Compliance Today

Fraud, Waste, and Abuse

Community Health Plan of Washington (CHPW) maintains a fraud, waste, and abuse (FWA) program to prevent, detect, and correct FWA. CHPWs FWA Program is designed to identify potential FWA risk through monitoring and auditing activities and reports from workforce members, CHPW members, providers, first tier, downstream, and related entities (FDR's), other health plans, and state or federal agencies.

Preventing, Detecting, & Correcting FWA

CHPW's providers, and first tier, downstream, and related entities (FDRs) play a vital role in preventing, detecting, and correcting potential FWA.

First, providers and FDRs must comply with statutory, regulatory, and other contractual FWA requirements. **Second**, providers, and FDRs have a duty to report concerns or violations. **Third**, providers and FDRs have a duty to follow CHPW's Standards of Conduct.

How can you prevent and detect Fraud, Waste or Abuse?

- Be aware of suspicious activity.
- Conduct yourself in an ethical manner.
- Ensure you coordinate with other payors.
- Ensure accurate and timely data/billing.
- Verify the information provided.
- Stay up to date on FWA laws, regulations, and CMS guidance; and
- Comply with CHPW's Standards of Conduct, which state that it is everyone's obligation to report suspected instances of FWA.

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 includes the overutilization of services, or other practices that, directly/indirectly, result in unnecessary costs. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

Abuse includes actions that may, directly/indirectly, result in unnecessary costs. 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.

Examples of FWA

Potential Enrollee FWA:

- Does the prescription look altered/forged?
- Have you filled numerous identical prescriptions for this patient, possibly from different doctors?
- Is the person receiving the service/picking up the prescription the actual patient (identity theft)?
- Is the prescription appropriate based on the patient's other prescriptions?
- Does the patient's medical history support the services requested?

Potential Pharmacy FWA:

- Are the dispensed drugs expired, fake, diluted, or illegal?
- Do you see altered prescriptions (changing quantities or "Dispense as Written")?
- Are proper provisions made if the entire prescription cannot be filled (no additional dispensing fees for split prescriptions)?

- Are generics provided when the prescription requires brand be dispensed?
- The Pharmacy Benefit Manager (ESI) billed for prescriptions that were not filled/picked up?
- Are drugs diverted (drugs meant for nursing homes, hospice, etc. sent elsewhere)?

Provider Billing Trends

CHPW has identified common inappropriate billing schemes through our post payment review audits:

- Upcoding coding: provider billing a higher code to receive higher reimbursement. The provider's medical record documentation must support the procedure codes submitted for payment.
- Presumptive and Definitive Testing performed on the same day: If a presumptive test is ordered, a definitive test on the same day is only medically necessary if there is an unexpected result of the presumptive test, as defined in *MM170 Urine Drug Testing in Addiction Treatment and Pain Management* that cannot be explained by a discussion between provider and patient. The unexpected result and discussion must be documented in the medical record. Routine testing or standing orders that are not documented in the treatment plan are not acceptable and claims will be denied.
- Body Mass Index (BMI) as a Primary Diagnosis: Provider must document and submit a clinical condition, such as overweight, obesity or morbid obesity to justify reporting a code for the body mass index on the claim. A claim with a BMI diagnosis as primary is not acceptable and will be denied. AHA Coding Clinic for ICD 2018 4Q.
- Bilateral Procedures and Modifier -50: Procedures identified by its description as "bilateral" requires the provider to not add Modifier 50 (Bilateral Procedure). Modifier 50 applies to (CPT codes 10040-69990) and to radiology procedures performed bilaterally, but not used with surgical procedures identified as "bilateral" (e.g., 27395, lengthening of hamstring tendon, multiple, bilateral), or "unilateral or bilateral" (e.g., 52290, cystourethroscopy, with meatotomy, unilateral or bilateral).
- External Causes of Morbidity (V00-Y99): The external causes of morbidity codes should not be sequenced as the first-listed or principal diagnosis.
- Radiology claims and diagnosis Z01.89: CHPW will not pay Medicaid claims for radiology services with diagnosis code Z01.89. Providers must bill the appropriate medical ICD-10 code.

Reporting Potential FWA to CHPW

- Complete a *Potential Fraud/ID Theft* form (https://www.chpw.org/provider-center/forms-and-tools) then email it to potential.fraud@chpw.org.
- Notify Compliance Officer, Marie Zerda at 206-613-5091 or email compliance.officer@chpw.org.
- Notify FWA Program Manager, Miles Glew at x7844 or email miles.glew@chpw.org.
- Notify the Office of the Inspector General (OIG) at (800) 447-8477, or hhstips@oig.hhs.gov, or http://oig.hhs.gov/fraud/hotline.

For More Information

- Fraud, Waste, and Abuse Policy (CO289)
- Fraud, Waste, and Abuse Procedure (CO290)
- False Claims Prevention and Whistleblower Protections Policy (CO310)

Compliance Today

Exclusion Screening

Community health Plan of Washington (CHPW) and its contracted provider network are prohibited from using federal or state funds to pay for goods and services furnished, ordered, or prescribed by a provider, supplier, employee, or first tier, downstream, and related entity (FDR) excluded by the Department of Health and Human Services (HHS) Office of the Inspector General (OIG) or Systems for Award Management (SAM). CHPW is prohibited by law from contracting or doing business with any person or entity that is currently debarred, suspended, excluded, proposed for debarment, or declared ineligible to perform work under any government contract or subcontract.

