# Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training

## Compliance Department

**careoregon.org**
twitter.com/careoregon
facebook.com/careoregon

CareOregon

# Introduction

This training will cover information on regulatory rules and organizational policies on Fraud, Waste, and Abuse (FWA) which can also be found within our FWA Handbook.

- You should have received our FWA handbook as an attachment with this training. If you did not receive a copy of our FWA Handbook with this training, please contact your business owner or email CareOregonComplianceDepartment@careoregon.org.

This training will also include details on CareOregon's Code of Conduct and your obligation to adhere to CareOregon's compliance program. Your good faith participation in supporting a strong ethical compliance culture is detailed in the CareOregon Code of Conduct.

## *Why Do I Need This Training?*

CareOregon contracts with CMS & OHA to offer health and prescription drug coverage to eligible enrollees of our Medicaid and Medicare plans. As a result, CMS & OHA require:

- Adherence to laws, regulations and guidance
- Education and training for employees at time of appointment and annually thereafter
- A Compliance and Fraud, Waste, and Abuse (FWA) Program supported by the Board of Directors and Senior Management

# Learning Objectives

## Throughout this training you will gain a better understanding of:

- Compliance, Fraud, Waste, and Abuse (FWA), and Health Insurance Portability and Accountability Act (HIPAA) regulations that govern CareOregon
- Relevant laws and examples of potential FWA
- Definitions and examples used to detect and prevent FWA
- CareOregon's Code of Conduct and your obligations to adhere
- How to report compliance and FWA issues

# Compliance Overview

## Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training

CareOregon

# Compliance Program

CMS requires plans to implement an effective compliance program for Medicare Parts C and D plans. CareOregon's compliance program is essential to prevent, detect, and correct Medicare and Medicaid non-compliance as well as fraud, waste, and abuse (FWA).

Medicare and Medicaid regulations (42 CFR 438.608) mandate that our compliance plan is composed of seven core elements. These elements are discussed further on the following slides.

As part of the Compliance Program and supported by CareOregon's Code of Conduct, 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 & any conflict-of-interest concerns

## The Health & Human Services (HHS) Office of Inspector General (OIG) has identified seven core elements of an effective compliance program:

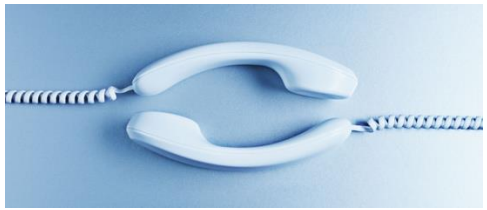
1. Written Policies, Procedures, and Standards of Conduct: Relevant policies are provided to subcontractors at time of contracting.
2. Compliance Officer, Compliance Committee and High-Level Oversight: CareOregon designates a Compliance Officer- Chris Zorn. An internal Compliance committee and compliance committee of the board as designed to ensure appropriate oversight of the compliance program.
3. Effective Training and Education: Training that is provided at time of contracting and annually thereafter.
4. Effective Lines of Communication: Ensuring constant communication with your CareOregon contact is essential for maintaining open lines of communication.
5. Enforcement and Disciplinary Guidelines: Enforcement of disciplinary standards are discussed in contract obligations and the CareOregon Code of Conduct.
6. Effective System for Routine Monitoring, Auditing, and Identifying Compliance Risks: Conduct routine monitoring and auditing of Sponsor's and FDR's operations to evaluate compliance with CMS requirements and contractual obligations, as well as the overall effectiveness of the compliance program.
7. Procedures and System for Prompt Response to Compliance Issues: The Sponsor must use effective measures to respond promptly to non-compliance and undertake appropriate corrective action.

*Even with seven elements we still wouldn't be successful without YOU! Ask questions whenever you see something suspicious or makes you say "hmmm" then email **your CareOregon contract contact for assistance.***

# Credentialing Compliance

- CareOregon, including its subcontractors are obligated to ensure contracted providers meet objective quality standards this is conducted through the credentialing process.

- Within 90 days of receipt of a completed application and every 36 months - to the day, thereafter, the credentialing process must ensure:
  - All providers are enrolled with the State of Oregon as a Medicaid provider
  - No providers are excluded from Federally funded programs (i.e. Medicare, Medicaid, CHIP)
  - If providers are identified on the OIG/SAM lists, CareOregon is obligated to report it to DHHS, OIG, and OHA's Provider Enrollment Unit.
    - Inform CareOregon of any provider identified during the credentialing process.
    - Send to CareOregonComplianceDepartment@careoregon.org and your CareOregon contact.



