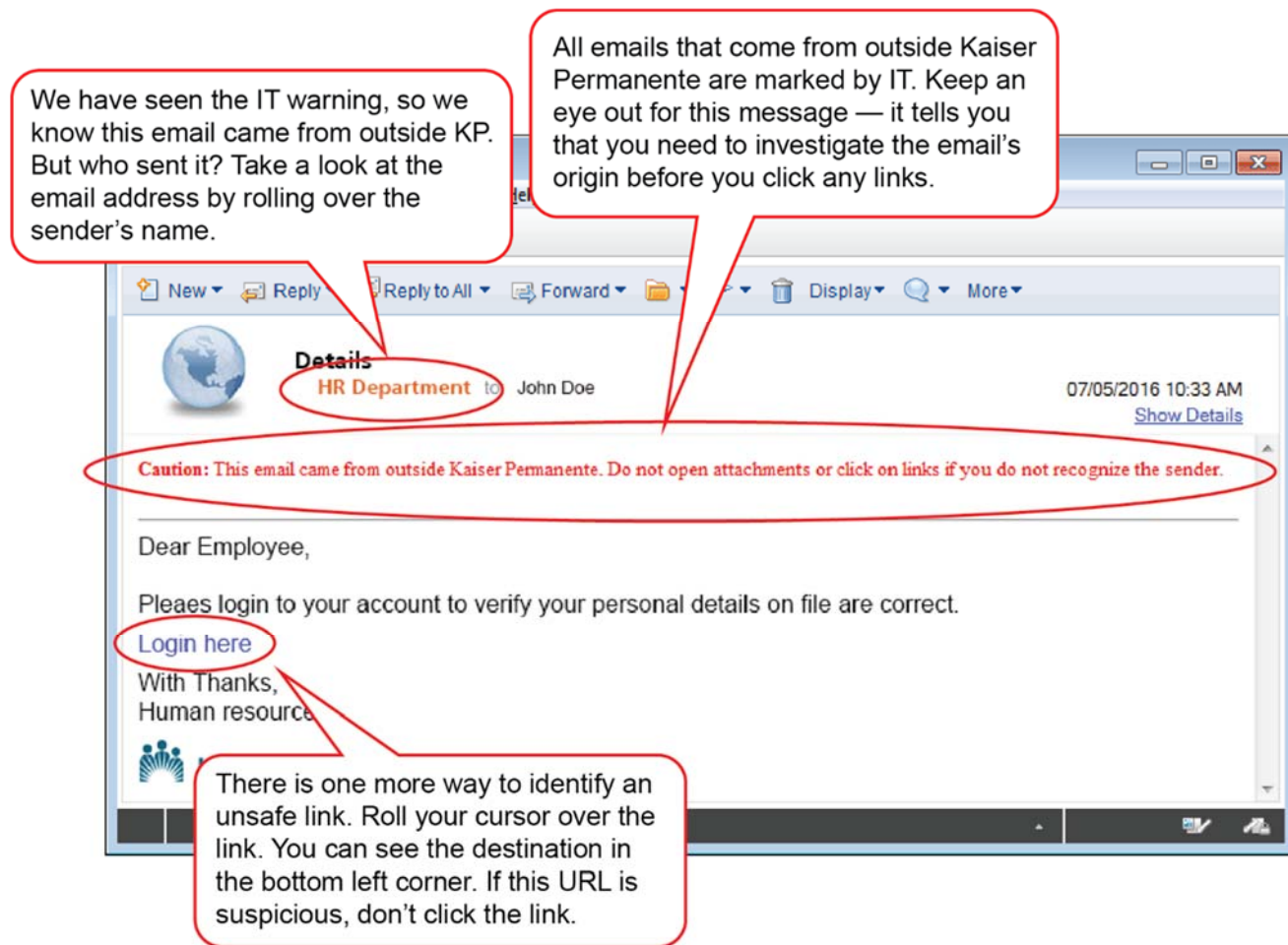
The process does not take more than 3 minutes.

To proceed to confirm your account information please click on the link below and follow the instructions that will be required.

[Verify Now >](#)

Thanks,
Customer Support

In this activity, you will learn how to verify that an email is safe before you click any links or open any attachments. We're going to focus on three clues that indicate an email is unsafe.



Reporting Potentially Dangerous Email

Spotting malicious email could save Kaiser Permanente from a headline-worthy data breach! It will save our members, patients and colleagues the pain of having their data hacked.

Report phishing emails:

- In Lotus Notes, click the "More" drop-down menu and select "Report Spam."
- In Office 365, click "Report Spam" on the Outlook Toolbar.
- From a mobile device with the absence of a report spam function, forward the email to spam@kp.org.

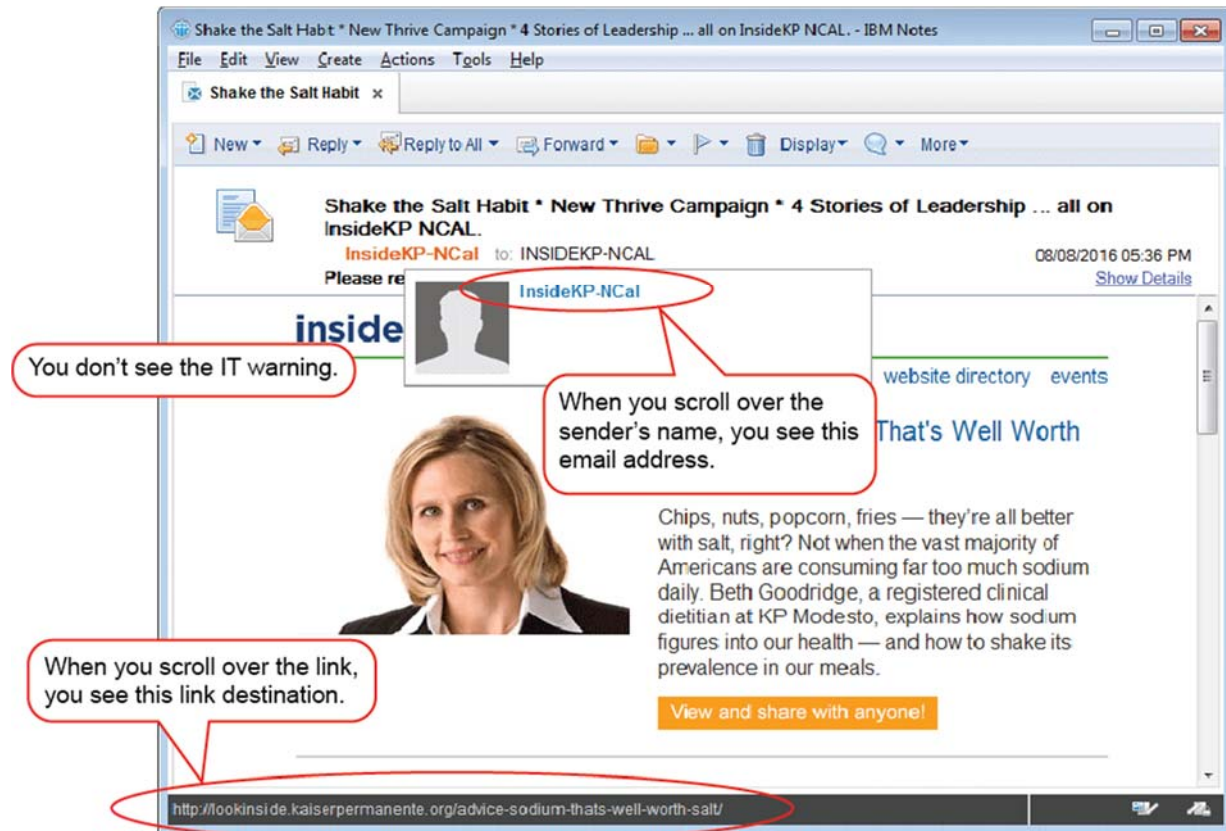
If you've clicked a malicious link or feel you're a victim of a phishing attack, immediately call the IT Service Desk at 1-888-457-4872.

