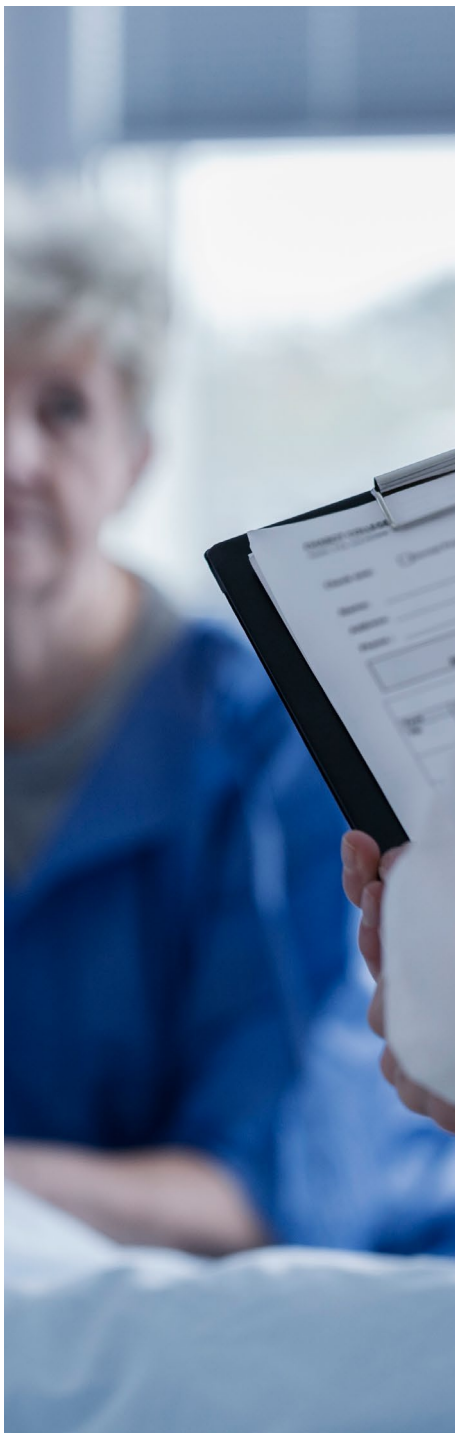
OHSU Health IDS

Compliance Training 2024

for Providers and Subcontractors of OHSU Health IDS Network

OHSU Health

Contents



Welcome 3

Compliance Program 5

Seven Elements of an Effective OHSU Health IDS Compliance Program 6

High-level oversight 6
Effective lines of communication 6
Effective training and education 6
Written policies and procedures 6
Enforcement and disciplinary guidelines 7
Auditing and monitoring 7
Prompt response to compliance issues 8

Fraud, Waste and Abuse 9

Potential consequences of committing fraud and/or abuse 9
Fraud and abuse spectrum 9
Health Care Fraud Statute 10
False Claims Act 10
Anti-kickback Statute 11
Stark Law/Physician Self-Referral 11
Civil monetary penalties 11
Understanding exclusions to the Medicare and/or Medicaid programs 12
Combating Fraud, Waste and Abuse 13
Government reporting 14

HIPAA 15

HIPAA Security Rule 15
HIPAA Privacy Rule 16
HIPAA Breach Notification Rule 18

Quiz 20

Congratulations! 23

Appendix 24

Code of Conduct and Conflict of Interest Policy 24
Annual Cultural Competency training 38
Provider manual 38

Welcome

Reducing fraud in Medicaid is a major objective of health reform.

Each year, providers and staff who work with people using these services need to refresh their education about compliance, the code of professional ethics and how to prevent, detect and report fraud and abuse. This annual compliance training is self-guided.

Training objectives

- Understand OHSU Health IDS commitment to ethical business behavior.
- Learn about an effective compliance program and fraud, waste and abuse.
- Recognize the scope of fraud and abuse.
- Know how to report compliance violations.
- Know HIPAA requirements for Information Security.

Centers for Medicare and Medicaid Services (CMS) require an effective compliance plan from all subcontracted entities and subcontractors of Medicaid (OHSU Health IDS).

You will be asked to attest that you have completed the training. Attestations will be tracked, as this training is a requirement for IDS credentialing.

Deadline for attestation:

- **Submit attestation before Dec. 31 2024.**
- Failure to complete the annual compliance training may lead to termination from the IDS network.

If you have questions, please contact your compliance officer, Nick Gross at nick.gross@modahealth.com or 503-952-5033

Thank you for your attention to this important material.

Abbreviations in this booklet

BA: Business associate

CCO: Coordinated Care Organization

CE: Covered Entity

CMS: Centers for Medicare and Medicaid Services

DHHS: Department of Health and Human Services

FWA: Fraud, waste and abuse

HIPAA: Health Insurance Portability and Accountability Act

HPMS: Health Plan Management System

IDS: Integrated Delivery System

OCR: Office for Civil Rights

OIG: Office of the Investigator General

PHI: Protected health information

USSC: United States Sentencing Commission

Compliance Program

A compliance program helps to prevent, detect and correct issues early to avoid the serious consequences of fraud, waste and abuse.

Core compliance program components for due diligence:

- Written policies and procedures and standards of conduct
- High-level oversight
- Effective training and education
- Effective lines of communication
- Enforcement and disciplinary guidelines
- Auditing and monitoring
- Prompt response to identified issues

The United States Sentencing Commission (USSC) capped an intensive five-year study by announcing the federal Sentencing Guidelines for Organizational Defendants. The guidelines tie an organization's exposure to penalties to its efforts to establish a strong compliance program and undertake other "good corporate citizen" actions.

The Office of Inspector General (OIG) within the Department of Health and Human Services (DHHS) has signaled support for the guidelines by promoting model Compliance Program Guidance for various health care subindustries. The OIG Compliance Program Guidelines stop short of promising reduced penalties for creditworthy compliance programs based on the federal Sentencing Guidelines. However, the guidelines make it clear that a demonstrated commitment to compliance can have a liability- and penalty-shielding impact.

What laws govern CMS Compliance Programs?

- The Office of Inspector General/Department of Justice (OIG/DOJ): www.oig.hhs.gov
- The Federal Sentencing Guidelines, Chapter 8
- Social Security Act: Title 18
- Code of Federal Regulations: 42 CFR Parts 422 (Part C) and 423 (Part D)
- CMS Guidance: Manuals
- Health Plan Management System Memos
- CMS contracts: Private entities apply, and contracts are renewed/nonrenewed each year
- Health and Human Services (HIPAA privacy)
- State Laws: Licensure

Remember
to submit attestation before Dec. 31 2024.

