CHPW Policies and Procedures (P&Ps)

P&P Development and Updating Process

The business owner developing or updating P&Ps must take the following steps:

1. Identify whether it is a new or existing P&P.
    a. If inew, be sure to check whether it already exists and/or has been retired/archived.
    b. Provide the title to the **Policy Procedures** mailbox, to request a document number **prior** to finalizing, and submitting for processing.
2. Use the appropriate template located in the "P&P Templates" library.
    a. **Note: Do not alter the structure/format of the template**.
3. Ensure state and federal laws, contractual requirements, and other regulatory obligations are compliant.
4. List and attach any appendices referenced. If there are none, type "**None**" under the heading "List of Appendices."
    a. Appendix pages should be formatted so that each is on its own page (use cntrl + enter).
5. At a minimum, check appropriate Line of Business (LOB) box(es). List regulatory and contract citations (chapter and section), and NCQA requirements in the "Citations & References" table. The Subject Matter Expert (SME) or business owner must review the document for accuracy and approval.
    a. **Note:** if a P&P is a CHPW corporate-wide P&P (not specific to a LOB), check all LOB boxes.
6. Update the "Revision History" table. The approval date must match the "Last Approval Date" in the table.
7. Perform Spelling & Grammar check prior to submitting.
8. Email the approved Microsoft Word version of the document to Policy.procedures@chpw.org. Never send a redline version.
9. The business owner is responsible for knowing if a P&P must be posted on a CHPW website(s) and for having the document posted. The business owner must submit a TrackIt ticket to have the website(s) updated with the document, as appropriate.
10. Compliance will post the document as a PDF to the Policies and Procedures SharePoint site and archive the previous version. Compliance will send an email to inform the business owner that the P&P has been posted on SharePoint.

P&P Style Guide

The type of document (i.e., Policy, Procedure, Policy & Procedure, Desk Procedure) is part of the document name/title and should be included at the end of the "Document Title" (e.g., Delegated Vendor Oversight Policy).

Avoid using his/her references and instead use gender-neutral language, such as they/their.

Font: Calibri, 12 pt (unless headings), black (unless hyperlink).

Headings and lists: use headings and bullet/numbered list styles built into MS Word and the P&P template. Do not customize. (Bullets or numbers shouldn't be gray and headings shouldn't be blue.)

Acronyms/Abbreviations: be sure to spell out the first instance of an acronym, for example: Delegated Vendor Oversight (DVO). Use the following line of business (LOB) abbreviations within the document:

- Washington Apple Health Integrated Managed Care: WAHIMC
- Behavioral Health Services Only: BHSO
- Medicare Advantage: MA
- Cascade Select: CS

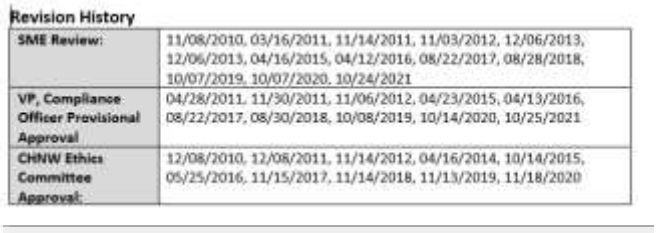
Citations: ensure citations are current and recorded accurately:

- Code of Federal Regulations: 42 CFR Part 2; 42 CFR § 422.503(b)(4)(vi)(C); 45 CFR §§ 160, 162, 164
- Revised Code of Washington: 19.255.010
- Washington Administrative Code: 284-04-625
- Medicare Managed Care Manual: MMCM Ch. 21/PDBM Ch. 9 § 50.4.1
- HCA Contract: § 9.4; Exhibit G § 8

File naming convention: "Delegated Vendor Oversight Policy - CO321.docx"

- The title of the document ("Delegated Vendor Oversight") followed by the type of document ("Policy," or "Procedure," or "Policy & Procedure," etc.) - followed by the document number.
- Do not use "&" in a file name, spell out "and."

Revision History: the below example is the proper intention for recording revision history.



Revision History	
SME Review:	11/08/2010, 03/16/2011, 11/14/2011, 11/03/2012, 12/06/2013, 12/06/2013, 04/16/2015, 04/12/2016, 08/22/2017, 08/28/2018, 10/07/2019, 10/07/2020, 10/24/2021
VP, Compliance Officer Provisional Approval	04/28/2011, 11/30/2011, 11/06/2012, 04/23/2015, 04/13/2016, 08/22/2017, 08/30/2018, 10/08/2019, 10/14/2020, 10/25/2021
CHNW Ethics Committee Approval:	12/08/2010, 12/08/2011, 11/14/2012, 04/16/2014, 10/14/2015, 05/25/2016, 11/15/2017, 11/14/2018, 11/13/2019, 11/18/2020

How to Convert from an Old to a New P&P Template

To ensure prior version, (non-standard formatting) is not copied, follow these steps:

1. Copy content from the old template.
2. Paste into Notepad.
3. Remove any artifacts and correct formatting.
4. Copy from Notepad.
5. Paste to new template.
6. Reformat content using Word's built-in headings, bullet/number list functionality.

For More Information

- CHPW Corporate Policy and Procedure Process Procedure (CO305)

Manager Oversight of Assigned Training and Privacy/Security Violations Process

People managers are responsible for monitoring and ensuring timely completion of any training assigned to their direct reports, as well as Privacy and Security Violation attestations.

Managers monitor and remind staff training must be completed by the **due date**.