# Credentialing Compliance

- In accordance with 42 CFR Part 455 Subpart B, during the credentialing/enrollment phase and during recredentialing, CareOregon and its Subcontractors are required to obtain the following information from providers:
    - Disclosures of ownership, control, and affiliations (e.g. SNFs, joint ventures, independent clinical labs, etc.)
    - Significant Business transactions
    - Denial of Federal financial participation
    - Information of any person convicted of crimes
        - Subcontractors must inform CareOregon once made aware of or has reason to believe a provider has been convicted of a crime.
        - Send this information to CareOregonComplianceDepartment@careoregon.org and your CareOregon contact.

*CareOregon does not employ, contract with, or pay prohibited individuals.*

# Consequences of Non-compliance

When we fail to requirements and don't follow our established Compliance Program policies and expectations, it can lead to real consequences which can include:

- Contract termination
- Criminal penalties
- Exclusion from participation in all federally funded programs
- Civil monetary penalties

CareOregon also has disciplinary standards for non-compliant behavior which if not adhered to can lead to:

- Mandatory training or re-training
- Disciplinary action
- Termination
- Other appropriate disciplinary actions

# Fraud, Waste, and Abuse (FWA) Overview

## Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training

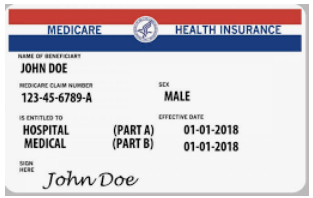
CareOregon

## Fraud, Waste, and Abuse: Spending and Recoveries

Training on FWA prevention and detection is an important piece of maintaining federally funded health care programs of Medicare and Medicaid.

- Medicare provided healthcare for an estimated 62 million people and was estimated to spend $846 billion for 2023. In 2022 Medicare spend was $747 billion. Medicaid provides healthcare for an estimated 78 million people and was estimated to spend $536 billion. This spending accounts for almost 26% of the federal budget *(Medicare 17%, Medicaid 9%)*[1]
- For fiscal year 2023 (ending in September) the DOJ received **$5 billion** in recoveries that involved healthcare fraud and false claims. $1.2 billion was returned to Medicare Trust fund and $98.7 million to Federal Medicaid fund. This only accounts for a small amount of the estimated money spent on healthcare fraud. Low estimates state that 10% of spend is lost to fraud and false claims.

$1.2 billion




$98.7 million


$$ lost to FWA


This is why it's everyone's responsibility to help combat FWA, even YOU!

# Fraud, Waste, and Abuse

## Definitions and Examples

Let's start with the basics, what is FWA and some examples?

**Fraud is defined as** an intentional act of deception, misrepresentation or concealment in order to gain something of value.

- *Fraud examples include knowingly billing for services not furnished or supplies not provided, billing for non-existent prescriptions and knowingly altering claim forms, medical records or receipts to receive higher payment.*

**Waste is defined as** the over-utilization of services (not caused by criminally negligent actions) and the misuse of resources.

- *Waste examples include conducting excessive office visits or writing excessive prescriptions, prescribing more medications than necessary for the treatment of a specific condition and ordering excessive laboratory tests.*

**Abuse is defined as** excessive or improper use of services or actions that are inconsistent with acceptable business or medical practice.

- *Abuse examples include billing for unnecessary medical services, billing for brand name drugs when generics are dispensed, charging excessively for services and supplies and misusing codes on a claim, such as upcoding or unbundling codes.*

# Fraud, Waste, and Abuse Laws and Regulations

To help combat FWA there were laws and regulations put in place such as:

**False Claims Act:** This act creates liability for the submission of a claim for payment to a government reimbursement program, such as Medicare or Medicaid, that is know to be false, in whole or in part.

**Whistleblower and Whistleblower Protections:** Permits private citizens with knowledge of fraud against the U.S. or state government to file suit on behalf of the government against the person/business that committed the fraud. These individuals are known as 'whistleblowers' and the Federal False Claims Act prohibits retaliation against these individuals for their participation in these suits.

**Anti-Kickback Law:** Makes it a crime for individuals or entities to knowingly and willfully offer, pay, solicit, or receive something of value to induce or reward referrals of business under federal health care programs.

**Stark Law (Self-Referral Prohibition Statute):** Prohibits physicians from referring Medicare or Medicaid patients to an entity with which the physician or a physician's immediate family member has a financial relationship.

# Fraud, Waste, and Abuse Penalties

Of course, with laws and regulations come consequences for committing FWA. The following are potential penalties, but actual consequences depend on the violation.

- Civil Money Penalties
- Criminal Conviction/Fines
- Civil Prosecution
- Imprisonment
- Loss of Provider License
- Exclusion from Federal Health Care programs
- Loss of Employment

# Health Insurance Portability and Accountability Act (HIPAA) Overview

## Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training

CareOregon

# HIPAA: Health Insurance Portability and Accountability Act

HIPAA broken into three sections:

- The **Privacy Rule** sets privacy standards to safeguard the privacy of personal health information (PHI) in any form oral, written and electronic, and gives individuals an array of Rights with respect to that information. These Rights are found in the Notice of Privacy Practices.