CHPW and its FDRs must review both the **List of Excluded Individuals and Entities (LEIE)** (at https://oig.hhs.gov/exclusions/exclusions_list.asp) and the **Excluded Parties List System (EPLS)** (at https://sam.gov/content/exclusions) lists before hire or contract of any workforce member, provider, consultant, or FDR, and monthly thereafter.

The LEIE includes health care providers and suppliers and the EPLS includes suppliers and vendors (non-health care providers) excluded from participation in federal or state health care programs.

If an individual or entity is identified during the LEIE and EPLS exclusion screening process, or by notification from the Washington State Health Care Authority (HCA), the Centers for Medicare & Medicaid Services (CMS), or the Washington State Office of the Insurance Commissioner (OIC), then CHPW must:

- Terminate employment, the contractual relationship, or the control relationship with the excluded individual or entity immediately and no later than five (5) business days from the date of discovery.
- Immediately recover any payments it discovers for goods or services that directly or indirectly benefit the excluded individual or entity; and
- Report the discovery, payments made, and termination to the appropriate state or federal agency.

Contracted Vendor Requirements

During the contracting process with CHPW, vendors are required to disclose any individual/entity with an ownership or control interest of 5% or more in the vendor.

Vendors must immediately disclose:

- Any exclusion or other event resulting in the vendor or individual/entity ineligible to perform work related directly/indirectly to a federal or state health care program.
- If the vendor or any individual/entity contracted by the vendor is convicted of any criminal/civil offence; and
- Any change in ownership or control (notify CHPW within 35 days of the change).

Requirements for FDRs

CHPW requires its contracted network of providers to maintain exclusion screening policies and procedures for their own workforce members and downstream contractors*. Exclusion screening activities must be performed monthly, with evidence of screening maintained for ten (10) years.

*Downstream contractors are also required to have similar processes.

For More Information

- Exclusion Screening Policy and Procedure (CO318)

CMS 2022 Part C and D Audit Protocol Training

The Centers for Medicare & Medicaid Services (CMS) announced in May 2021 the approval and release of the Final Program Audit protocols used to conduct Medicare Part C and Part D Program Audits.

The Medicare Parts C and D Oversight and Enforcement Group (MOEG) encouraged organizations to review the protocols*, including the crosswalk of changes*, in preparation for upcoming audits.

The MOEG hosted a series of User Calls in August 2021 to provide training on the protocols.

If you were unable to attend any of the sessions, the PPT presentations, are available on the CMS Education and Learning page at: Outreach and Education. *CMS will also post audio recordings, once available.* Links to each presentation is listed below:

Organization Determinations, Appeals and Grievances: https://www.cms.gov/files/document/2021-audit-training-odag508.pdf

Formulary Administration: https://www.cms.gov/files/document/2021-audit-trainingfa508.pdf

Coverage Determinations, Appeals and Grievances: https://www.cms.gov/files/document/2021-audit-trainingsession-2coverage-determinations-appeals-and-grievances508.pdf

Special Needs Plan Care Coordination: https://urldefense.com/v3/__https://www.cms.gov/files/document/2021-audit-trainingsession-3special-needs-plans-care-coordination508.pdf

Compliance Program Effectiveness (CPE): https://urldefense.com/v3/__https://www.cms.gov/files/document/2021-audit-trainingsession-3compliance-program-effectiveness508.pdf

The 2022 Part C and D Program Audit Protocols are located on the CMS website at: https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-andAudits/ProgramAudits or at T:\Public\Medicare\CMS Audit Protocols\2022 CMS Audit Protocols.

Acceptable Use Policy

All company technology assets, including but not limited to computer equipment, software, operating systems, storage media, and network and email accounts provided by CHPW and data furnished to workforce members are the property of CHPW and are intended for business purposes use only.

While CHPW desires to provide a reasonable level of privacy, users should be aware that the data they create, store, or move through the corporate systems remain the property of CHPW. All electronic communications are subject to monitoring to enforce security and privacy standards. Workforce members are responsible for exercising good judgment regarding the reasonableness of personal use.

Compliance Today

Workforce members are prohibited from modifying the hardware configuration of any CHPW issued equipment without authorization from Information Services and Technology (IS&T). Workforce members will not modify any predefined configuration settings such as antivirus settings or removal of administrative accounts.

Data that is created, sent, posted for public view, obtained, or requested via the internet, an email system, or any CHPW system must not contain material that could be considered discriminatory, offensive, obscene, threatening, harassing, or intimidating. CHPW reserves the right to audit company owned networks, systems, workstations, or mobile devices on a periodic basis to ensure compliance with this Policy.

Network Connectivity

No personal computers or peripheral devices may be connected to a CHPW computer or network without prior approval from IS&T. Examples of these network devices requiring explicit approval are hubs, switches, wireless access points, other networking devices, and any form of personal computer. This authorization may be rescinded at any time if deemed necessary for the health of the overall network. CHPW IS&T will exclusively manage all wireless access points to ensure proper configuration.

