Compliance Today

The Importance of Auditing and Monitoring

Community Health Plan of Washington (CHPW) is required to have an effective system for routine monitoring and identification of compliance risks that includes internal monitoring and audits, as well as external monitoring and audits to evaluate first tier, downstream, and related entity (FDR) compliance with regulatory and contractual requirements.

A **First Tier Entity** is any party that enters into a written arrangement with CHPW to provide administrative services or healthcare services to our members. The term "subcontractors" is the equivalent of a first-tier entity. A **Downstream Entity** is any party that enters into a written arrangement, below the level of the arrangement between CHPW and a first-tier entity. The term **Related Entity** means any entity that is related to CHPW by common ownership or control and performs some of CHPW's management functions under contract or delegation.

Monitoring and auditing activities validate compliance with regulations, guidance, contractual obligations, state and federal laws, and CHPW's policies and procedures (P&Ps) to protect against non-compliance and potential fraud, waste, and abuse (FWA). Effective monitoring and auditing assists CHPW to proactively identify outliers and implement efforts to correct deficiencies and ensure they are unlikely to reoccur.

The Office of the Inspector General (OIG) notes that of all the deficiencies found during audits, FWA was the largest category. Of those FWA-related findings, 22.1% of organizations did not have an effective compliance program in place.

While monitoring and auditing are often referred to as one activitiy, they are in fact two disctinct activities each with their own purpose and goal. Monitoring is a process that is part of normal operations and is designed to provide continuous observation, ongoing measuring, early identification, and corrective action designed to determine whether problems exist before they can cause non-compliance. Auditing is a formal process with a particular set of standards that includes planning, sampling, testing, validating, and a formalized corrective action plan (CAP) for identified issues.

Monitoring and auditing activities are focused on reducing organizational risk by focusing on processes that are highest risk of potential non-compliance. The Compliance department conducts an annual risk assessment to assess CHPW's compliance and FWA risk areas. Based on the annual risk assessment, the Compliance department develops an Audit Work Plan, which outlines the audits scheduled for the upcoming year.

Any deficiencies or potential risk areas identified through monitoring or audit activities must be addressed and correctly timely. When deficiencies are identified a CAP is issued to the business owner, or FDR, which requires a root cause analysis and the development of a detailed plan to address the root cause, correct the deficiencies, and ensure they are unlikely to reoccur.

The Compliance department utilizes dashboards, self-assessment tools, and business owner reports to document CHPW's monitoring and auditing efforts. In addition, CAPs are tracked and monitored for areas identified to be non-compliant in order to ensure non-compliant areas are corrected. All monitoring, auditing, and corrective action activities are reported to both the CHPW Compliance Committee and the Community Health Network of Washington (CHNW) Ethics Committee.

For more information:

- *Compliance Audit* policy (CO363) and *Compliance Audit* procedure (CO364)
- Medicare Managed Care Manual Chapters 21 & 9, Compliance Program Guidelines

Corrective Action Plans and Root Cause Analysis

A corrective action plan (CAP) is a formalized way to document known deficiencies, identify remediations, and track corrective actions through completion.

An effective CAP includes a detailed action plan to remedy the noncompliance, a validation of the entire process, and expected completion dates. Effective action plans have three key elements:

1. Specific tasks detailing what will be done and by whom;
2. Timeframe: when will each task be completed and overall expected date of CAP closure, and;
3. Resource allocation: what funds or resources are, or will be, available to support the action plan.

The Compliance department has developed the following templates for CAP management:

- **Internal Corrective Action Plan (iCAP)**, issued by Compliance to a business owner for an identified deficiency.
- **FDR CAP**, issued by Compliance or CHPW business owner to the FDR.

Root Cause Analysis

An essential element of the CAP and remediation process is effective root cause analysis. Root cause analysis is a systematic approach to get to the true root of a problem. Root cause is the fundamental breakdown or failure of a process which, when resolved, prevents a recurrence of the problem. Without an effective root cause analysis, an effective action plan cannot be developed, and the likelihood of the non-compliance is likely to reocurr.

An effective root cause analysis will include:

- How the issue of occurred;
- What factors contributed to the non-compliance, at what level;
- Whether policies and procedures (P&Ps) were in place or disregarded, and;
- Whether mitigating strategies or interventions were identified prior to the issue occurring.