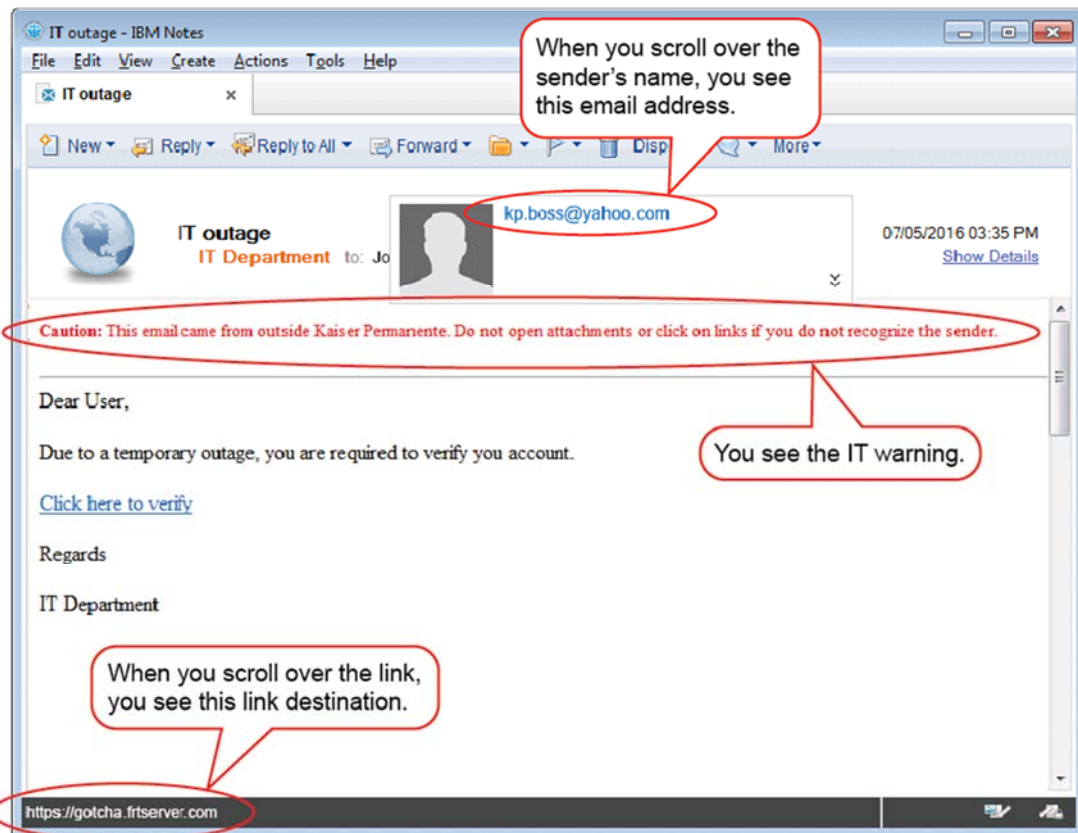
Activity

It's important that we develop good habits with our email. In this activity, you will see three emails. Two are safe, and one is malicious.

Follow these steps to identify unsafe emails:

1. Look for the IT warning.
2. Roll over the sender's name.
3. Roll over the link to see the destination URL.





What Should You Do?

We encounter confidential information daily, and it's critical that we protect all of it.

No matter if it's personal information, PHI, business information, or payment card information, it's important to remember that all confidential information requires our attention and protection.

Question 1

You see that one of your colleagues is discussing a KP member's diagnosis and prescriptions on social media.

What should you do?

Select the best answer.

- A.** Ignore it – it's none of your business.
- B.** Notify compliance.

Feedback

The best response is B.

Our patients and members deserve our respect and we have a moral duty to safeguard their privacy. After all, that's how we would want to be treated.

It's important that you report this situation as quickly as possible to a compliance expert, as it's potentially very upsetting for the member and very damaging to Kaiser Permanente's reputation.

Question 2

Your colleague wrote a password on a post-it and left it on the desk.

What should you do?

Select all that apply.

- A.** Leave it there – it'll probably be fine.
- B.** Remove the post-it.
- C.** Speak up! Talk respectfully to your colleague about the risk to member data.

Feedback

The best responses are B and C.

Exposed passwords are risky!

You could help by hiding the password and reminding your co-worker of the risks. If we help each other manage risk at work, we can prevent them from becoming reportable incidents.

GOOD THINGS HAPPEN WHEN WE PROTECT CONFIDENTIAL INFORMATION

You can make a difference. By minimizing privacy risks, we can keep confidential information safe.

It's not easy and there's always room for improvement. Remember, there's a support system in place for you; your manager and compliance officer are there to help.

By doing your part to minimize risk in your work environment and reporting when things aren't right, we can avoid costly incidents.

MODULE 2: SELF CHECK

Instructions: Select the best answer(s) for each question.

Question 1:

Which of the following present risks to confidential information?

Select all that apply.

- A. Secure areas
- B. PCs and laptops
- C. KP iPhones
- D. KP printers
- E. Trash bins

Question 2:

Which of the following can be prevented?

Select all that apply.

- A. A laptop stolen from a car
- B. A cell phone left on a bus
- C. A piece of malware installed from a phishing email
- D. An email attachment sent to the wrong recipient

SUMMARY

Protecting confidential information is like locking your car doors. If you take the necessary steps to minimize risk in your work environment, you're doing your part to prevent data loss or theft.

We must protect all confidential information, including PHI, financial information, and other sensitive data. By doing so, we protect our assets and the privacy and security of our patients, members, and colleagues.

MODULE 3: PREVENTING FRAUD, WASTE, AND ABUSE

INTRODUCTION

Every year billions of dollars are improperly spent because of fraud, waste, and abuse. It affects everyone, including you.

In this module, you'll learn how to recognize the warning signs, identify the major laws and regulations, recognize potential consequences and penalties associated with violations, and identify prevention methods. Like avoiding road hazards, preventing incidents protects our members' health, our resources, our good name, and our jobs.

FRAUD, WASTE, AND ABUSE DEFINED

There are differences among fraud, waste, and abuse. One of the primary differences is intent and knowledge.

When someone commits fraud, he or she *intends* to obtain payment and knows that what he or she is doing is wrong. When someone wastes or abuses items or services, he or she may obtain an improper payment or create an unnecessary cost to Kaiser Permanente, but that person doesn't necessarily have the same intent and knowledge as someone committing fraud.

Fraud

Fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program, or to obtain, by means of false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or under the custody or control of, any health care benefit program.

Waste

Waste is the extravagant, careless, or needless use of KP or government funds. Waste includes overusing services, or other practices that result in unnecessary costs to Kaiser Permanente (or the government).

Waste is generally not associated with criminally negligent actions, but rather with simple carelessness.

Abuse

Abuse includes actions that may, directly or indirectly, result in unnecessary costs to Kaiser Permanente (or the government). Abuse involves payment for items or services when there is not legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

FRAUD, WASTE, AND ABUSE EXAMPLES

The following examples illustrate the differences between fraud, waste, and abuse.

Fraud Examples

Examples of fraud include:

- Knowingly billing for services not furnished or supplies not provided, including billing Medicare for appointments that the patient failed to keep
- Billing for non-existent prescriptions
- Knowingly altering claim forms, medical records, or receipts to receive a higher payment

Waste Examples

Examples of waste include:

- Conducting excessive office visits or writing excessive prescriptions
- Prescribing more medications than necessary for the treatment of a specific condition
- Ordering excessive laboratory tests
- Purchasing from non-approved KP vendors
- Ordering excessive inventory

Abuse Examples

Examples of abuse include:

- Billing for unnecessary medical services
- Billing for brand name drugs when generics are dispensed
- Charging excessively for services or supplies
- Misusing codes on a claim, such as upcoding or unbundling codes

IS IT FRAUD, WASTE, OR ABUSE?

Question

Is it fraud, waste, or abuse?

- A. A lab director routinely billed Medicare for unordered lab work.
- B. A pharmacist ordered too much of a drug. The supply expired.
- C. A physician received \$6,000 in bribes from a laboratory in return for referring patients to the laboratory.
- D. An employee used a KP copy machine to make flyers for her son's school.

Feedback

- A. This is fraud. The lab director intended to benefit from the surplus generated. The laboratory was subject to a penalty per claim under the False Claims Act (FCA).
- B. This is waste. The pharmacist did not intend to over-order supplies. However, in doing so, she cost the organization money. The pharmacist violated local policies and guidelines.
- C. This is fraud. The physician intentionally referred patients to a laboratory that provided him with a financial incentive. The physician violated the Anti-Kickback Statute.
- D. This is abuse. She used KP supplies for her own benefit. The employee violated local policies and guidelines.

HOW MUCH DOES FRAUD, WASTE, AND ABUSE COST?

The cost of fraud, waste, and abuse adds up quickly and can result in inflated costs to the company, damage to the company's reputation, mandatory retraining, disciplinary action, and possible termination.

Question 1

How much revenue do you think the average business loses every year to fraud, waste, and abuse?

Select your best guess.

- A. 0% of revenue
- B. 1% of revenue
- C. 2% of revenue
- D. 3% of revenue
- E. 4% of revenue
- F. 5% of revenue

Feedback

The best response is F.

It's impossible to know *exactly* how much revenue is lost because not all fraud, waste, and abuse is reported.

However, the Association of Certified Fraud Examiners estimates that on average, five percent of a business' revenue is lost to fraud each year. That may not sound like a lot, but for our members, five percent can mean higher premiums overall.

Question 2

How much can you save if you book a flight for business travel well in advance?

Select your best guess.

- A. \$0
- B. \$100
- C. \$200
- D. \$300
- E. \$400
- F. \$500
- G. \$600
- H. \$700

Feedback

The best response is F.

The difference in reserving a cross-country flight two days prior versus two months in advance could be as high as \$500. KP business travel reservations should be made at least 14 days ahead of time.

Question 3

How much do individuals impact health care insurance companies by seeking drugs for personal gain?

Select your best guess.

- A. \$0 B
- B. \$22.5 B
- C. \$32.5 B
- D. \$42.5 B
- E. \$52.5 B
- F. \$62.5 B
- G. \$72.5 B
- H. \$82.5 B
- I. \$92.5 B

Feedback

The best response is G.

Individuals can cost medical insurance companies up to \$72.5 billion per year from stealing drugs. It's financially costly, and it's also costing lives: 40 percent of deaths from drug overdose are from prescription pain relievers.

YOUR RESPONSIBILITIES

You play a vital part in preventing, detecting, and reporting potential fraud, waste, and abuse.

1. You must comply with all applicable statutory, regulatory, and other government requirements.
2. You have a duty to the government to report any compliance concerns, and suspected or actual violations that you may be aware of.
3. You have a duty to follow the *Principles of Responsibility*.
4. Stay informed about policies and procedures.

UNDERSTANDING THE LAWS

To detect fraud, waste, and abuse, you need to know the law. For details about the specific laws, such as safe harbor provisions, consult the applicable statute and regulations.