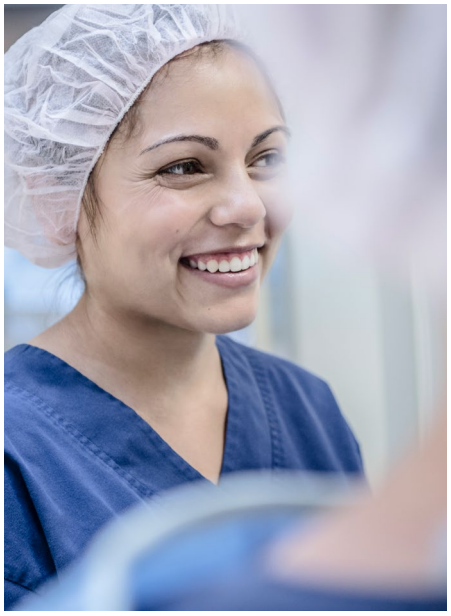
Seven Elements of an Effective OHSU Health IDS Compliance Program

High-level oversight

The OHSU Health IDS board of directors have formally endorsed the compliance program and delegated day-to-day responsibility for the program to senior management.

The primary responsibility for the compliance committee and the compliance officer is implementation, administration and oversight of the compliance program.

- Compliance officer: Part of senior management with responsibility to administer all facets of compliance within the organization. This role has direct access to the governing authority.
- Compliance committee: Made up of senior management, including the executive staff.
  This team develops goals and benchmarks to measure effectiveness.



Effective lines of communication

Hotline: 1-877-733-8313
Email: www.ohsu.edu/hotline

Written policies and procedures

Code of Conduct

- Articulates the expectations of OHSU Health IDS for ethical behavior on the part of employees. The code also lists the principles and values by which OHSU Health IDS operates.

Compliance policies and procedures

Compliance policies and procedures include policies relating to the Compliance Program, Fraud and Abuse detection and prevention and Information Security. These policies are kept up-to-date and are written for easy understanding.

Effective training and education

Training is part of the job, as is networking and collaboration.
Key components of education and training include:

- Conflict identification and fact gathering.
- Review of applicable laws, changes in laws, policies and procedures.
- Consulting compliance personnel, manager and/or hotline for guidance and direction.
- Analyzing the consequences of each course of action.
- Choosing a resolution that meets criteria.
- Decision-making tools such as risk assessments
- Responsibilities of the employee and management

Enforcement and disciplinary guidelines

OHSU Health IDS has well-publicized disciplinary standards. Disciplinary standards articulate expectations for reporting compliance issues and for assisting in the resolution of compliance. Act promptly.

Enforcing disciplinary standards gives the compliance program credibility as well as demonstrating organizational integrity, commitment to compliance and a desire to prevent recurrence.

There are a range of consequences for noncompliance which can be imposed:

- **Programs:** Penalties can be harsh. One example is the federal False Claims Act. Penalties for violations of this act can include fines of up to $11,000 per claim, triple damages and exclusion from federal health care programs.
- **Employees:** Consequences may include warnings, being placed on probation, termination of employment, loss of federal funding, financial penalties and criminal prosecution.

Auditing and monitoring

To identify compliance issues, OHSU Health IDS proactively audits our programs. These efforts include annual oversight audits of each delegated plan partner functions or providers and ongoing monitoring of corrective action, including:

- Review of written materials and documentation prepared.
- Screening for excluded parties.

Prompt response to compliance issues

When compliance issues are identified, OHSU Health IDS responds promptly and undertakes appropriate corrective action.

Noncompliance

Noncompliance is conduct that does not conform to the law, federal or state health care program requirements, or to an organization's ethical and business policies. Noncompliance may include:

- Appeals and grievance review
- Claims processing
- Conflicts of interest
- Credentialing and provider networks
- Documentation and timeliness requirements
- HIPAA
- Oversight and monitoring
- Quality of care

Noncompliance with federal, state or CMS requirements may result in:

- Civil monetary penalties
- Contract termination
- Criminal penalties
- Disciplinary action
- Exclusion from participation in all federal health care programs
- Termination of employment

How to report noncompliance

Reporting options for employees or members:

- Compliance hotline at 1-877-733-8313
- Website form at www.ohsu.edu/hotline
- Compliance Officer Nick Gross, 503-952-5033, nick.gross@modahealth.com

Reporting options for subcontractors:

- Report to contractor's compliance officer

No retaliation

There can be **no** retaliation against anyone for reporting suspected noncompliance in good faith. OHSU Health IDS subcontractors must offer reporting mechanisms that are confidential, anonymous and nonretaliatory.

Fraud, Waste and Abuse

Fraud, waste and abuse results in loss of dollars for medical care for our most fragile members. This results in increased government costs, harm to patient care, overutilization and unfair competition.

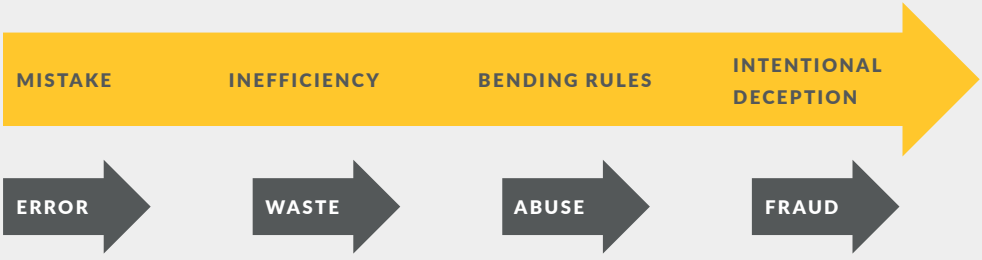
Potential consequences of committing fraud and/or abuse

- Civil prosecution or Civil Money Penalties: Fines can range between **$11,181-$22,363 for each claim**. The damages may be tripled.
- Risk of imprisonment: The individual may be fined, imprisoned or both. If the violations resulted in death, the individual may be imprisoned for any term of years or for life, or both.
- Exclusion from federal health care programs: excluded individuals or entities can't be paid, directly or indirectly by the federal health care programs for any items or services they provide for a minimum of five years.
- Loss of provider license.

Fraud and abuse spectrum

Program Integrity encompasses a range of activities to target the various causes of improper payments.

Fraud doesn't just happen. It moves along the spectrum. There are differences between fraud, waste and abuse. The difference is intent and knowledge. Fraud is willfully and knowingly committing an action to obtain payment when they had knowledge it was wrong. Waste and abuse involve creating unnecessary costs to the program or receiving an overpayment but doesn't involve the same intent and knowledge.



What is fraud, waste and abuse?

Fraud: Intentionally submitting false information to the government or a government contractor to get money or a benefit.

Waste: Overutilization of services resulting in unnecessary costs to a health care program.