- The **Security Rule** is a subset of the privacy rule and specifically relates to the protection of Electronic Protected Health Information (ePHI) that is created, received, used or maintained by a covered entity.

- The **Breach Notification Rule** sets requirements for timely notification to individuals and regulatory entities when it is determined that PHI or ePHI has been acquired, accessed, used or disclosed without authorization and outside of Treatment, Payment or Healthcare Operations (TPO).

# Who must comply with the HIPAA regulations?

## Covered Entities and Business Associates

Covered entities are:

- **Health plans:** CareOregon Advantage, Kaiser, United Healthcare etc.
- **Health care clearinghouses:** claims-based companies that submit claims to health plans
- **Health care providers:** such as HouseCall Providers, Multnomah Physical and Dental clinics

Covered Entities

**Business Associates:** individuals or agencies contracted and have a business associate agreement with a Covered Entity to do work on behalf of the Covered Entity

All workforce members of a Covered Entity and Business Associate are mandated to follow the HIPAA laws

# Protected Health Information- What is PHI?

The following individually identifiable data elements, when combined with health information about that individual, make such information Protected Health Information (PHI):

| | | |
|---|---|---|
| • Name | • Social Security Number | • Device identifiers or serial numbers |
| • Address | • Health Plan Number (DMAP/Medicare ID #) | • Biometric identifiers, i.e. finger, retinal or voice prints |
| • Date of birth | • Certificate/License number (Driver's License) | • Full face photographs |
| • Telephone number | • Vehicle license plate number | • Medical record number |
| • Fax number | • Web site uniform resource locator (URL) web address | • Insurance, credit/debit card numbers |
| • Email address | • Internet Protocol (IP) address | • Any other unique identifying number, characteristic, or code |

# HIPAA Privacy Rule: Member Rights

We must work to uphold and support our members' Rights provided under HIPAA

## Notice of Privacy Practices address the right to:

- request restrictions on certain uses and disclosures of PHI
- receive confidential communications of PHI
- inspect and receive a copy of their PHI within 30 days of the request
- request an amendment to their PHI
- receive an accounting of disclosures of PHI
- obtain a paper copy of the Privacy Notice from the covered entity upon request
    - request an alternate means or location of contact
    - 'opt out' of:
        - Phone messages
        - Non-regulatory mailings

# Minimum Necessary Standards

What does this mean?

- Acquire, access, use, or disclose only the amount of information necessary to do your job.
  - It's never ok to use systems to look up someone you know (friends, family, acquaintances, etc.) for yourself or others.
- Disclose only the minimum amount of information necessary for others to do their job.
  - Not every employee needs to see member PHI.
- If you know the member, have someone else help the member.

**Remember** even if you have legitimate access to PHI, it is a violation to access, use or disclose PHI if you do not need it to perform the task you are doing at the time or if it is not your job duty to do so.

**Our responsibility is to:** Treat members' PHI with the same privacy and security you expect others to treat yours.

# HIPAA Security Rule: Safeguarding PHI and ePHI

## Administrative Safeguards

- Policies and procedures
- Training and education
- Contract and business associate agreements

## Physical Safeguards

- Locked records or server rooms
- Key card access badges
- Proper disposal (Shred bins) of PHI
- No visitors where PHI is stored, be acquired or accessed

## Technical Safeguards

- Computer and network permission
- Password protection
- Store PHI on company issued devices
- Encrypt outbound emails that contain PHI
- Deploy audit controls for safeguards in place

## Work from Home Tips

- Use company issued devices to do your work (laptop, iPad, etc.)
- Ensure privacy of health information and have a designated workspace in a private location

# Cybersecurity

You are our first line of defense!

Social Engineering: the use of deception to manipulating people into divulging confidential or personal I information that may be used for fraudulent purposes

- Phishing: is a form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware

Tips to protect our organization:

- To spot phishing emails be wary of generic greetings, urgent requests, poor grammar, suspicious links, and unsolicited attachments
- Always verify the sender's identity independently

# HIPAA Breach Notification Rule

Review contracts to identify additional notifications required

## Individual Breach Notification Letters

- Written in plain language, explain what happened, what information was exposed, what steps are being taken, and how individuals can protect themselves.
- Sent without unreasonable delay, but no later than 60 calendar days after discovery of the breach

## Notification Requirements

### 500 or Less

- Notification to Office for Civil Rights by the 60th of the end of the calendar year in which the breach was discovered

## Additional Notification Requirements

### 500 or More

- Notification to OCR as described
- Notification to prominent media sites within 60 days
- Substitute notice posting on website within 60 days