Law	Description
Civil False Claims Act (FCA)	<p>The civil provisions of the FCA make a person liable to pay damages to the Government if he or she knowingly:</p> <ul style="list-style-type: none">• Conspires to violate the FCA• Carries out other acts to obtain property from the Government by misrepresentation• Knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay the Government• Makes or uses a false record or statement supporting a false claim• Presents a false claim for payment or approval <p>Refer to 31 U.S.C. Sections 3729-3733.</p> <p>Damages and Penalties</p> <p>Any person who knowingly submits false claims to the Government is liable for three times the Government's damages caused by the violator plus a penalty. The Civil Monetary Penalty may range from \$5,500 to \$11,000 for each false claim.</p>
Law	Description

<p>Civil False Claims Act (FCA) (cont.)</p>	<p>Example</p> <p>A Medicare Part C plan in Florida:</p> <ul style="list-style-type: none"> • Hired an outside company to review medical records to find additional diagnosis codes that could be submitted to increase risk capitation payments from the Centers for Medicare & Medicaid Services (CMS) • Was informed by the outside company that certain diagnosis codes previously submitted to Medicare were undocumented or unsupported; • Failed to report the unsupported diagnosis codes to Medicare; and • Agreed to pay \$22.6 million to settle FCA allegations. <p>Whistleblowers</p> <p>A whistleblower is a person who exposes information or activity that is deemed illegal, dishonest, or violates professional or clinical standards.</p> <p>Protected: Persons who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.</p> <p>Rewarded: Persons who bring a successful whistleblower lawsuit receive at least 15 percent but not more than 30 percent of the money collected.</p>
<p>Health Care Fraud Statute</p>	<p>The Health Care Fraud Statute states that “Whoever knowingly and willfully executes, or attempts to execute, a scheme to...defraud any health care benefit program... shall be fined...or imprisoned not more than 10 years, or both.”</p> <p>Conviction under the statute does not require proof that the violator had knowledge of the law or specific intent to violate the law. For more information, refer to 18 U.S.C. Section 1346 on the Internet.</p> <p>Examples:</p> <p>A Pennsylvania pharmacist:</p> <ul style="list-style-type: none"> • Submitted claims to a Medicare Part D plan for non-existent prescriptions and for drugs not dispensed. • Pleaded guilty to health care fraud. • Received a 15-month prison sentence and was ordered to pay more than \$166,000 in restitution to the plan.

Law	Description
<p>Health Care Fraud Statute (cont.)</p>	<p>The owners of two Florida durable medical equipment companies:</p> <ul style="list-style-type: none"> • Submitted false claims of approximately \$4 million to Medicare for products that were not authorized and not provided. • Were convicted of making false claims, conspiracy, health care fraud, and wire fraud. • Were sentenced to 54 months in prison. • Were ordered to pay more than \$1.9 million in restitution.
<p>Criminal Fraud</p>	<p>Persons who knowingly make a false claim may be subject to:</p> <ul style="list-style-type: none"> • Criminal fines up to \$250,000 • Imprisonment for up to 20 years <p>If the violations resulted in death, the individual may be imprisoned for any term of years or for life.</p> <p>For more information, refer to 18 U.S.C. Section 1347 on the Internet.</p>
<p>Anti-Kickback Statute</p>	<p>The Anti-Kickback Statute prohibits knowingly and willfully soliciting, receiving, offering, or paying remuneration (including any kickback, bribe, or rebate) for referrals for services that are paid, in whole or in part, under a Federal health care program (including the Medicare Program).</p> <p>For more information, refer to 42 U.S.C. Section 1320A-7b(b) on the Internet.</p> <p>Damages and Penalties</p> <p>Violations are punishable by:</p> <ul style="list-style-type: none"> • A fine of up to \$25,000 • Imprisonment for up to 5 years <p>For more information, refer to the Social Security Act (the Act), Section 1128B(b) on the Internet.</p>

Law	Description
<p>Anti-Kickback Statute (cont.)</p>	<p>Example</p> <p>A radiologist who owned and served as medical director of a diagnostic testing center in New Jersey:</p> <ul style="list-style-type: none"> • Obtained nearly \$2 million in payments from Medicare and Medicaid for MRIs, CAT scans, ultrasounds, and other resulting tests; • Paid doctors for referring patients; • Pleaded guilty to violating the Anti-Kickback Statute; and • Was sentenced to 46 months in prison. <p>The radiologist was among 17 people, including 15 physicians, who have been convicted in connection with this scheme.</p>
<p>Stark Statute</p>	<p>The Stark Statute prohibits a physician from making referrals for certain designated health services to an entity when the physician (or a member of his or her family) has:</p> <ul style="list-style-type: none"> • An ownership/investment interest, or • A compensation arrangement (exceptions apply). <p>For more information, refer to 42 U.S.C. Section 1395nn on the Internet.</p> <p>Damages and Penalties</p> <p>Medicare claims tainted by an arrangement that does not comply with the Stark Statute are not payable. A penalty of up to \$15,000 may be imposed for each service provided. There may also be up to a \$100,000 fine for entering into an unlawful arrangement or scheme.</p> <p>For more information, visit https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral on the CMS website and refer to the Act, Section 1877 on the Internet.</p> <p>Example</p> <p>A physician paid the Government \$203,000 to settle allegations that he violated the physician self-referral prohibition in the Stark Statute for routinely referring Medicare patients to an oxygen supply company he owned.</p>

Law	Description
<p>Civil Monetary Penalties Law</p>	<p>The Office of Inspector General (OIG) may impose Civil penalties for a number of reasons, including:</p> <ul style="list-style-type: none"> • Arranging for services or items from an excluded individual or entity • Providing services or items while excluded • Failing to grant OIG timely access to records • Knowing of an overpayment and failing to report and return it • Making false claims • Paying to influence referrals <p>For more information, refer to the Act, Section 1128A(a) on the Internet.</p> <p>Damages and Penalties</p> <p>The penalties range from \$10,000 to \$50,000 depending on the specific violation. Violators are also subject to three times the amount:</p> <ul style="list-style-type: none"> • Claimed for each service or item, or • Of remuneration offered, paid, solicited, or received <p>Example</p> <p>A California pharmacy and its owner agreed to pay over \$1.3 million to settle allegations they submitted claims to Medicare Part D for brand name prescription drugs that the pharmacy could not have dispensed based on inventory records.</p>
<p>Exclusion</p>	<p>No Federal health care program payment may be made for any item or service furnished, ordered, or prescribed by an individual or entity excluded by the OIG. The OIG has authority to exclude individuals and entities from federally funded health care programs and maintains the List of Excluded Individuals and Entities (LEIE). You can access the LEIE at https://exclusions.oig.hhs.gov on the Internet.</p> <p>The United States General Services Administration (GSA) administers the Excluded Parties List System (EPLS), which contains debarment actions taken by various Federal agencies, including the OIG. You may access the EPLS at https://www.sam.gov on the Internet.</p> <p>If looking for excluded individuals or entities, make sure to check both the LEIE and the EPLS since the lists are not the same. For more information, refer to 42 U.S.C. Section 1320a-7 and 42 Code of Federal Regulations Section 1001.1901 on the Internet.</p>

Law	Description
<p>Exclusion (cont.)</p>	<p>Example</p> <p>A pharmaceutical company pleaded guilty to two felony counts of criminal fraud related to failure to file required reports with the Food and Drug Administration concerning oversized morphine sulfate tablets. The executive of the pharmaceutical firm was excluded based on the company’s guilty plea. At the time the executive was excluded, he had not been convicted himself, but there was evidence he was involved in misconduct leading to the company’s conviction.</p>
<p>Health Insurance Portability and Accountability Act (HIPAA)</p>	<p>HIPAA created greater access to health care insurance, protection of privacy of health care data, and promoted standardization and efficiency in the health care industry.</p> <p>HIPAA safeguards help prevent unauthorized access to protected health care information. As an individual with access to protected health care information, you must comply with HIPAA.</p> <p>For more information, visit http://www.hhs.gov/ocr/privacy on the Internet.</p> <p>Damages and Penalties</p> <p>Violations may result in Civil Monetary Penalties. In some cases, criminal penalties may apply.</p> <p>Example</p> <p>A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining protected health information with the intent to use it for personal gain. He was sentenced to 12 months and 1 day in prison.</p>

WARNING SIGNS

The following issues may indicate potential fraud, waste, or abuse. Each topic provides questions to ask yourself about different areas, depending on your role.

Key Indicators	Questions
Key Indicators for Member Issues	<ul style="list-style-type: none"> • Does the prescription, medical record, or laboratory test look altered or possibly forged? • Does the beneficiary's medical history support the services requested? • Have you filled numerous identical prescriptions for this beneficiary, possibly from different doctors? • Is the person receiving the medical service the actual beneficiary (identity theft)? • Is the prescription appropriate based on the beneficiary's other prescriptions?
Key Indicators for Provider Issues	<ul style="list-style-type: none"> • Are the provider's prescriptions appropriate for the member's health condition (medically necessary)? • Does the provider bill the Sponsor for services not provided? • Does the provider write prescriptions for diverse drugs or primarily for controlled substances? • Is the provider performing medically unnecessary services for the member? • Is the provider prescribing a higher quantity than medically necessary for the condition? • Is the provider's diagnosis for the member supported in the medical record?