Abuse: Requesting payment for items and services when there is no legal entitlement to payment. Unlike fraud, the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

Health Care Fraud Statute

This statute makes it a crime to intentionally defraud a health care benefit program. This is punishable by imprisonment for up to 10 years and fines up to $250,000. Conviction doesn't require proof that the violator had knowledge of the law or specific intent to violate it.

Example of fraud:

The owner of multiple durable medical equipment companies provided no supplies to any members as claimed. This person submitted almost $1 million in false claims, of which, $300,000 were paid (18USC Section 1346).

False Claims Act

This act creates liability for the submission of a claim for payment to the government that is known to be false, whether in whole or in part. 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.

Whistleblower protections under the False Claims Act

- **Whistleblowers:** A whistleblower is a person who exposes information or activity that is deemed illegal, dishonest or violates professional or clinical standards.
- **Protected status:** People who report false claims or bring legal actions to recover money paid on false claims are protected from retaliation.
- **Rewarded:** People who bring a successful whistleblower lawsuit receive a percentage of the money collected. They receive at least 15%, but not more than 30%.

Whistleblower policy

Having a whistleblower policy is mandatory for organizations with 20 or more employees and annual revenues exceeding $1 million.

The whistleblower policy must include:

- Reporting procedures for known or suspected violations of law or company policy.
- A designated person to receive reports, who then reports that information to the Compliance Committee.
- Assurance of no retaliation.
- Distribution of the policy to officers, directors, employees and volunteers who provide substantial service to the organization.

Anti-kickback Statute

This statute makes it a crime for individuals or entities to knowingly and willfully offer, pay, solicit or receive something of value (any service or item) to induce or reward referrals of business under federal health care programs. Violations are punishable by fines up to $100,000 and up to 10 years imprisonment.

Example of a kickback:

Receiving speaker fees from drug manufacturers.

Stark Law/Physician Self-Referral

The Stark Law 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. Improper referrals can lead to overutilization, increased costs, corruption of medical decision-making, reducing member choice and unfair competition.

Penalties include fines and exclusion from participation in federal health care programs.

Example of breaching Stark Law:

A California hospital was ordered to pay more than $32 million to settle violations for maintaining financial relationships with physicians and physician groups outside the fair market value standards or that were improperly documented as exceptions. (42 USC Section 1395nn)

Civil monetary penalties

The Office of Inspector General may impose civil monetary penalties for:

- Arranging or paying for services from an excluded individual or entity.
- Knowing and failing to report and return an overpayment.
- Making false claims.
- Paying to influence referrals.

(42 USC 1320a-7a and section 1128A (a) of the Act)

Remember
to submit attestation before Dec. 31 2024.

Understanding exclusions to the Medicare and/or Medicaid programs

Exclusion means that items or services furnished by a specific provider who has defrauded or abused the Medicare/Medicaid program will not be reimbursed under Medicaid. (42 CFR 455.2)

Excluded individuals or entities cannot be paid, directly or indirectly, by federal health care programs for any items or services that are provided.

Exclusion types:

Mandatory exclusions: OIG is required by law to exclude from participation in all federal health care programs individuals and entities convicted of the following types of criminal offenses: Medicare or Medicaid fraud, as well as any other offenses related to the delivery of items or services under Medicare, Medicaid, SCHIP, or other State health care programs; patient abuse or neglect; felony convictions for other health care-related fraud, theft or other financial misconduct; and felony convictions relating to unlawful manufacture, distribution, prescription or dispensing of controlled substances.

Permissive exclusions: OIG has discretion to exclude individuals and entities on a number of grounds, including (but not limited to) misdemeanor convictions related to health care fraud other than Medicare or a State health program, fraud in a program (other than a health care program) funded by any Federal, State or local government agency; misdemeanor convictions relating to the unlawful manufacture, distribution, prescription or dispensing of controlled substances; suspension, revocation, or surrender of a license to provide health care for reasons bearing on professional competence, professional performance or financial integrity; provision of unnecessary or substandard services; submission of false or fraudulent claims to a Federal health care program; engaging in unlawful kickback arrangements; defaulting on health education loan or scholarship obligations; and controlling a sanctioned entity as an owner, officer or managing employee.*

**Definitions taken from the OIG website.*

Exclusion checks

- OHSU Health IDS is responsible for conducting monthly checks for exclusions and before payment is made.
- Subcontractors should screen against the OIG's list of exclusions. (Find this list at www.oig.hhs.gov/fraud/exclusions.asp).
- Subcontractors should self-disclose if they discover they have employed an excluded individual.
- Maintain documentation of all searches.

Combating Fraud, Waste and Abuse

Activities and controls in place to combat FWA:

- Have claims auditors conduct post-processing claims review.
- Utilize management review.
- Monitor practitioner grievance and appeals.
- Confirm that services billed by the provider were received by the member (Oregon Health Plan).
- Provide training about potential FWA.
- Provide a FWA reporting hotline.

Responsibilities to report FWA

If you suspect noncompliance or suspect fraud, waste or abuse, please:

- Report to the OHSU Health IDS-designated Compliance Officer Nick Gross at nick.gross@modahealth.com

OR

Call the Anonymous Compliance Hotline at 1-877-733-8313

OR

Send a message through www.ohsu.edu/hotline.

Report Medicare FWA directly to CMS: 1-800-294-8455.

Report to your supervisor or manager.

Government reporting

Federal level

To report to the federal government, please use one of the following contact methods:

HHS Office of Inspector General

- Phone: 1-800-TIPS (1-800-447-8477)
- TTY: 1-800-377-4950
- Fax: 1-800-223-8164
- Email: HHSTIPS@oig.hhs.gov
- Online: https://oig.hhs.gov/fraud/report-fraud/index.asp

Mailing address:
Office of Inspector General
ATTN: OIG Hotline Operations
P.O Box 23489
Washington, DC 20026

State level – Oregon

Medicaid Fraud Control Unit (MFCU)
Oregon Department of Justice

Phone: 971-673-1880
Fax: 971-673-1890

Mailing address:
Oregon Department of Justice
ATTN: MFCU
100 SW Market St.
Portland, OR 97201

Office of Program Integrity (OPI)

Phone: 1-888-372-8301
Fax: 503-378-2577
Secure email:
OPI.Refferals@oha.oregon.gov
Online: www.oregon.gov/oha/FOD/PIAU/Pages/Report-Fraud.aspx

Mailing address:
Office of Program Integrity
3406 Cherry Ave. NE
Salem, OR 97303-4924

Where to Report a Case of Fraud or Abuse by a Member

DHS Fraud Investigation Unit

Hotline: 1-888-FRAUD01
(888-372-8301)
Fax: 503-373-1525 Attn: Hotline
Online: https://www.oregon.gov/odhs/financial-recovery/Pages/fraud.aspx

Mailing address:
P.O. Box 14150
Salem, OR 97309

Regulations about compliance

- 42 CFR 422.503 (b) (4) (vi)
- 42 CFR 423.504 (b) (4) (vi)
- Medicare Managed Care Manual Chapter 21
- Medicare Prescription Drug Benefit Manual Chapter 9
- U.S Sentencing Guidelines Chapter 8

HIPAA

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required Health and Human Services to adopt national standards for electronic health care transactions and code sets, unique health identifiers and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. *

The Health Insurance Portability and Accountability Act

CFR Part 164: HIPAA

- Security Rule
- Privacy Rule
- Breach Notification Rule

**Taken from the OCR website.*

HIPAA Security Rule

We are required to guard data integrity, confidentiality and availability. Electronic protected health information (e-PHI) is safeguarded through the implementation of security standards: administrative, physical or technical. There are 51 standards in the Security Rule.