# 42 CFR Part 2

## Confidentiality of Substance Use Disorder Treatment Records

- 42 CFR Part 2 is a federal regulation that protects the confidentiality of substance use disorder (SUD) treatment records. It applies to all records relating to the identity, diagnosis, prognosis, or treatment of any individual receiving treatment at Part 2 program.
- Part 2 Programs are defined as those who received Federal assistance and who hold themselves out as providing alcohol or drug abuse diagnosis, treatment, or referral of treatment.
- 42 CFR Part 2 laws are stricter than the HIPAA laws and provides additional privacy protections for individuals in substance use disorder treatment. Consent it required
- Accidental disclosure would include acknowledgment of any types of these services.

# HIPAA and 42 CFR Part 2 Authorization and Consent Forms

## HIPAA Authorization Form

- Valid Authorization to Disclose forms must contain:
  - Signature of individual or representative
  - Release to individual or entity
  - Release or exchange of specific information
    - HIV, Genetic Testing, MH and SUD
- Disclosures may be made without authorization for the purposes of Treatment, Payment and Healthcare Operations (TPO)

## 42 CFR Part 2 Consent Form

- Valid Consent forms to disclose must contain:
  - Signed by the individual
  - Release to individual or entity
  - Release must contain for Treatment, Payment, and Operations
- Consent is required for disclosures for Treatment, Payment, and Healthcare Operation (TPO)

With consent for TPO, a Covered Entity may share SUD information, and the records become protected under HIPAA

# Reporting Concerns

## Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training

CareOregon

# Annual HIPAA, Compliance, and Fraud, Waste, and Abuse Training: Reporting Concerns

**You are obligated to report any issues or concerns of potential compliance, privacy, or fraud, waste, and abuse immediately. You have the option to file a report anonymously. The following slides include reporting methods.**

When you file a report, the Compliance Team promptly conducts a preliminary investigation. During the investigation you may be contacted to provide additional information.

If an issue is discovered that is in violation of state or federal regulations, fraud, abuse or other misconduct, it will be sent to the appropriate department for investigation or closed and disciplinary actions will be taken, as appropriate.

All potential and actual fraud, waste, or abuse violations will be reported, by the Compliance Department, to the appropriate government agency as required:

- Medicare: PPI MEDIC, Office of Inspector General (OIG).
- Medicaid: Medicaid Fraud Control Unit of the Oregon Department of Justice and/or OPI (Office of Program Integrity) within seven (7) days - including reports from subcontractors.

*If you filed an anonymous report via EthicsPoint, you will be given a key code to check the status of your report five days after filing. The report will be researched and then responded to within EthicsPoint.*

# Report ***any concern*** through EthicsPoint at https://secure.ethicspoint.com/ or Call the Compliance Hotline at 888-331-6524

You can always report your concern anonymously

We will make sure it gets to the right place.*

| You may also report any concern by: |
| --- |
| Emailing your CareOregon Business or Contract Owner |
| Contacting CareOregon's Compliance Officer, Christian Zorn<br>315 SW 5th Ave Portland, OR 97204<br>Zornc@Careoregon.org<br>(503) 416-4700 |
| Emailing CareOregonComplianceDepartment@careoregon.org |

**CareOregon expressly prohibits retaliation against anyone who – in good faith – reports or participates in the investigation of compliance concerns.**

** When reporting through EthicsPoint you will be asked whether you want to remain anonymous.*

# In addition to reporting to CareOregon, you may also report by calling, writing, or faxing to:

## OHA Office of Program Integrity (OPI)

3406 Cherry Ave. NE
Salem, OR 97303-4924
**Fax:** 503-378-2577
**Secure email:** OPI.Referrals@oha.oregon.gov
**Hotline:** 1-888-FRAUD01 (888-372-8301)

## Medicaid Fraud Control Unit (MFCU)

Oregon Department of Justice
100 SW Market Street
Portland, OR 97201
**Phone:** 971-673-1880
**Fax:** 971-673-1890

## DHS Fraud Investigation Unit

PO Box 14150
Salem, OR 97309
**Hotline:** 1-888-FRAUD01 (888-372-8301)
**Fax:** (503) 373-1525

# High Level Take Aways

- You play a MAJOR role in helping detect, correct and prevent FWA and issues of non-compliance.
- You are obligated to immediately report any known or suspected compliance, HIPAA, or FWA violations.
    - *There are multiple options for you to report, all options are listed on previous two slides.*
- Please disclose any debarment or exclusion from federal healthcare programs to Human Resources immediately.
- Adherence to CareOregon's Privacy and Security policies and procedures and HIPAA rules are taken seriously. Violation can result in termination, lawsuit, and/or criminal prosecution.