Key Indicators	Questions
Key Indicators for Pharmacy Issues	<ul style="list-style-type: none"> • Are drugs being diverted (drugs meant for nursing homes, hospice, and other entities being sent elsewhere)? • Are the dispensed drugs expired, fake, diluted, or illegal? • Are generic drugs provided when the prescription requires that brand drugs be dispensed? • Are Pharmacy Benefits Managers being billed for prescriptions that are not filled or picked up? • Are proper provisions made if the entire prescription cannot be filled (no additional dispensing fees for split prescriptions)? • Do you see prescriptions being altered (changing quantities or Dispense As Written)?
Key Indicators for Wholesaler Issues	<ul style="list-style-type: none"> • Is the wholesaler distributing fake, diluted, expired, or illegally imported drugs? • Is the wholesaler diverting drugs meant for nursing homes, hospices, and Acquired Immune Deficiency Syndrome (AIDS) clinics and then marking up the prices and sending to other smaller wholesalers or pharmacies?
Key Indicators for Manufacturer Issues	<ul style="list-style-type: none"> • Does the manufacturer promote off-label drug usage? • Does the manufacturer provide samples, knowing that the samples will be billed to a Federal health care program?
Key Indicators for Sponsor Issues	<ul style="list-style-type: none"> • Does the Sponsor encourage/support inappropriate risk adjustment submissions? • Does the Sponsor lead the beneficiary to believe that the cost of benefits is one price, only for the beneficiary to find out that the actual cost is higher? • Does the Sponsor offer cash inducements for beneficiaries to join the plan? • Does the Sponsor use unlicensed agents? <p>Note: Kaiser Foundation Health Plan is the "Sponsor" entity in our organization. The term "Sponsor" is short for "Medicare Plan Sponsor" and covers Kaiser Foundation Health Plan, Inc., and each of its subsidiary regional health plans.</p>

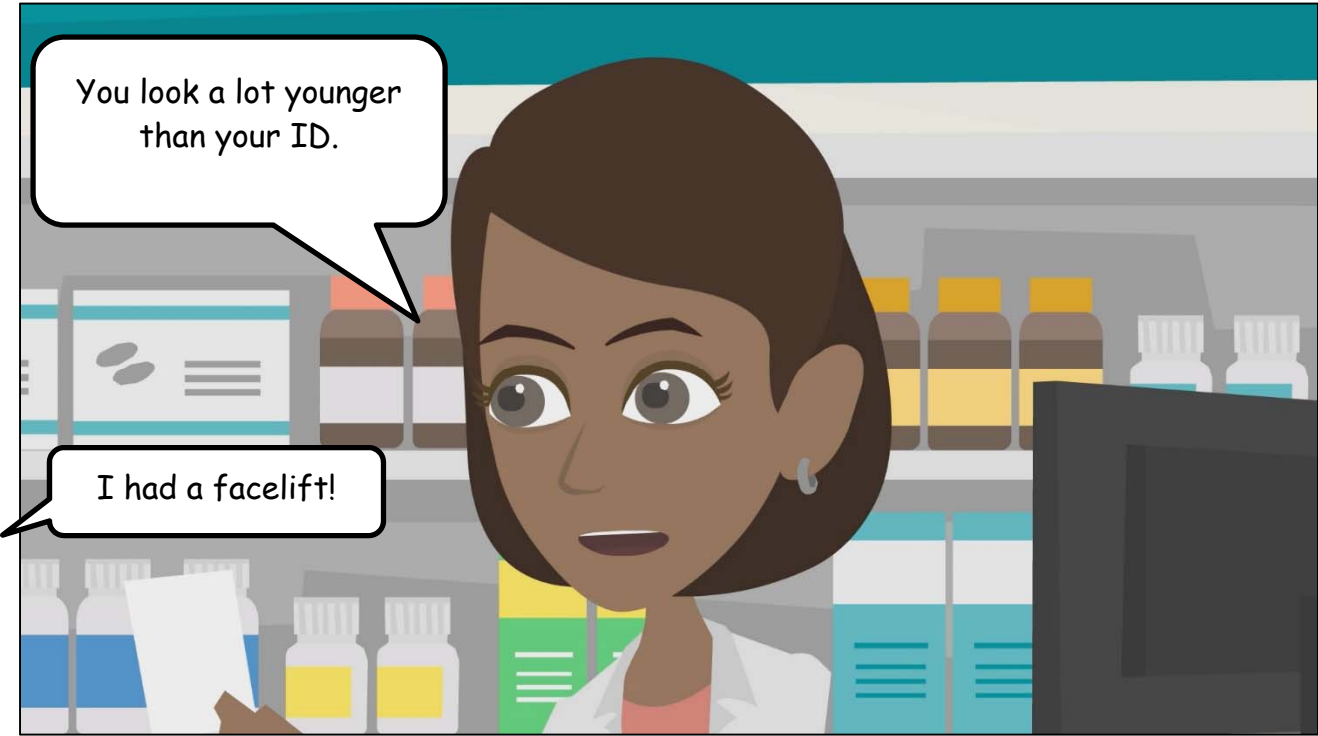
COULD IT BE FRAUD?

Most of us are accustomed to seeing similar surroundings and situations each day we spend at work. By being on the lookout for the unusual or incorrect things, we're more likely to prevent an incident.

See if you can spot the signs for fraud in the following situations.

Scenario







Question

What are the warning signs?

Select all that apply.

- A.** Mr. Lee doesn't look like his picture ID.
- B.** The prescription is for a pain killer, and isn't due for a refill.

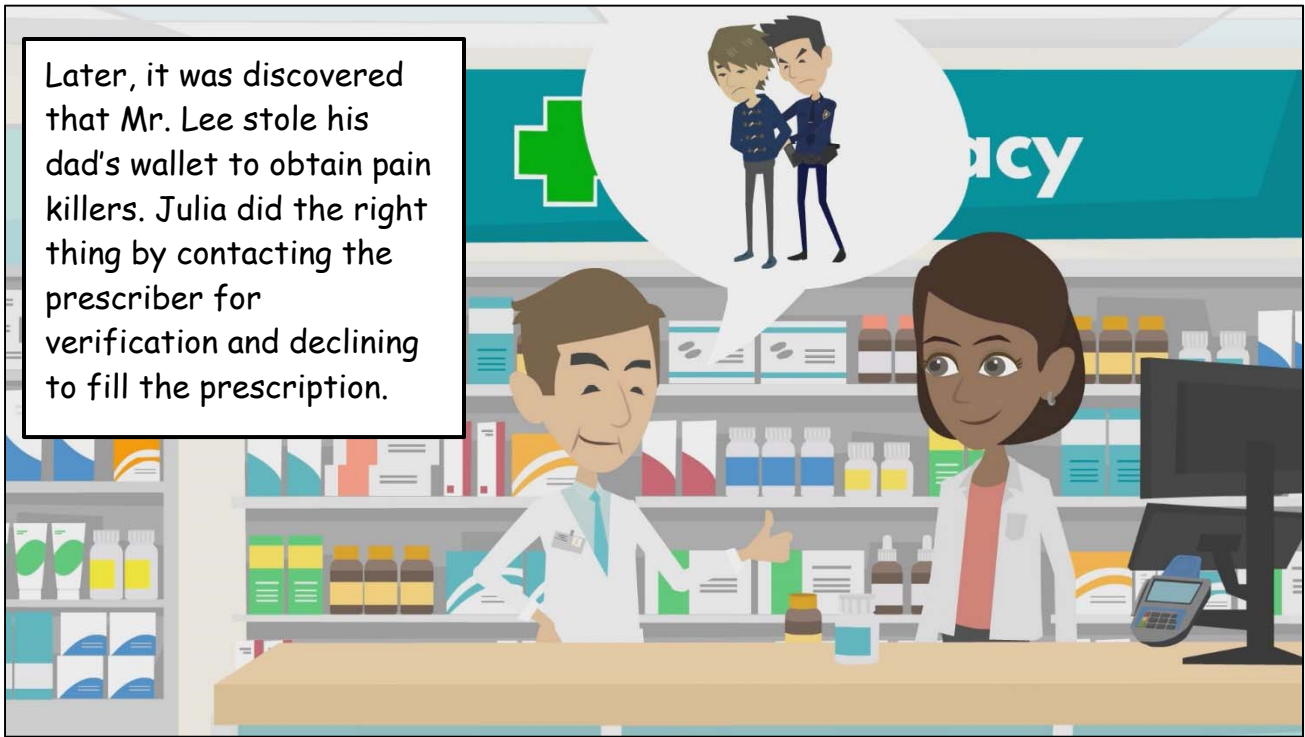
Feedback

The best responses are A and B.