HIPAA called on the Secretary of Health and Human Services to issue security regulations regarding measures for protecting the integrity, confidentiality and availability of e-PHI that is held or transmitted by covered entities. HHS developed a proposed rule and released it for public comment Aug. 12, 1998. The Department received approximately 2,350 public comments. The final regulation, the Security Rule, was published Feb. 20, 2003. The Rule specifies a series of administrative, technical and physical security procedures for covered entities to use to assure the confidentiality, integrity and availability of e-PHI.

The Security Rule establishes a national set of minimum-security standards for protecting all ePHI that a Covered Entity (CE) and Business Associate (BA) create, receive, maintain or transmit. The Security Rule contains the administrative, physical and technical safeguards that CEs and BAs must put in place to secure ePHI. There is a clear message in the Security Rule that protecting an organization's ePHI is the responsibility of all employees, not just the IT department. More than half of the standards are administrative rather than technical.

Administrative standards include:

- Contingency planning
- Facility access
- Media control

Physical standards include:

- Policy and procedure
- Risk assessment and mitigation
- Staff training
- System evaluation
- Workstation use and security

HIPAA Privacy Rule

The HIPAA Privacy Rule establishes national standards for the protection of certain health information. It addresses the use and disclosure of PHI. It also sets standards for individuals' privacy rights to understand and control how their health information is used and shared, including the right to examine and obtain a copy of their health records as well as to request corrections.

General principles for use and disclosures:

- Administrative requirements
- Authorized uses and disclosures
- Enforcement and penalties
- Minimum necessary uses and disclosures
- Notice of Privacy Practices and Individual Rights
- Permitted uses and disclosures

Permitted disclosures

HIPAA permits disclosure without member authorization for:

- Treatment: Provision, coordination or management of health care
- Payment: Reimbursement
- Operations: Quality assessment and improvement, auditing

Under HIPAA, a CE can disclose (orally, on paper, by fax or electronically) PHI to another CE or that CE's business associate for the following subset of health care operations activities of the recipient CE (45 CFR 164.501) without needing patient consent or authorization (45 CFR 164.506(c)(4)).

However, before a CE can share PHI with another CE for one of the reasons noted below, the following requirements must also be met:

- Both CEs must have or have had a relationship with the patient (past or current patient).
- The PHI requested must pertain to the relationship.

Acceptable disclosures without member authorization:

- Conducting case management and care coordination (including care planning).
- Conducting patient safety activities as defined in applicable regulations.
- Conducting population-based activities relating to improving health or reducing health care costs.
- Conducting quality assessment and improvement activities.
- Conducting training programs or credentialing activities.
- Contacting health care providers and patients with information about treatment alternatives.
- Developing clinical guidelines.
- Developing protocols.
- Evaluating performance of health care providers and/or health plans.
- Reviewing qualifications of health care professionals.
- Supporting fraud and abuse detection and compliance programs.

Remember
to submit attestation before Dec. 31 2024.

Minimum necessary provisions

Not every employee needs to see a member's PHI. Under HIPAA's minimum necessary provisions, a health care provider must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. (45 CFR 164.502(b)).

For example, in sharing information with an individual's health plan for population health programs (like a diabetes management program), a provider should disclose the PHI that is necessary for the program to be effective.

Access, use and disclose only the minimum amount of PHI necessary to perform your job duties at the time you are doing it. 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 you are doing it or if it is not your job duty to do so.

There are two things to remember about protecting confidential information:

- Access information only if you need it to do your job.
- Share information only with others who need it to do their job.

HIPAA Breach Notification Rule

If a breach of unsecured PHI occurs, this rule requires written notification to affected individuals and the federal government. Also, it requires notification to the media if more than 500 individuals are affected.

Risk factors to consider for breach notification

An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following four factors listed below.

A breach risk assessment **must** be completed every time acquisition, access, use or disclosure of PHI in a manner not permitted has occurred. This is to demonstrate that there is a low probability that the PHI has been compromised.

The factors listed below must be addressed. If you think you have breached PHI, let your supervisor or privacy/security officer know so an assessment can be completed.

Risk assessment is based on the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of reidentification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the protected health information was in fact acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Online resources for more information regarding compliance

https://oig.hhs.gov/compliance/provider-compliance-training/files/Provider-Compliance-Training-Presentationv2.pdf

https://oig.hhs.gov/authorities/docs/physician.pdf

https://www.cms.gov/About-CMS/Components/CPI

https://www.cms.gov/Outreach-and-Education/MLN/WBT/MLN1857916-OMH-AHE/OMHAHE/ahe/index.html

Quiz

Take the quiz to see what you've learned about compliance.

1. Noncompliance is conduct that conforms to the law, federal or state health care program requirements, or to an organization's ethical and business policies.
   - ☐ True
   - ☐ False

2. Compliance is the responsibility of the Compliance Office, the Compliance Committee and Senior Leadership only.
   - ☐ True
   - ☐ False

3. Ways to report a compliance issue include:
   - ☐ A. Telephone hotlines
   - ☐ B. Report on the sponsor's website
   - ☐ C. In-person reporting to the compliance officer
   - ☐ D. All the above

4. What is the policy of nonretaliation?
   - ☐ A. Allows the sponsor to suspend employees who violate the Code of Conduct.
   - ☐ B. Prohibits management and supervisor from harassing employees for misconduct.
   - ☐ C. Protects employees who, in good faith, report suspected noncompliance.
   - ☐ D. Prevents fights between employees.

5. Correcting noncompliance _____.
   - ☐ A. Protects beneficiaries, promotes efficiency, and avoids recurrence of the same noncompliance.
   - ☐ B. Ensures bonuses for all employees.
   - ☐ C. Neither of the above.

6. If you knowingly submit a false statement of material fact to get a Medicare or Medicaid payment when no entitlement would otherwise exist for someone other than yourself, you did not commit Medicare/Medicaid fraud.