Note: 'Human error' is not the conclusion of a root cause analysis, it is the beginning. A root cause is typically a finding related to a process or system that has potential for redesign to reduce risk.

When a CAP is issued, the Compliance department tracks the completion of the CAP and confirms the remediations have been effective, through a validation audit. Compliance maintains a CAP tracker that is reported to the CHPW Compliance Committee and the CHNW Ethics Committee.

For more information:

- For iCAPs, contact Amie Schippa, Compliance Manager at ext. 5092, or at amie.schippa@chpw.org.
- For FDR CAPs, contact Josh Martin, Delegated Vendor Oversight (DVO) Program Manager at ext. 8805, or at josh.martin@chpw.org.
- *Compliance Audit* policy (CO363)
- *Compliance Audit* procedure (CO364)
- *Delegated Vendor Oversight* policy (CO321)

Compliance Today

Cybersecurity: Loss or Theft of Equipment and Data Threats

The theft of equipment and data is a pervasive threat for organizations. Daily, mobile devices such as laptops, tablets, smart phones, and USB/thumb drives are lost or stolen. While the value of the device is one loss, the consequences of losing a device containing sensitive data is much worse.

If a lost device was not appropriately safeguarded or password protected, the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data. Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to members, applicable regulatory agencies, or the media. Loss of protected health information (PHI) may lead to a clear case of patient identity theft, and, with the potential theft of records, the plan's reputation could be at stake if the information makes it to the dark web for sale.

Workforce members must take extra precautions when working with ePHI or portable eMedia to ensure the security of CHPW's members' information, as well as proprietary and confidential business information.

In September 2016, CHPW implemented a technology control mechanism disabling read/write capabilities for removable eMedia devices, except in limited circumstances. In addition, CHPW laptops are automatically encrypted using Kaspersky. Workforce members with read/write access **must encrypt all portable eMedia** containing ePHI or proprietary and confidential business information using an approved method of encryption. Contact the Help Desk at x8989 if you have questions or need help with encryption.

ePHI and other sensitive information should never be stored on your laptop or desktop computer, but rather on CHPW's secured network. As with printed PHI and your laptop, workforce members **must secure all portable eMedia when away from your desk and at the end of each workday**.

Disposing of Portable eMedia

Portable eMedia such as CDs or DVD/Blu-Rays must be placed in specific secure shredding bins for destruction, just as with printed PHI. Secure shredding bins for portable eMedia are found on the 10th floor. Workforce members must return portable eMedia (such as flash drives or mobile phones) to IS&T when no longer in use, for cleaning and proper disposal.

Loss of Portable eMedia

If you lose a device, **immediately** report the loss to the VP, Compliance Officer, Marie Zerda, at compliance.officer@chpw.org, and to the VP of IS&T, Steve Swanson, at steve.swanson@chpw.org. After you notify the VP, Compliance Officer and VP of IS&T, complete a *Privacy/Security Incident Report* and forward to the Compliance department at compliance.incident@chpw.org.

For more information, see:

- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Removale Media Device* policy (IT111)

42 CFR Part 2

42 CFR Part 2 are federal regulations prohibiting the disclosure of patient information (without patient consent) that could reasonably be used to identify an individual with a substance use disorder (SUD) receiving treatment by a federally assisted SUD program (Part 2 program).

CHPW cannot disclose Part 2 Protected Records without written authorization/consent by the member using the *Authorization to Release Confidential Substance Use Disorder Treatment Information* form. Authorized disclosures of Part 2 Protected Records must be limited to the information necessary to carry out the purpose of the disclosure. When making a disclosure of patient identifying information with member consent, CHPW must include the notice to the recipient that re-disclosure is prohibited unless the member consents in writing to the re-disclosure.

Part 2 prohibits CHPW from affirmatively revealing that a member has been, or is being, disgnosed or treated for a SUD by a Part 2 program. Unless CHPW has a member's valid written consent to disclose patient identifying information, any response to a request for disclosure of member records must be made in a way that will not affirmatively reveal that the member has been or is being diagnosed or treated for a SUD by a Part 2 program.

Part 2 records may be used or disclosed only as permitted by the regulations and may not otherwise be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any Federal or State agency. Restrictions on use and disclosure apply whether the holder of the information believes that the person seeking the information already has the information, or has other means of obtaining the information, is law enforcement or other official, has a subpoena, or asserts any other justification for the disclosure.