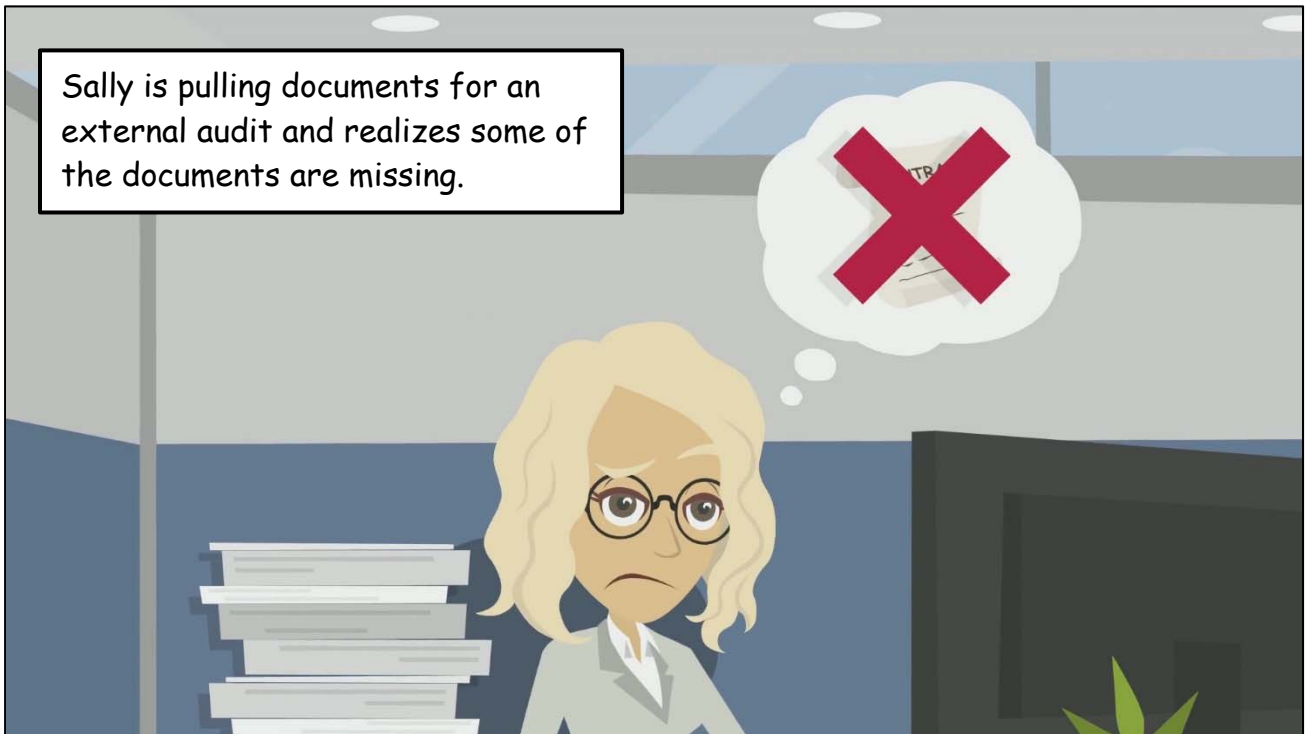
The warning signs are:

- Mr. Lee doesn't resemble his picture ID.
- The prescription isn't due for a refill.





Scenario





Question

What are the warning signs?

Select all that apply.

- A.** Some documents are missing.
- B.** Sally's boss encourages her to make inappropriate adjustments.
- C.** Sally pulls documents for an audit.

Feedback

The best responses are A and B.

The warning signs are:

- Some documents are missing.
- Sally's boss encourages her to make inappropriate adjustments.

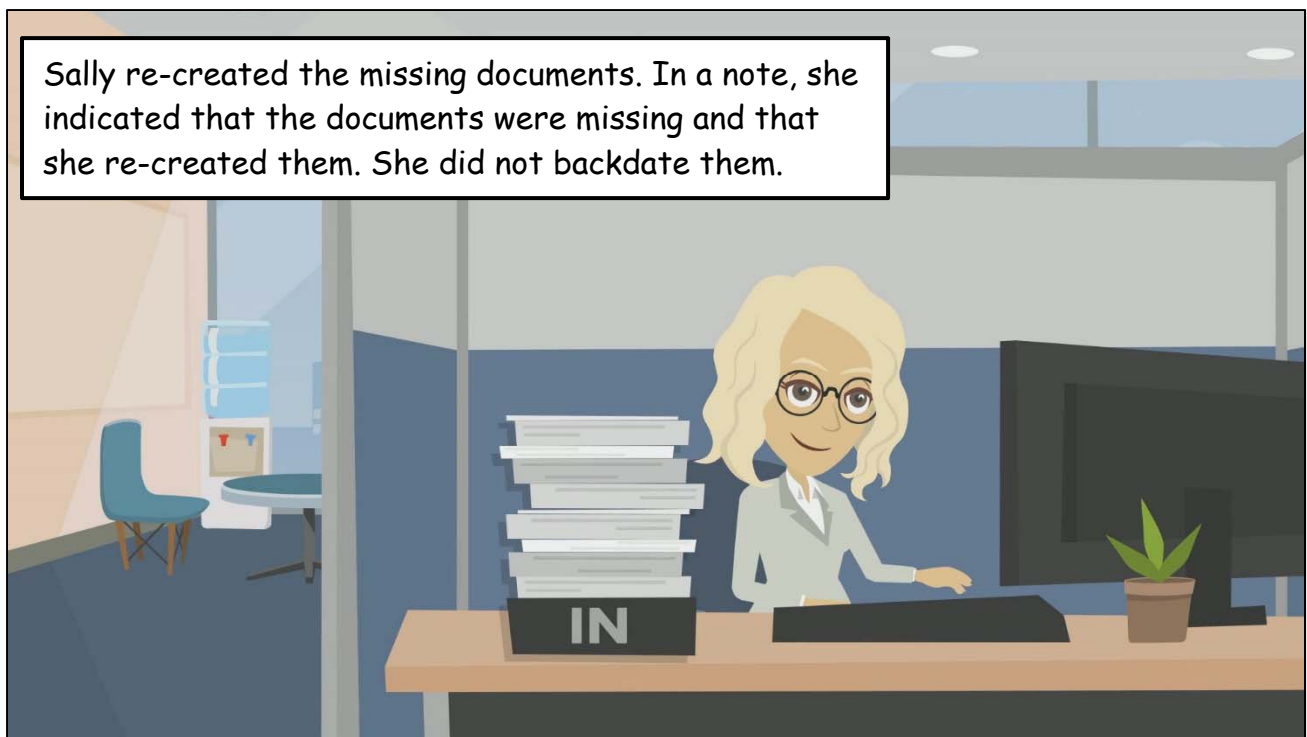
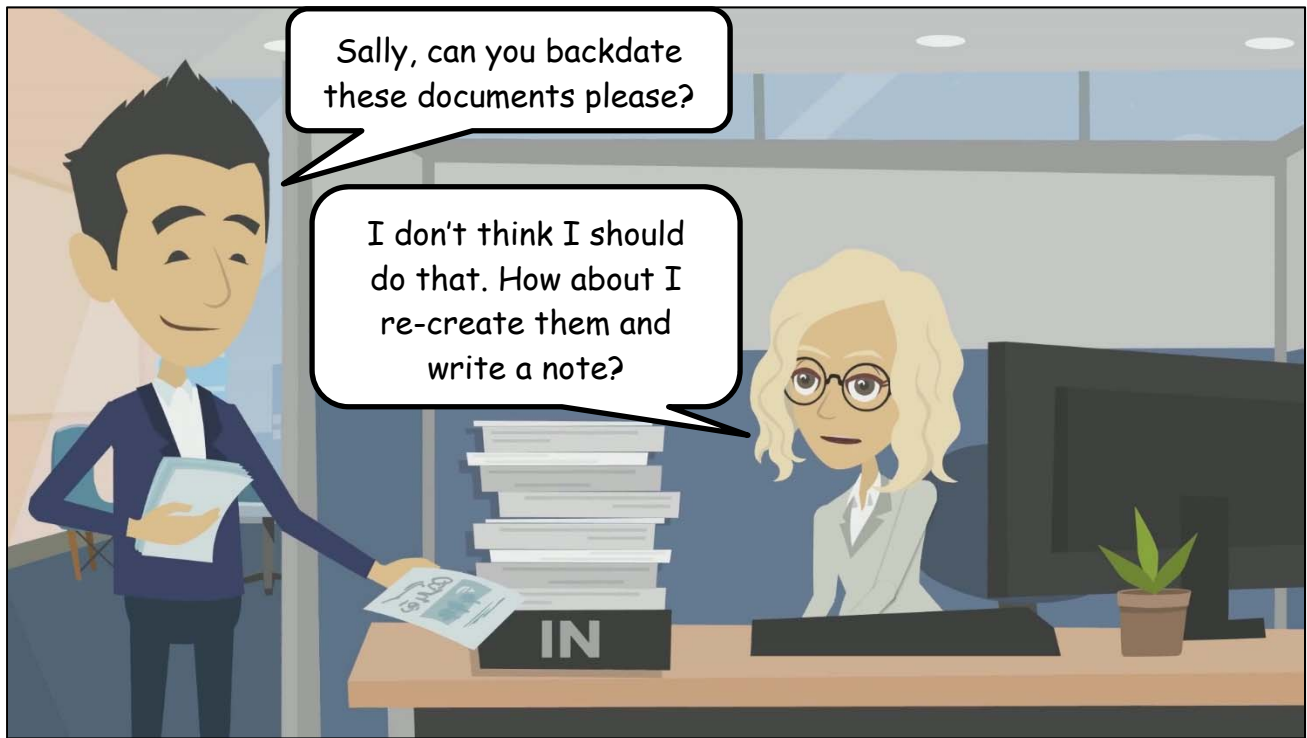
The auditors discovered the documents were backdated. Our organization's reputation was put at risk.



In this case, Sally's boss and several of his employees were let go, including Sally.



How could this have been prevented?



When you see a sign of possible fraud, take time to assess the situation. You may simply need to ask a patient, member, or co-worker some clarifying questions. Or, you may need to report a possible incident.

PREVENTING FRAUD, WASTE AND ABUSE

We all play a role in preventing fraud, waste, and abuse. Follow these guidelines.