   ☐ True

   ☐ False

7. The federal fraud and abuse laws are the False Claims Act, the Anti-Kickback Statute, the Physician Self-Referral Law (Stark Law), Criminal Health Care Fraud Statute, Social Security Act, and the Civil Monetary Penalties Law.

   ☐ True

   ☐ False

8. Practitioner credentialing and recredentialing is a way to monitor for possible fraud, waste or abuse.

   ☐ True

   ☐ False

9. Any employee who attempts to retaliate or intimidate someone who has reported suspected fraud, waste or abuse will be subject to disciplinary action up to and including termination of employment.

   ☐ True

   ☐ False

Quiz answers

1. **False.**

   Compliance is conduct that conforms to the law, federal or state health care program requirements, or to an organization's ethical and business policies.

2. **False.**

   Compliance is the responsibility of all employees and subcontractors.

3. **D. All the above.**

   There are several ways to report a compliance issue including telephone hotlines, through the sponsor's website and in-person to the compliance department or supervisor.

4. **C. Protects employees who, in good faith, report suspected noncompliance.**

   The policy of nonretaliation is meant to protect employees who report suspected noncompliance in good faith.

5. **A. Protects beneficiaries, promotes efficiency and avoids recurrence of the same noncompliance.**

   Ensuring noncompliance is corrected protects beneficiaries, avoids recurrence of the same noncompliance and promotes efficiency.

6. **False.**

   Knowingly submitting a false statement or claim for payment when no entitlement would exist is considered fraud.

7. **True.**

   These are all examples of federal laws that address fraud, waste and abuse.

8. **True.**

   Practitioner credentialing and recredentialing is a way to monitor for possible FWA.

9. **True.**

   Any employee who attempts to retaliate or intimidate someone who has reported suspected fraud, waste or abuse will be subject to disciplinary action up to and including termination of employment.

?

If you have questions

Please contact your compliance officer, Nick Gross at nick.gross@modahealth.com or 503-952-5033.

Congratulations!

You have reached the end of the training for this year.

As a condition of membership, all providers credentialed with OHSU Health IDS must acknowledge that they have completed annual compliance and fraud, waste and abuse training and clarified any questions or concerns regarding the training.

To attest to your completion of this self-guided course, please sign and return the accompanying attestation form. Download a copy of this booklet, the clinic and provider attestation forms at www.ohsu.edu/health-services/ohsu-health-services-providers-and-clinics. The documents are in the tab for Compliance Guides and Attestations.

Email: ohsuhealthprvrelations@ohsu.edu
Fax: 503-346-8041

Deadline for attestation:

- **Submit attestation before Dec. 31 2024.**
- Failure to complete the annual compliance training may lead to termination from the IDS network.

Thank you for your diligence in following the laws and rules that govern fraud, waste and abuse.

Appendix

Code of Conduct and Conflict of Interest Policy

OHSU Health IDS LLC **Policy & Procedure**		
Company: OHSU Health Services IDS LLC	**Committee Name:** IDS Regulatory Compliance	
Subject: IDS Code of Conduct & Conflict of Interest		
P&P Original Effective Date: 1/1/2020	**P&P Orientation Date:** 1/1/2020	**P&P Published Date:** 1/1/2020
P&P Previous Revision Effective Date: 1/1/2020	**P&P Revision Published Date:** 3/14/2022	
Reference Number: COMP-101	**Next Review Date:** 3/2024	

I. Policy Statement and Purpose

A. This Code of Conduct and Conflict of Interest Policy (the "Code") has been adopted by the OHSU Health IDS and the Board of Directors in order to set forth the general principles and standards to which our Board of Directors as well as any Covered Person, are expected to adhere. All Covered Persons are expected to perform their responsibilities in compliance with the Code, applicable laws, company policies and contractual requirements. In addition, if at any time you believe that a legal or ethical violation has occurred, we ask that you report it to OHSU Health IDS' Compliance Officer or the Compliance hotline.

B. Honesty, integrity and transparency are core values for OHSU Health IDS. Covered Persons are expected to lead with sound, ethical decisions as they interact with members, regulators, providers, suppliers, colleagues and customers at large. As part of our ethics and integrity focus, OHSU Health IDS has adopted this Code of Conduct that describes ethical and legal responsibilities of all Covered Persons acting on behalf of OHSU Health IDS. The Code is the framework for OHSU Health IDS Corporate Compliance Program and is developed to protect the interests of OHSU Health IDS in connection with any transaction or arrangement that might benefit the private interests of any Covered Person, as identified below. The Code provides the framework and a systematic mechanism for disclosing and evaluating potential and actual conflicts; and provides procedures for the

Board of Directors in considering any transaction or arrangement where a conflict may exist.

C. The Code of Conduct applies to all members of the workforce, and the members of Board. OHSU Health IDS will provide a work environment that supports honesty, integrity, and respect in the treatment of workers related to the below areas.

1. **Ethical Conduct and Compliance:** In the performance of duties, staff members will set an example of ethical behavior, and comply with all laws and regulations that govern the business. Staff must never sacrifice ethical and compliant behavior in the pursuit of business objectives.
2. **Accuracy, Retention and Disposal of Documents and Records:** Employees responsible for the integrity and accuracy of any organizational documents or records that are written or modified. Falsifying or altering documents or records is absolutely prohibited. This includes improperly back-dating documents. Employees are also expected to become familiar with and comply with policies and procedures that address the retention and disposal of the organization's documents and records.
3. **Business and Financial Reporting and Records:** In order to provide accurate and reliable financial records, all financial transactions shall be recorded and according to generally accepted accounting principles (GAAP) and OHSU Health IDS policies and procedures. Internal controls have been implemented to provide reasonable assurance that management has authorized a transaction and that it has been properly recorded.
4. **Confidentiality of Business and Member Information:** Employees have an ethical duty to protect the confidentiality of information about trade secrets, confidential business plans, and proprietary business information. When in doubt about whether or not information may be shared, it is the responsibility of the employee to contact the Chief Executive Officer (CEO) or Chief Compliance Officer. Employees are also expected to comply with policies and procedures regarding the confidentiality of member health information. Identifiable member information shall not be shared with others who do not have a legitimate need to know in order to perform their specific job or to carry on business. The use of member, worker or any individual's or entity's information for personal benefit is absolutely prohibited.