If a member consents to a disclosure of their records for payment or health care operations, a lawful holder who receives the records may futher disclose the records as necessary to contractors, subcontractors, or legal representatives to carry out payment or health care operations. However, for purposes of Part 2, care coordination and case management **are not** considered a part of a health plan's health care operations activities. Lawful holders who wish to further disclose patient identifying information, must have a written contract in place with the contractor or legal representative which provides that the contractor, subcontractor, or legal representative is bound by the provisions of Part 2 upon receipt of the patient identifying information.

Any CHPW workforce member who knows of an impermissible disclosure or acquisition of Protected Records, or who suspects one has occurred, must **immediately** report the violation to their supervisor and to the Compliance department. Failure to report will result in disciplinary action, up to and including termination.

Steps for reporting a violation are:

1. Complete a *Privacy/Security Incident Report*
2. Email the form to the Compliance department at compliance.incident@chpw.org

For detailed information, including disclosures for minors in Washington State, see the *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367).

Anonymous Compliance 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 now 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 InsideCHPW home page, and from a link on the Compliance department page on InsideCHPW.

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 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

Annual Compliance/FWA Training

CHPW maintains an Education Program by which the Compliance department administers ongoing education and training related to our Compliance Program. Core training for workforce members is provided through a mandatory Training Program, to be completed within **90 days of hire or contract and annually thereafter**.

The Compliance Program Training is comprehensive, covering each of the four sub-programs within the Compliance Program. Examples of topics covered include an overview of CHPW's Standards of Conduct; channels for reporting compliance, ethics, privacy, fraud, waste, or abuse concerns: an overview of the Compliance policies and procedures; consequences of noncompliance; important related laws; and CHPW's monitoring and auditing processes.

The Compliance Program Training consists of six (6) separate modules, accessible through LearningConnect. Each module contains a quiz requiring a passing score of **90%** or higher.

The six modules are:

- Compliance Program
- Use and Disclosure of PHI & 42 CFR Part 2 Substance Use Disorder Records
- Fraud, Waste, and Abuse
- HIPAA and HITECH
- Member Rights & Responsibilities
- Cybersecurity

Annual training was assigned in LearningConnect to workforce members employed in 2018 and earlier on August 12, 2019.

All modules must be completed **no later than end of day, Friday, November 29, 2019.**

If you have any questions related to the Compliance Program Training requirements or the modules, please contact the Compliance department at compliance.training@chpw.org.

Please be sure you complete training using **Chrome**, not Internet Explorer, thank you.

Compliance Today

Expanded DVO Toolkit

In 2018, the Compliance department rolled out a DVO Toolkit that included standard forms and templates to assist business owners who have a delegated relationship with a vendor. This year, Compliance has expanded the DVO Toolkit to include auditing and monitoring tool templates. The goal of the DVO Toolkit is to provide business owners a one-stop-shop for DVO-related forms and templates. The templates are intended to be a starting point to assist business owners.

Information included in the DVO Toolkit:

- Compliance Program and Compliance/FWA Training guides.
- Ownership and Control Disclosure form.
- Delegated Vendor Criteria (used to determine if a vendor is a FDR).
- Delegated Vendor Requirements Checklist (used to ensure all contractual, pre-delegation, and ongoing requirements are met).
- FDR Welcome Letter template.
- Audit Notice and Summary letter templates.
- Audit and file review templates.
- CAP template.
- CAP Tracker template.
- And more

For more information, contact Josh Martin, DVO Program Manager, at x8805, or at josh.martin@chpw.org.

Recently Updated Compliance P&Ps

- *Compliance Education Program* procedure (CO294).
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317).
- *Compliance Audit* policy (CO363).
- *Substance Use Disorder Records Use and Disclosure* policy and procedure (CO367).
- *Compliance Hotline* policy (CO318).
- *Compliance Hotline* procedure (CO320).
- *Cooperation with Auditors and Investigators* procedure (CO328).
- *Fraud, Waste, and Abuse* policy (CO289).
- *Fraud, Waste, and Abuse* procedure (CO290).
- *Fraud and Provider Payment Suspension* procedure (CO339).