UKG Pro provides tools to people managers for monitoring training assigned to their direct reports.

Navigate to UKG Pro Learning and search for the training titled, "View Team Course Completion." This training outlines how people managers can view their direct reports training completion status in UKG Pro.

In addition to ensuring timely workforce member completion of Privacy and Security Violation attestations and assigned retraining, managers are responsible for engaging their HR Business Partner (HRBP) for any coaching and/or disciplinary actions.

For More Information

- HR's article on how to search for training courses in UKG Pro Learning
- Corrective Action and Discipline Policy (EE204)
- HIPAA and Privacy/Security Safeguards Violations Policy (CO325)

Cybersecurity: Microsoft Teams Targeted with Malware

Microsoft Teams is emerging as an increasingly popular attack target for cybercriminals. Cybercriminals are targeting Teams users by planting malicious documents in chat threads that execute Trojans that ultimately can take over end-user machines. Cybersecurity researchers report, "By attaching the file to a Teams chat, hackers have found a new way to target millions of users."

To plant malicious documents, cybercriminals have to obtain access to the application. This is possible when an email is compromised through phishing, resulting in obtaining credentials or other access to a network. The cybercriminal can compromise a partner organization and listen in on inter-organizational chats. They can compromise an email address and use that email to access Teams. They can steal Microsoft 365 credentials, giving them open access to Teams as well as the entire Office suite.

The cybercriminal attaches a .exe file to a chat (called "User Centric") which is an actual trojan. To the end-user, it looks legitimate, because it appears to come from a trusted user. Many users won't think twice and will click on the file.

If that happens, the executable will then install DLL files that install malware as a Windows program

and create shortcut links to self-administer on the victim's machine. The ultimate goal of malware is to take over control of the machine and perform other nefarious activities.

Workforce members must be aware that clicking on links "*anywhere*" can have the same implications as clicking on a link in an email. It is vitally important all workforce members always be cautious of opening attachments or clicking on links, no matter where it is presented.

For More Information

- Information Privacy: Workforce Member Responsibilities Procedure (CO317)
- Acceptable Use Policy (IT130)
- Malware Protection Policy (IT137)
- Password Management Policy (IT129)

Workforce Badge Use and Access

Secured access and proper badge use are important parts of protecting our members' privacy and the security of CHPW's facility. **All individuals are required to visibly display their ID badge while in the building**. It is your responsibility to **always** swipe your badge at every secured access door.

CHPW issues the following types of badges:

- CHPW Employees (Regular or Temporary)
- Contingent Worker (Contractor)
- Board member
- Vendor
- Visitor
- Loaner

Proper use of your ID badge is mandatory and ensures CHPW's facility remains secure. Things to keep in mind:

- Always make sure your badge is visible.
- Always keep your ID (image and name) visible.
- Never follow another employee through the door (tailgate).

All visitors, including children, must be checked in with reception and receive a visitor badge before entering CHPW's facilities. Visitors **must be escorted at all times.**

If you observe someone attempting to tailgate, gently remind them to use their access badge.

If you forget your badge, you can obtain a loaner badge from reception (for a period of up to three (3) days). If reception is not open, **you must wait** until someone is able to issue you a loaner badge before entering CHPW's facility. You can obtain a loaner badge up to two-times per month. More than two-times in a month, your manager will need to obtain and return the loaner badge on your behalf.

For More Information

- Information Privacy: Workforce Member Responsibilities Procedure (CO317)
- Facility Access Controls Physical Security Safeguards Policy (FA310)

Compliance Today

Compliance Hotline Anonymous Reporting

CHPW provides access to a confidential, anonymous **Compliance Hotline** for workforce members to report instances of suspected or detected non-compliance, potential fraud, waste, and abuse (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.

To ensure confidentiality 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 will be required to create a password in order to follow up on your report. You will not be able to follow up on your submission with the Report Key and password. 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 VP, General Counsel for investigation and resolution.

Updates and Reminders:

Compliance Launches e-Visual Control Board

In Compliance's ongoing effort of transparency and providing insight into the functions of the Compliance Team, we have converted the Visual Control Board (located near the Community Lounge) into an e-Visual Control Board on *inside CHPW*.

Visit the new e-Visual Control Board for information related to:

- Incident and Breach reports
- Member Rights requests
- Privacy and Security Violations
- FWA case status
- Audit schedule (by month)
- Audit status
- Lines of Business (LOBs) operational performance results
- Compliance/FWA Training Status Report

Recently Updated Compliance P&Ps

- Advance Directives Procedure (CO292)
- Compliance Education and Training Program Procedure (CO294)

- Member Privacy Policy (CO298)
- Identify Theft Prevention Procedure (CO303)
- CHPW Corporate Policy and Procedure Process Procedure (CO305)
- Member Privacy: PHI Use and Disclosure Procedure (CO316)
- Information Privacy: Workforce Member Responsibilities Procedure (CO317)
- Exclusion Screening Policy and Procedure (CO318)
- Delegated Vendor Oversight Policy (CO321)
- HIPAA and Privacy/Security Safeguards Violations Policy (CO325)
- Cooperation with Auditors and Investigators Policy (CO327)
- Employee Network and Facility Access Authorization (MAC Form) Procedure (CO335)
- Verificaiton of Services (VOS) Policy and Procedure (CO356)
- Compliance Audit Procedure (CO364)
- Substance Use Disorder Records Use and Disclosure Policy and Procedure (CO367)
- Compliance Program Description
- Compliance Education and Training Program Description