5. **Treatment of others:** OHSU Health IDS prohibits all forms of discrimination, including harassment of any kind. Members of the staff shall be treated with dignity and respect, regardless of their age, gender, gender identity, race, ethnicity, national origin, religion, sexual orientation, disability, socioeconomic status, or any other basis protected by applicable law.
6. **Conflict of Interest:** A conflict of interest occurs when personal interests could interfere with their ability to make a fair and objective decision on behalf of OHSU Health IDS or create opportunities for fraud or self-enrichment. Employees should avoid relationships and activities that create, or even appear to create, a conflict of interest. At times, an employee may be faced with situations in which business actions taken on behalf of OHSU Health IDS may conflict with the employee's own personal interests. OHSU Health IDS property, information or business opportunities may not be used for personal gain. If one is unsure whether a conflict of interest exists, they should talk with the person to whom they report or the Chief Compliance Officer.
7. **Gifts and Gratuities:** OHSU Health IDS employees will not accept items from vendors in excess of $50.00 (fifty dollars) per year, per individual. For perishable or consumable gifts, the aggregate value of the gift may not exceed $1,000.00 (one thousand dollars). Regardless of value, no more than two perishable or consumable gifts may be accepted per vendor per year. For gifts that are not perishable or consumable, the aggregate value of the gift may not exceed $250.00 (two-hundred and fifty dollars). All gifts, gratuities, or other compensation from a vendor must be disclosed to the employee's supervisor or manager, or to the CEO for members of OHSU Health IDS board of directors.
8. **Personal Use of OHSU Health IDS Resources:** Anything beyond incidental personal use of OHSU Health IDS materials, supplies or equipment is prohibited without prior approval from executive leadership. Property must not be removed from a facility owned or managed by OHSU Health IDS without proper authorization. If removed, property must be returned to the facility as soon as practicable, after it is no longer needed for authorized purposes. 411.690(2)).

D. Framework of Compliance

1. Antitrust laws make sure competition between companies is fair. These laws also protect the public against business competitors who band together or "collude" to unfairly set prices. You could be breaking these laws if you do things as simple as discuss competitors pricing, terms and conditions of sales; or dealings with customers, suppliers or other competitors. Our competitors include managed care organizations, health care delivery companies and insurance companies that operate in our markets.
2. To the extent that, OHSU Health IDS is subject to the Federal Procurement Integrity Act when bidding on Federal contracts. All Covered Persons must comply with these federal statutes: 41 USC §423 and 18 USC §§207 and 208. In general, these laws prohibit certain business conduct for companies seeking to obtain work from the federal government. More specifically, these laws place restrictions or prohibitions on staff and contractors from engaging in the following activities:
    a. Offering or discussing employment or business opportunities at OHSU Health IDS with current or former agency procurement officials
    b. Offering or giving gratuities or anything of value to any agency procurement official
    c. Seeking or obtaining any confidential information about the selection criteria before the contract is awarded
3. Resources, seeking guidance and reporting violations. Each Covered Person should feel free and comfortable to contact OHSU Health IDS Compliance Officer at nick.gross@modahealth.com, careyba@ohsu.edu or the Compliance Hotline at 1-877-733-8313 (toll free) or www.ohsu.edu/hotline.
4. If OHSU Health IDS initiates an investigation to determine whether there has been illegal or unethical conduct, OHSU Health IDS expects Covered Persons to cooperate with the investigation and disclose all information and records that are relevant to the investigation. Failure to cooperate with an internal investigation is a violation of this Code of Conduct and can lead to disciplinary action and/or contract termination.

5. Once a problem or suspected violation is reported, OHSU Health IDS pledges to quickly investigate and resolve the problem. OHSU Health IDS won't retaliate against any Covered Person for reporting ethics or compliance violations in good faith. As much as possible, OHSU Health IDS takes reasonable precautions to maintain the confidentiality of those who report compliance concerns.
6. Any retaliation against a Covered Person, who, in good faith, reports a suspected violation of this Code, the law, company policies, or contractual obligations, is not permitted and should be immediately reported to the Compliance Officer. Any Covered Person who makes malicious or purposely false reports also violates this Code of Conduct.
7. Failure to follow this Code and any other company policies, applicable laws and contractual obligations will compromise OHSU Health IDS integrity and reputation. No Covered Person is ever authorized to commit or direct another person to commit an unethical and illegal act. In addition, no person can use a contractor, agent, consultant, distributor or other third party to perform any act not allowed by law, this Code, OHSU Health IDS policies or any applicable contractual obligation.

E. Conflict of Interest

1. A Covered Person may have a conflict of interest with respect to a transaction or arrangement whenever they, or any of their family members:
    a. Receives compensation or other funding directly or indirectly from the Corporation and the transaction or arrangement involves such compensation or funding;
    b. Has or anticipates having a compensation arrangement with any entity or individual that: sells or purchases IDS from OHSU Health IDS; has other transactions or arrangements with OHSU Health IDS; or competes with OHSU Health IDS;
    c. Has or anticipates having any ownership interest, investment interest, or serves or anticipates serving as a director or officer of, any entity as described in b above;

d. Has accepted any gift or other favor where such acceptance might create the appearance of influence on the Covered Person (other than gifts of nominal value (less than $50.00), which are clearly tokens of respect and friendship unrelated to any particular transaction).

2. There is no conflict of interest if the Covered Person owns securities of a publicly traded company with which OHSU Health IDS has a transaction or arrangement if the securities owned are less than 5% of the outstanding securities of the publicly traded company; and the fair market value is less than 5% of the Covered Person's annual gross income.

II. Definitions

Covered Person- Any director or officer of OHSU Health IDS, a member of any OHSU Health IDS committee, council, workgroup, task force, and employees and independent contractors of OHSU Health IDS.

III. Procedures

A. Code of Conduct and Conflict of Interest Responsibilities of Covered Persons

1. Every Covered Person is expected perform their duties for OHSU Health IDS in good faith and with the degree of care that an ordinarily prudent person would exercise under similar circumstances. This is known as "Duty of Care."
2. Every Covered Person is expected to be loyal to OHSU Health IDS. A Covered Person is not using their position with OHSU Health IDS for personal profit or gain other personal advantage. This is known as "Duty of Loyalty."
3. Every Covered Person must refrain from conducting any transaction or making an arrangement with other organizations that involve a conflict of interest and should avoid both actual conflicts and the appearance of conflicts of interest. Every Covered Person is required to:
   a. Disclose all actual and potential conflicts; and
   b. Recuse themselves from voting on any transaction or arrangement in which they have a potential or actual conflict of interest, and, if so, requested by the Board's Chair, not be present when any such vote is taken.

B. Disclosure and Evaluation of Conflicts

1. Each Covered Person promptly and fully discloses all material facts of every actual or potential conflict of interest:
    a. Existing at the time when they become a Covered Person;
    b. That arises while they are a Covered Person, at the time such actual or potential conflict arises; and
    c. Annually through the annual Conflict of Interest Questionnaire.
2. The Board Chair discloses to the Board of Directors all conflicts of interest reported to them under this Code. The Board of Directors evaluates the disclosures to determine whether they involve actual conflicts of interest and may attempt to develop alternatives to remove the conflict from the situation.