- Look for suspicious activity.
- Conduct yourself in an ethical manner.
- Ensure accurate and timely data and billing.
- Ensure to coordinate with other payers, if applicable.
- Keep up-to-date with policies and procedures, the *Principles of Responsibility*, laws, regulations, and the CMS guidance.
- Verify all information provided to you.

REPORTING AND CORRECTING FRAUD, WASTE AND ABUSE

Reporting

Everyone must report suspected instances of fraud, waste, and abuse. The *Principles of Responsibility* clearly states this obligation. As mandated by the government, Kaiser Permanente may not retaliate against you for making a good faith effort in reporting.

Don't be concerned about whether it's fraud, waste, or abuse. Just report any concerns to your compliance department. Kaiser Permanente's compliance department area will investigate and make the proper determination.

Correcting

Once fraud, waste, or abuse has been detected, it must be promptly corrected. Correcting the problem saves the government money and ensures Kaiser Permanente is in compliance with government requirements.

To correct an issue, our compliance community develops a plan.

Consult your organization's compliance officer to find out the process for the corrective action plan development. The actual plan is going to vary, depending on the specific circumstances. In general, the compliance community:

- Designs the corrective action to correct the underlying problem that results in program violations and to prevent future non-compliance;
- Tailors the corrective action to address the particular fraud, waste, or abuse, problem, or deficiency identified;
- Documents corrective actions addressing non-compliance or fraud, waste, and abuse committed by employees, dentists, and physicians, and includes consequences for failure to satisfactorily complete the corrective action; and
- Once started, continuously monitors corrective actions to ensure they are effective.

MODULE 3: SELF CHECK

Instructions: Select the best answer(s) for each question.

Question 1:

Which of the following are examples of fraud?

Select all that apply.

- A.** Altering claim forms, medical records, or receipts to receive a higher payment
- B.** Accidentally prescribing the wrong medications to a member
- C.** Over-ordering supplies that expire and must be discarded
- D.** Billing for appointments that a patient failed to keep

Question 2:

True or false?

If an individual knowingly and willfully solicits, receives, offers, or pays compensation (including any kickback, bribe, or rebate) for referrals for services that are paid, in whole or in part, under a Federal health care program, it's a criminal offense.

Select the best answer.

- A.** True
- B.** False

Question 3:

A physician referred a member for an unnecessary MRI at a lab where the physician has an investment interest.

What indicates that this is fraud, waste, or abuse?

Select the best answer.

- A.** The provider billed the member for services not provided.
- B.** The provider sent the member to a lab with which the provider has a financial relationship.
- C.** The provider referred a member to a lab.

Summary

Combatting fraud, waste, and abuse is everyone's responsibility.

You play a vital part in preventing, detecting, and reporting potential fraud, waste, and abuse. With your assistance, we can improve our efforts to prevent incidents and reduce our exposure to civil fines and penalties.

When faced with a potentially deceptive situation, remember:

- There are laws and regulations in place to help you identify and prevent fraud, waste, and abuse.
- There are potential consequences associated with violations.
- The compliance team and leadership will support you if you report compliance concerns in good faith.

MODULE 4: YOUR COMPLIANCE ROLE

Introduction

Let's shift gears to your compliance responsibilities. This module will cover what you need to know to protect confidential information, how you can help prevent fraud, waste, and abuse, and how to report any compliance concerns that arise as you focus on your job.

DO THE RIGHT THING

Like being a good driver, doing the right thing is usually just using common sense. Let's look at what this means for you and your compliance role.

Know the Rules of the Road

Know your job's scope and limitations, and follow our rules of the road — the Principles of Responsibility and our policies and procedures.

Stay informed about policies and procedures. Work with your manager if there are policy changes or a change to your job role.

Know the Road Hazards

Be prepared by knowing the risks in your work environment, such as physical risks, security risks, privacy and security risks, and fraud, waste, and abuse risks.

Your awareness will help us avoid them.

Self-Monitor

Check your work. Take personal accountability by following the established work process and doing your job well. Before exchanging information, such as sending an email, or handing an AVS to a member, be sure the information will go to the intended recipient.

If you work with PHI, make sure you appropriately use, access, and disclose it.

Report

Speak up! Report fraud, waste, abuse, and any other compliance concerns that you encounter. Remember, you have several options for reporting compliance concerns.

Know your compliance resources; if you need to report something, knowing who to report to will save you time and effort.

Report a compliance concern to local management whenever possible. When it's not, report to the KP Compliance Hotline (call or click) or another compliance resource.

Navigate

Complete all compliance training as well as any additional training required for your job role and function.

Training, practice, and consistency help us follow KP policies and procedures and do the right thing in all of our encounters.

WHAT SHOULD THEY DO?

You play a vital role in preventing fraud, waste, and abuse. See if you can determine the right thing to do in each of the following scenarios.

Scenario



Question

Should he take the tickets?

Select the best answer.

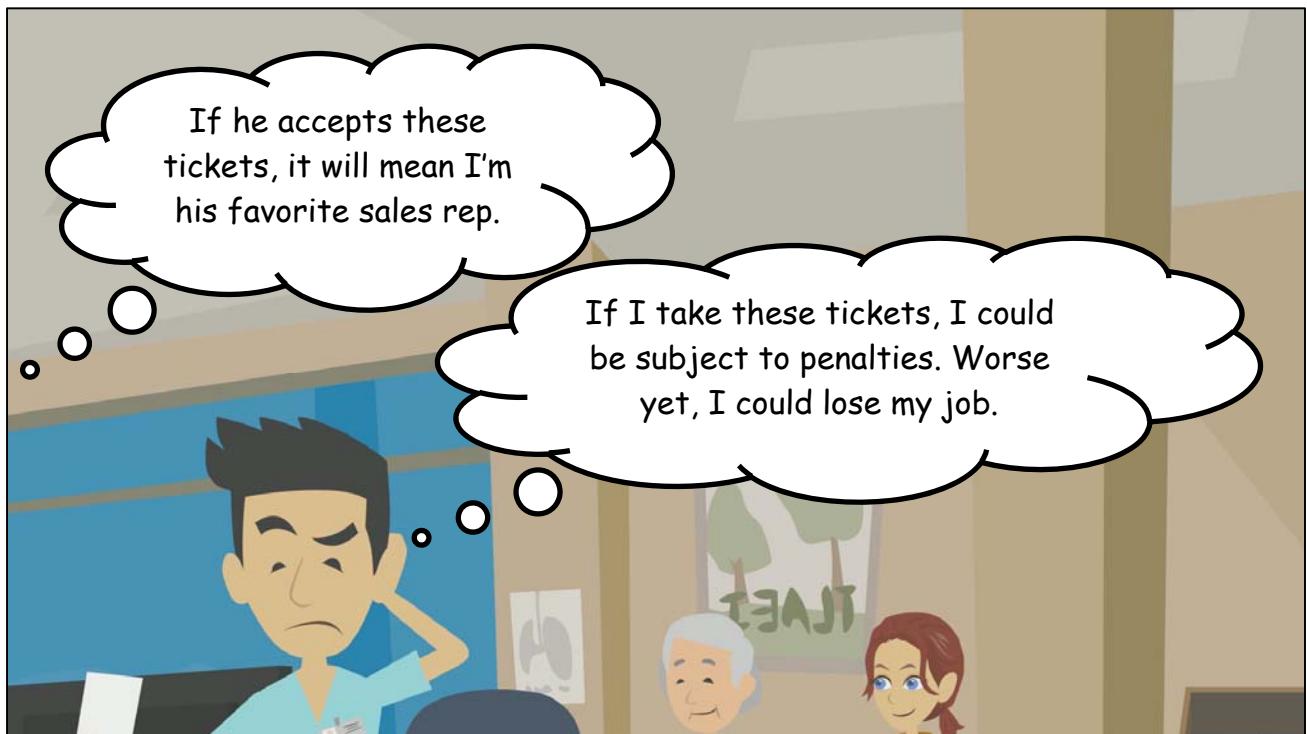
- A. Yes
- B. No

Feedback

The best response is B.

He should not take the tickets. Our policies and our *Principles of Responsibility* say not to do this.

Scenario



Question

What should he do now?

Select the best answer.

- A. Play it cool. No one needs to know he took the tickets.
- B. Refuse the tickets and report the incident to his supervisor.

Feedback

The best response is B.

He should report the incident.

Scenario



Maintaining and protecting Kaiser Permanente's reputation depends directly on our actions and the integrity with which we conduct our work.

Scenario

KP employees Salina and Naomi are friends and are connected on Facebook. Salina posts about a transgender member who just had surgery at a KP hospital. Naomi sees this and she's immediately concerned.



Question

What should Naomi do?

Select the best answer.