Remote Network Connectivity

Workforce members are responsible for adhering to all CHPW's policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for CHPW.

All users granted remote access privileges must attest and comply with the Acceptable Use Agreement. Attestations must be kept on file with the Human Resources department or other departments as necessary. It is the remote access user's responsibility to ensure that the remote worksite meets security and configuration standards established by CHPW. This includes configuration of personal routers and wireless networks as specified in the Remote Working Guide or other standards issued by IS&T.

Remote access users must take necessary precautions to secure all CHPW's equipment and proprietary information in their possession.

Copying of confidential information, including ePHI, to personal media (hard drive, USB, CD, etc.) is prohibited to all but those the organization has granted prior approval in writing. See Computing Devices and Media Controls Policy (IT131).

Remote users are prohibited from using or printing paper documents that contain PHI without express prior approval from the IS&T department and the Compliance Officer. Documents containing PHI must be shredded before disposal consistent with Information Privacy: Workforce Member Responsibilities Procedure (CO317).

Email Use

All email sent from, received by, and subsequently stored on CHPW 's email systems is considered the exclusive property of CHPW. See also Electronic Communications Policy (EE206).

PHI is not to be sent by email unless the data is first encrypted or is sent by a secure email portal. Refer to the email encryption guidance in the HIPAA Security Policy (CO330) for more information. The use of personal email accounts (Yahoo!, Gmail, Hotmail, etc.) to conduct CHPW business and the forwarding of CHPW email to personal accounts is prohibited.

Security and Confidentiality

Access to CHPW's computing resources is controlled through individual accounts and passwords. Sharing of CHPW user accounts and passwords is not permitted. See HIPAA Security Policy (CO330) and Password Management Policy (IT129) for additional information regarding password requirements. Each user is personally responsible for any access made through their account. Use of systems and networks in attempt to gain unauthorized access is prohibited. Information about CHPW systems including security measures and means of access is restricted to authorized CHPW workforce members.

Monitoring

CHPW workforce members shall have no expectation of privacy in anything they send, receive, or store on any company owned or managed asset. To appropriately manage its information system assets and enforce security policies, CHPW may log, review, or monitor any data stored or transmitted on its information system assets.

For More Information:

- Acceptable Use Policy (IT130)

Compliance Anonymous Reporting

CHPW provides access to a confidential, anonymous **Compliance Hotline** for workforce members to report instances of suspected or detected non-compliance, potential FWA, and other compliance and ethics concerns. The Hotline is operated and available 24 hours a day, seven days a week at **(800) 826-6762**, by NAVEX (vendor). You can also make an anonymous report online by visiting the Compliance Hotline reporting site at: http://chpw.ethicspoint.com/. You can access the online reporting site with the link above, visiting the 'Compliance Hotline' button from the Employee Quick Links on the inside CHPW home page, and from a link on the Compliance Page on inside CHPW.

In order to ensure confidentiality and comfort in reporting, the Hotline vendor does not trace or record calls. When you make a report online, you are provided with a 'Report Key' and create a password in order to follow up on your report. Without these, you will not be able to follow up on your submission. NAVEX is unable to recover this information for you. If you choose to remain anonymous, no one will attempt to identify you. If you choose to identify yourself, CHPW will keep your identity confidential, to the fullest extent possible or allowed by law.

When you make a report, the information is provided to the VP, Compliance Officer and the VP, General Counsel for investigation and resolution. You can request an update on the progress or outcome of the investigation by contacting the Compliance Hotline and using the unique identification number and PIN provided during your initial report, or by logging in to the online reporting tool using the 'Report Key' and password mentioned above.

Reminders and Updates

CHPW's External Websites

CHPW maintains three external websites, one for each line of business. Business owners who have content, or

policies and procedures (P&Ps), located on "the website" should be aware that content or P&Ps they own may be located on one or all the websites. When updated content or P&Ps, ensure content and P&Ps are updated on **all** relevant websites.

CHPW's external websites:

- General CHPW and Medicaid: https://www.chpw.org/
- Medicare: https://medicare.chpw.org/
- Cascade Select: https://chnwhealthinsurance.chpw.org/

For questions or additional information related to the external website or the content on each, contact the Marketing department.

Annual Compliance Program Training and Stards of Conduct Attestation

CHPW assigned annual Compliance Program Training, including the annual Standards of Conduct attestation to all workforce members in April 2021. Training must be completed by **Friday, November 26, 2021**.

As of September 2, 2021, 47% of workforce members have completed training.

Training is assigned through UKG Pro. Contact compliance.training@chpw.org if you have any questions or issues with the training modules.

Recently Updated Compliance Policies and Procedures

- Fraud, Waste, and Abuse Procedure (CO290)
- False Claims and Whistleblower Protections Policy (CO310)
- Privacy Incidents and Breach Notifications Procedure (CO312)
- Cooperation with Auditors and Investigators Procedure (CO328)
- Fraud and Provider Payment Suspension Procedure (CO339)