C. Acting on Conflict of Interest Transactions

1. OHSU Health IDS may enter into a transaction or arrangement in which a Covered Person has a conflict of interest if:
    a. The Covered Person has disclosed the conflict of interest according to this Code
    b. A majority of directors who have no interest in the transaction or arrangement approve the transaction or arrangement at a Board meeting after determining, in good faith and after reasonable investigation, that the transaction or arrangement is fair and reasonable to OHSU Health IDS and is in OHSU Health IDS best interest;
    c. Any Covered Person who has an actual or potential conflict with respect to a transaction or arrangement does not participate in and, if so, requested by the OHSU Health IDS Chair, is not present for the vote regarding the transaction or arrangement (however, that Covered Person may appear at a meeting to answer questions concerning the transaction or arrangement); and
    d. The Board of Directors relies upon appropriate comparability data, such as an independent appraisal or an independent compensation study, in reaching its determination as to the equity and reasonableness of the transaction or arrangement to OHSU Health IDS.

2. It is not a violation of the Code if all the requirements for formal approval, outlined above, are not satisfied, so long as the transaction or arrangement is equitable to OHSU Health IDS.

D. Code of Conduct and Conflict of Interest Records of Proceedings

1. The minutes of the Board of Directors described above shall contain:
    a. The names of the persons who disclosed an actual or potential conflict of interest or otherwise were found to have a conflict of interest, and the nature of the conflict of interest; and
    b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement considered and the appropriate comparability data relied upon, and a record of any votes taken.
2. The minutes are prepared by the next succeeding meeting of the Board of Directors meeting.
3. Disposal or destruction of all records is governed by law and policy. The retention of records will be in accordance with legal and regulatory requirements. Records pertaining to litigation (current/threatened), government investigation or audit shall not be destroyed.
4. Records will be maintained in appropriate format (paper, electronic copies and images) and available within a reasonable timeframe. Records are maintained for a period of ten (10) years.

E. Fraud and Abuse Reporting Obligation and Resources

1. Personal Obligation to Report: Covered persons are responsible to report any activity that appears to violate applicable laws, rules, regulations, or the Code of Conduct. If a concern has been reported and one believes that it has not been resolved, contact the Chief Compliance Officer.
2. Resources for Guidance: OHSU Health IDS encourages discussions regarding concerns with a manager, CEO or President or the Chief Compliance Officer. The Compliance Officer may be reached via the Hotline at 1-877-733-8313 or at www.ohsu.edu/hotline. OHSU Health IDS cannot guarantee that it will keep personal identity confidential, but OHSU Health IDS will maintain confidentiality within the limits of the

law and ability to investigate the issues brought to OHSU Health IDS attention. OHSU Health IDS absolutely prohibits, and will not tolerate, retaliatory discipline against a worker who reports concerns using the channels described above. Claims of retaliation will be investigated and, if substantiated, appropriate action will be taken. OHSU Health IDS takes health care fraud and abuse very seriously. It is OHSU Health IDS policy to provide information to all employees, contractors and agents about the federal and state false claims acts, remedies available under these acts and how employees and others can use them, and about whistleblower protections available to anyone who claims a violation of the federal false claims acts. OHSU Health IDS will also advise our employees, contractors, and agents of the steps OHSU Health IDS has put in place to detect health care fraud and abuse. An employee, contractor, temporary worker, or volunteer who provides care or has access to clients, client information, or client funds within or on behalf of any entity or agency licensed, certified, registered, or otherwise regulated by the Department or Authority is subject to a standard criminal history check at hire and monthly sanction check.

3. Procedure for Reporting: If it is believed that OHSU Health IDS may have made a false claim as discussed above, Covered Persons are encouraged to: Report it to the Chief Compliance Officer at (877) 733--8313 or at www.ohsu.edu/hotline for further investigation. It may also be reported directly to the federal Department of Justice; reporting to OHSU Health IDS is not required first.
4. Report any retaliation that may be experienced from OHSU Health IDS to OHSU Health IDS or the federal government of a possible false claims act violation to the Federal Department of Justice.
5. OHSU Health IDS Policies and Procedures for Detecting Fraud and Abuse: Policies and procedures for detecting fraud and abuse are found in the OHSU Health IDS Compliance Plan. More detailed information about the False Claims Act is available from the Chief Compliance Officer.
6. Training Policy: OHSU Health IDS will train all new members of the workforce, contractors, and agents regarding federal and state false claims acts and also provides annual and periodic updates for existing members of our workforce, contractors, and agents. All members of OHSU Health

IDS workforce are required to participate in training. All contractors and agents are required to participate in scheduled training, as determined by Chief Compliance Officer.

F. Accounting and Record Keeping

1. Covered Persons must maintain reliable records that facilitate accurate reporting to OHSU Health IDS and governmental agencies and comply with applicable legal requirements.
2. Improper or fraudulent accounting, documentation or financial reporting may be in violation of the law. Adequate documentary evidence must support all cost reports or claims submissions.
3. Every Covered Person is expected to comply with the Health Insurance Portability and Accountability Act (HIPAA) legal requirements regarding Protected Health Information (PHI). PHI includes medical diagnosis and treatments, personal data, billing and contract information. OHSU Health IDS policies regarding handling and use of PHI will be adhered to by all Covered Persons who become our Business Associates pursuant to HIPAA in order to receive or process our Members' PHI. The policies conform to federal and state laws and are designed to safeguard patient privacy.

G. Each Covered Person is responsible to sign a statement acknowledging that they have received a copy of this Code, that they have read and understand its content, and agrees to comply with it. They are also required to complete a Conflict of Interest Questionnaire.

H. If the Board of Directors has reasonable cause to believe that a Covered Person has failed to comply with the Code, the Board may counsel the Covered Person regarding such failure and, if the issue is not resolved to the Board's satisfaction, may consider additional corrective action as appropriate.

IV. Fraud, Waste and Abuse Statutes

A. OHSU Health IDS takes health care fraud and abuse very seriously. It is OHSU Health IDS policy to provide information to all Covered Persons about the federal and state false claims acts, remedies available under these acts and how Covered Persons can use them, and about whistleblower protections available to anyone who claims a violation of the federal false claims acts.

OHSU Health IDS also advises Covered Persons of the steps OHSU Health IDS has put in place to detect health care fraud and abuse. The Federal False Claims Act is a federal law that imposes liability on persons and companies who defraud governmental programs. It is the federal government's primary litigation tool in combating fraud against the government. The law includes a qui tam provision that allows people who are not affiliated with the government, called "relators" under the law, to file actions on behalf of the government (informally called "whistleblowing").