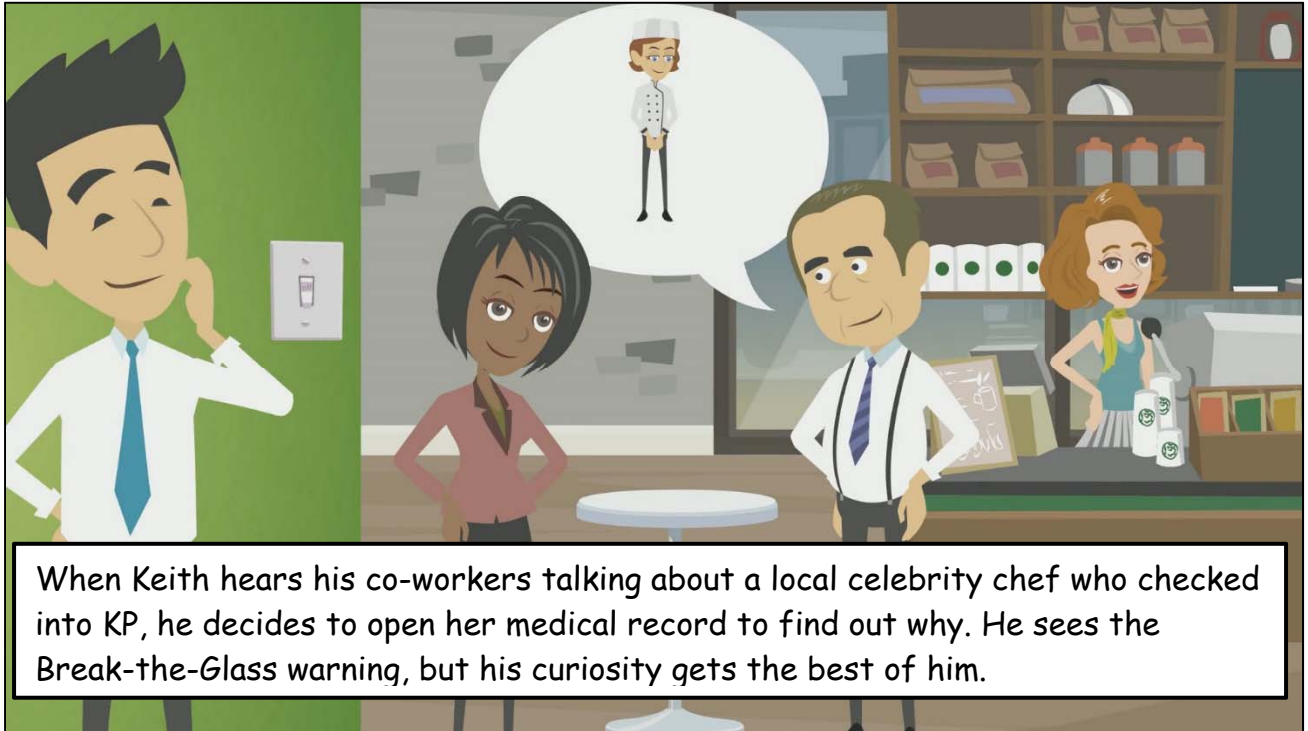
- A.** She should ask Salina to delete her post, then notify her immediate supervisor of the situation.
- B.** She should unfriend Salina and not mention the post to anyone.

Feedback

The best response is A.

She should ask Salina to delete her post, then notify her immediate supervisor of the situation. Writing about members and patients on social media can cause a privacy violation. This includes posting on blogs, podcasts, discussion forums, and social networks such as LinkedIn and Facebook.

Scenario



Question

What should Emma do?

Select the best answer.

- A. She should tell her manager.
- B. She should call HR.
- C. She should just walk away.

Feedback

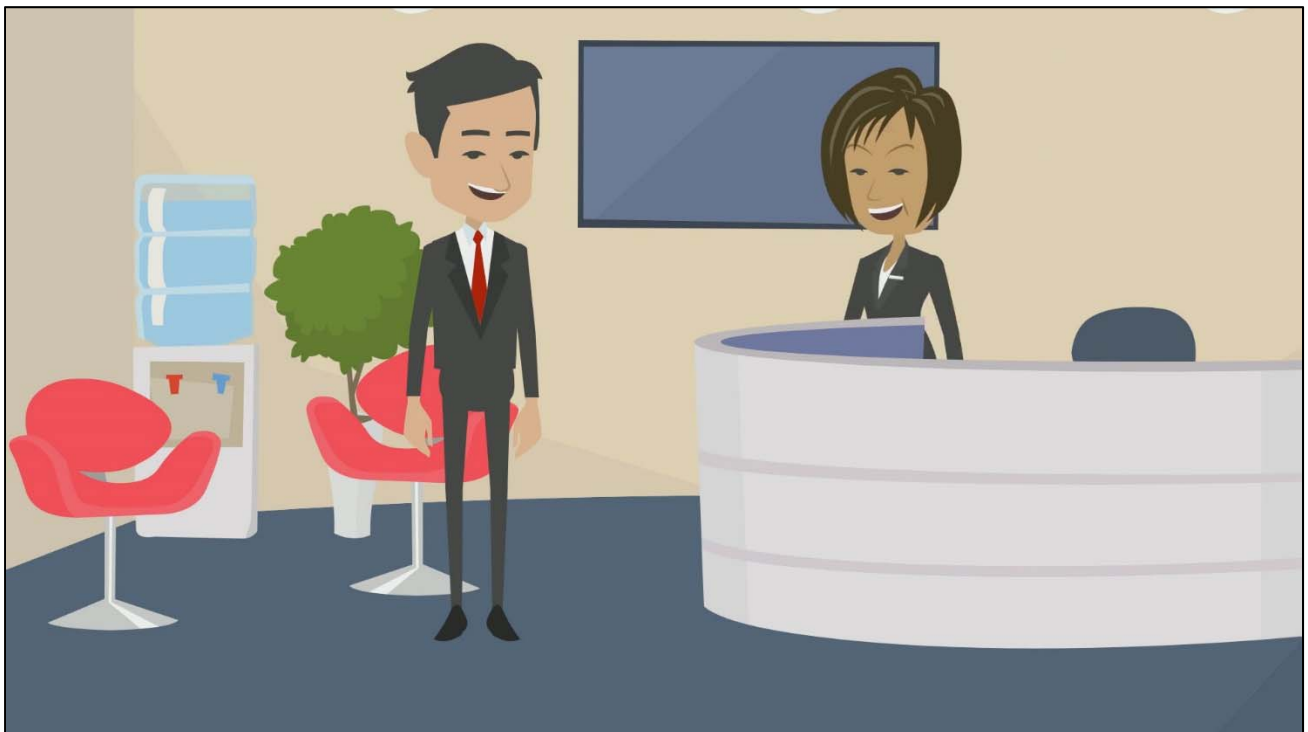
The best response is A.

Emma should tell her manager. KP HealthConnect® and other electronic systems at Kaiser Permanente make an abundance of information easily available to authorized individuals. However, to access, use, or disclose it you must have a job-related reason to do so.

Keith and his coworkers could face severe consequences. They could lose their jobs, licenses, and their ability to practice their professions. They could even face penalties and jail time.

Scenario

To validate KP's compliance with regulations, internal and external teams conduct inspections. What will you – as a physician or an employee – do if you are the first to encounter an inspector or a law enforcement officer? It's possible you'll be the first person to talk to the inspector.



It's important to follow these steps when an inspector arrives in your department:

- Greet the inspector or law enforcement officer.
- Ask for identification.
- Ask for the purpose of the visit.
- You may not deny entry.

Question

What should you do when an inspector or law enforcement officer arrives?

Select the best answer.

- A.** Greet the inspector or law enforcement officer
- B.** Ask for identification
- C.** Ask for the purpose of the visit
- D.** All of the above

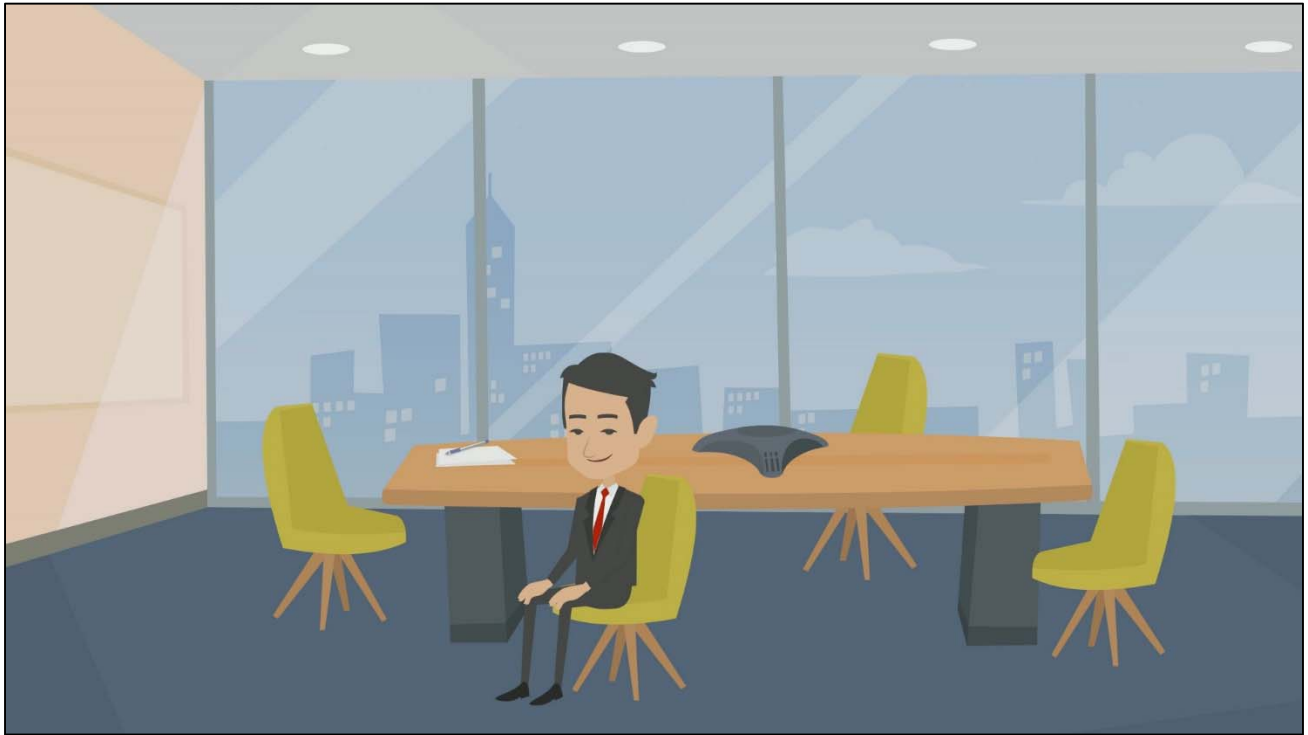
Feedback

The best response is D.