1. Persons filing under the Act stand to receive a portion of any recovered damages. This statute allows a civil action to be brought against a health care provider who:

   a. Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval to any federal employee;

   b. Knowingly makes, uses or causes to be made or used a false record or statement to get a false or fraudulent claim paid; or

   c. Conspires to defraud the government by getting a false or fraudulent claim allowed or paid (31 USC SEC 3729(a)).

2. Examples of a False Claim: Billing for procedures not performed; up-coding health care services; falsifying information in the medical record. Remedies: A federal false claims action may be: brought by the U.S. Department of Justice, or brought by an individual as a qui tam action (this means the individual files an action on behalf of the government); punishable by a civil penalty of between $10,781 and $21,563 per false claim, plus three times the amount of damages incurred by the government; and subject to a statute of limitations that controls how much time may pass before an action may no longer be brought for violation of the law. Under the False Claims Act, the statute of limitations is six (6) years after the date of violation or three (3) years after the date when material facts are known or should have been known by the government, but no later than ten (10) years after the date on which the violation was committed.

3. Federal Whistleblower Protections: Federal Law prohibits an employer from discriminating against an employee who initiated or otherwise assisted in a false claims action. The employee is entitled to all relief necessary to make the employee whole. 31 USC 3730(h).

4. Oregon Whistleblower Statutes: Criminal and civil laws that prohibit Medicaid fraud are outlined below. It is a crime if a health care provider knowingly submits, or causes to be submitted, a claim for payment to which the provider is not entitled. ORS 180.755; ORS 411.675; ORS 165.690.692. A healthcare provider is subject to civil damages if it has been previously warned against certain billing practices. ORS 411.690(2)).
5. Oregon Whistleblower Protections: Oregon law contains several provisions that prohibit retaliatory action by a healthcare provider against an employee who, in good faith, brings evidence of unlawful practices to the attention of the proper authority. ORS 441.181, ORS 441.057, ORS 659A.233, ORS 659A.203. Further, an employee who believes he or she is the victim of retaliation may file a complaint with the Oregon Bureau of Labor and Industries. (ORS 659A.200 – 659A.233).
6. Medicaid Waste and Abuse: In addition to an intolerance of Medicaid fraud, OHSU Health IDS prohibits Medicaid waste and abuse, defined as follows:
    a. Waste: The extravagant, careless, or unnecessary utilization of, or payment for, health care services.
    b. Abuse: An activity or practice undertaken by a member, practitioner, employee, or contractor that is inconsistent with sound fiscal, business or health care practices and results in unnecessary cost to OHSU Health IDS, reimbursement for services that are not medically necessary, or an activity or practice that fails to meet professionally recognized standards for health care.
    c. Additional Information: If you have any questions about this information, contact the Chief Compliance Officer at 503-952-5033 or call the Hotline at (877) 733-8313.
    d. Obeying All Laws: Members of OHSU Health IDS workforce are required to follow all applicable federal, state and local laws. Any member of the OHSU Health IDS workforce who believes theirself to have received instructions otherwise must immediately inform the Chief Compliance Officer or members of the OHSU Health IDS Board of Directors.

B. Oregon State Laws

1. Wrongful Claims (ORS 411.670 – 411.690)
   Any person who submits a claim or accepts a payment from the Department of Human IDS for IDS that were not provided is liable to refund or credit the amount of such payment, and if found to have violated this prohibition after an administrative hearing pursuant ORS chapter 183, shall be liable for treble the amount of the payment wrongfully received.
2. Unlawful Trade Practices (ORS 646.605 – 646.656)
   Any person who wrongfully collects or attempts to collect any debt in excess of what is owed, or by unfair means, may be held liable for the debtor's actual damages or $200, whichever is greater, plus reasonable attorneys' fees. Any person who violates a court injunction or assurance of voluntary compliance under these provisions may be liable to the state for up to $25,000 per violation.
3. Perjury and Falsification (ORS Chapter 162)
   A person commits the crimes of perjury (if the falsehood is material) and false swearing by making false sworn statements, and can be convicted of a Class C felony or Class A misdemeanor, respectively, A person commits the crime of unsworn falsification by knowingly making any false written statement to a public servant in connection with an application for any benefit, and can be convicted of a Class B misdemeanor.
4. Falsification of Business Records (ORS 165.080)
   A person commits the crime of falsifying business records if, with intent to defraud, the person makes a false entry in business records, alters, deletes or prevents a true entry, or fails to make a true entry in violation of a known, legal duty, and thereby commits a Class A misdemeanor.
5. False Claim for Health Care Payment (ORS 165.690 – 165.698)
   A person or entity commits the crime of submitting a false claim for health care payment by knowingly making or causing to be made a claim for any health care payment that contains any false statement or false representation of material fact in order to receive the payment. It is also a crime for any person or entity to conceal from or fail to disclose to a health care payor the existence of any information with intent to obtain any health care payment to which the person or entity is not entitled.

a. In addition, it is also a crime for any person or entity to obtain or attempt to attain any state-funded medical assistance payment by submitting or causing to be submitted any false claim for payment, or accepting any such payment, for any duplicate claim for payment not clearly labeled as such, or any claim for which payment has already been received from any source, unless clearly labeled as such.

b. These crimes are Class C felonies and may be punishable by up to five years' imprisonment and/or a fine not to exceed $125,000.00.

6. Racketeering (ORS 166.715 – 166.735)
A person commits the crime of racketeering by engaging in a pattern of activity to collect or receive the proceeds of unlawful debts, or conspire or attempt to do so, and may be held liable for up to three times the amount or three times the gross value gained, or the gross loss caused, whichever is greater, plus reasonable attorneys' fees and costs.

V. Related Policies & Procedures, Forms and References

COMP-100 OHSU Health IDS Compliance Plan

Attachment A- Code of Conduct and Conflict of Interest Acknowledgement Form

Annual Cultural Competency training

The Oregon Health Authority requires Cultural Competency training of all health professionals. You can find the Oregon Health Authority-approved Cultural Competence continuing education training options here.

How to fulfill the two hour requirement

- Complete two hours of cultural competency education. This education does not need to be accredited or provide continuing education unit hours.
- The Oregon Health Authority maintains a list of approved current approved cultural competency continuing education that can be used to locate courses if your employer does not offer any.

For more information regarding the Cultural Competence requirement, please visit the Oregon Health Authority Office of Equity and Inclusion website www.oregon.gov/oha/OEI/Pages/CCCE.aspx.

Provider manual

OHSU Health IDS Provider manual is available online at www.ohsu.edu/health-services/ohsu-health-services-providers-and-clinics under the Provider Resources tab.

OHSU Health Services
PO Box 40384
Portland, OR 97240
Customer Service 844-827-6572
www.ohsu.edu/health-services

PAY 21994338 4/24