You should take all of these steps when an inspector or law enforcement officer arrives.

Scenario

A private location doesn't provide the inspector access to documentation. Tell the inspector you must contact the appropriate personnel, and then escort him to a private area, like a conference room or office. Make sure no confidential material is easily accessible.



Question

A private location ensures that the inspector _____:

Select the best answer to fill in the blank.

- A.** Doesn't have access to confidential material
- B.** Can access important information

Feedback

The best response is B.

A private location doesn't provide the inspector access to confidential documentation. Ask for the purpose of the visit and follow the local notification procedures. Be sure to contact your supervisor immediately. Be sure to maintain a professional manner at all times.

KEEP IT SECURE

We've looked at the role of compliance and the risks that you may encounter at Kaiser Permanente. Now we'll build on those concepts.

Let's explore some more ways you can protect confidential information at work.

Passwords

Use strong passwords on all of your devices. To create a strong password:

- Do use at least eight characters, if the device permits it.
- Do use both upper- and lowercase letters, and include alphanumeric and special characters.
- Do use a password that's easy for you to remember, but hard for someone else to guess.
- Do **not** use a word that would be found in a dictionary, or a name, login name, date, phone number, address, or Social Security number.
- Do change your password immediately if you think someone else knows it.

Minimum Necessary Principles

Follow minimum necessary principles for using confidential information:

- If you don't need confidential information to complete a task, don't access it.
- If specific information is requested, such as a list of specific members or a person's name, send only that.
- If you need to reply to or forward an email or text message, remove all non-essential PHI from the message before you send it.
- If you're attaching or embedding a spreadsheet or object, remove any sensitive data in hidden columns, rows, or worksheets in Excel, and any sensitive data in PowerPoint graphs, before sending it.

Email Encryption

When you have a job-related reason to send an email message containing confidential information from a KP email address to a non-KP email account, always encrypt the message by using Send Secure in Lotus Notes. If you use Outlook, a smartphone, or a tablet, you must encrypt email messages by typing PHI or ENCRYPT in parentheses or brackets in the subject line.

When you have a job-related reason to send confidential data, especially large files, use the Secure File Transfer system (SFT). SFT allows you to send and receive files securely, both inside and outside of Kaiser Permanente.

System Protection

Even though KP computers are well-protected to prevent and detect most malicious software (malware), the best plan is to not get infected to begin with.

To protect our information and prevent the introduction of viruses onto KP-managed devices (as well as your own):

- Don't open unsolicited email or attachments.
- Don't click unsolicited links.
- Don't download or install applications from unknown sites.
- Be sure you have up-to-date anti-virus software installed on your personal system.

SECURE ELECTRONIC STORAGE

Don't save confidential information on a desktop, laptop, or removable media (such as a flash drive) unless you're granted an exception to do so.

If you have a valid need, work with your supervisor to obtain an exception to the Secure Electronic Storage policy. Failure to comply with this policy may result in disciplinary action, up to and including termination.

Access the Secure Electronic Storage policy from the KP Policy Library:

<http://npl.kp.org/pl/do/public/record?rgid=900&subcatid=5002&VIEW=M&rid=112382601>

DISCUSS COMPLIANCE, FRAUD CONCERNS, AND REPORTING WITH YOUR SUPERVISOR

This course cannot anticipate every compliance-related situation you may face. That's why it's important to talk to your supervisor about your compliance accountabilities.

Having a compliance conversation now will make future compliance discussions easier.

- **Schedule time with your supervisor.**
We advise having this conversation while your questions are still fresh in your mind.
- **Plan for the discussion.**
Prepare specific questions that will ensure you have the information you need to meet your compliance expectations. Use the Compliance Discussion Questions handout to prepare.

Access a pdf copy of Compliance Discussion Questions here:

https://sites.sp.kp.org/teams/lna/ProductResources/General%20Compliance%20Training/ACT2017/GC_ACT2017_CDQ_sp.pdf

THE RISK OF NOT REPORTING

Did you know that most non-compliance cases are uncovered through tips from employees like you?

For example, a hospital in Long Beach received referrals for spinal surgeries. The owner inflated the costs of spinal devices and billed the insurers at the inflated rates, resulting in more than \$500 million in fraudulent bills. This wasn't reported for 16 years.

We can't take that long to speak up. It's a risk to KP when compliance concerns go unreported; the health, financial, and emotional impact can be far-reaching. So why wouldn't we report?

Fear of Retaliation

Some people may worry about the negative impact of reporting compliance concerns. They may be thinking:

"I could lose my job."

"Everyone will think I'm a snitch."

"I won't be anonymous."

An employee who's worried about retaliation for reporting is experiencing fear of retaliation. If you believe you or others are being retaliated against, or being intimidated for reporting an issue in good faith or for participating in an investigation, contact your local management, a compliance resource, or the KP Compliance Hotline. Remember, you can report anonymously.

Rationalization

Some people may justify not reporting compliance concerns. They may be thinking:

"It's none of my business."

"It takes too long to report it."

"Someone else will report it."

If you find yourself coming up with excuses for not reporting concerns, consider the impact of not reporting. Federal laws, including HIPAA, state laws, and our policies require us to take immediate action to reduce harm to members, patients, and employees. And remember, your report could help prevent fraud, waste, and abuse.

REPORT COMPLIANCE CONCERNS

When reporting concerns, having complete information will make it easier for your manager or compliance officer to evaluate the situation and take immediate action.

At a minimum, be prepared to answer the five W's:

- Who's involved?
- What happened?
- When did it happen?
- Where did it happen?
- Why did it happen?

If you don't have all of the information, report as much as you can. Should you need it, the "Reporting Preparation Checklist" is available on the Course Resources page.

MODULE 4: SELF CHECK

Instructions: Select the best answer(s) for each question.

Question 1:

Which of the following are part of your compliance role?

Select all that apply.

- A.** Reporting compliance concerns
- B.** Following the *Principles of Responsibility*
- C.** Checking your work
- D.** Following policies and procedures

Question 2:

True or false?

We can help prevent fraud, waste, and abuse by doing the following:

- Looking for suspicious activity
- Conducting ourselves in an ethical manner
- Ensuring accurate and timely data/billing
- Ensuring we coordinate with other payers
- Keeping up to date with fraud, waste, and abuse policies and procedures, the *Principles of Responsibility*, laws, regulations, and CMS guidance
- Verifying all information provided

Select the best answer.

- A.** True
- B.** False

Question 3:

When reporting compliance concerns, what information should you be prepared to provide?

Select all that apply.

- A.** Who's involved?
- B.** What happened?
- C.** When did it happen?
- D.** Where did it happen?
- E.** Why did it happen?

Summary

Following the rules of the road, looking out for hazards, doing your job well, and navigating the many policies and procedures are a big part of your compliance role. And, like a good driver, you must also keep the environment safe for everyone else by being alert and reporting when something doesn't seem right. That means when you have questions, seek help, either from the *Principles of Responsibility*, or from your supervisor.

When we fulfill our compliance role, we protect confidential information, prevent fraud, waste, and abuse, provide higher quality patient care, and ensure that our services are in alignment with standards.

Fulfilling your compliance role means you act ethically and with integrity, and that you *always* do the right thing and make the *best* decisions.

Summary

Just like the experienced drivers who need to refresh their skills and revisit the rules of the road from time to time, we need to maintain our compliance knowledge. We've reviewed how to protect confidential information, how you can help prevent fraud, waste, and abuse, and how to report any compliance concerns that arise as you focus on your job.

When you take the time to check your work, manage risks, and report something that doesn't seem right, you're protecting Kaiser Permanente, you, your co-workers and — especially — our members and patients from incidents and costly consequences.

We work in a complex and rapidly changing industry, which means it can be hard. Know that you are never alone. The compliance community and leadership are here to support your efforts to do the right thing.

Thank you for taking the time to complete this training.

Meet With Your Supervisor or Manager

Your supervisor, manager, or designated training administrator will review your answers to the self-check questions. Be sure you've answered all of them accurately. This is your time to clarify any information and ask questions about the course.

Complete the Course Completion Form

To receive credit for taking the course, you must complete this form.

1. Receive the course completion form from your supervisor, manager, or designated training administrator.
2. Fill in the required information and sign both signature lines. One signature indicates completion of the course, and one is your *Principles of Responsibility* attestation; both are required.
3. Return the completed and signed course completion form to your supervisor, manager, or designated training administrator.

Complete the Course Evaluation Form

To provide feedback on this course:

1. Complete the course evaluation form distributed by your supervisor, manager, or designated training administrator.
2. Return the form to your supervisor, manager, or designated training administrator.

POST-TRAINING RESOURCES

To view the resources, fact sheets, handouts and other support materials referenced in this course, follow these steps:

Step 1: Go to KP.org/compliance.

Step 2: Select Kaiser Permanente Employees & Physicians.

Step 3: Select *Training* from the top navigation bar.

Step 4: Select Course Resources.

Step 5: Select *Annual General Compliance Training 2017* from the list.