COMMUNITY HEALTH PLAN
of Washington™

March 2018

Compliance Program

Compliance Today

Risk Assessments

A **risk** is an event or condition that, if it occurs, could have a negative impact to our members, providers, or to CHPW. **Risk Management** is the process of identifying, assessing, correcting, mitigating, and ongoing monitoring of risks. Risk Assessment is the processes of analyzing, root cause identification, evaluating the level of risk and potential impact, and identifying actions in order to reduce or eliminate identified risks. Through effective Risk Assessment, CHPW can proactively identify areas of risk, gaps in processes, and likelihood of reoccurrence.

Risk can be identified in a number of ways, such as a pattern or problems is observed, changes are made to laws or regulations, or even new technology. All of which leave CHPW open to risk in not meeting its federal and state contractual obligations, meeting the needs of our members, which can potentially have serious consequences. Everyone has the ability to identify potential risk.
As an organization, CHPW utilizes many methods to identify and assess risk.

- The Internal Audit department utilizes model audit methodology to conduct internal audits throughout CHPW.
- The Compliance department also utilizes model audit methodology to conduct internal audits throughout CHPW.
    - In addition, The Compliance department conducts many monitoring and oversight activities to monitor performance and ensure CHPW meets its obligations.
- Various departments and individuals through their daily work conduct ongoing assessments of potential threats, potential vulnerabilities, gaps in process, complexity in regulations, staff competency, and much more.

For more information, see Compliance policy *Compliance Audit Procedure* (CO364)

CHPW Cybersecurity Community

In today's technology-driven world, cybersecurity is a critical issue to be aware of. The always-on, always-connected environment we are accustomed to and the rapid increase of mobile computing means that everything we do in our lives and at work relies on technology and the Internet; communication (email and smartphones), entertainment (digital streaming services such as Hulu, Pandora, and Amazon), transportation (automobile engine systems, airplane navigation), shopping (online retailers, credit card information), and more. Cybersecurity involves protecting this information by preventing, detecting, and responding to attacks.

Our reliance on technology and the Internet brings with it many cybersecurity risks, such as viruses, worms, hackers or intruders, malicious code (malware), spyware/adware, and system and software application vulnerabilities. It is important for each of us to be aware of and recognize these risks and to take steps to minimize hose risks. Steve Swanson, VP of IS&T, notes, "I am confident that CHPW has placed the appropriate attention toward improving our already solid protections against cybersecurity threats." However, the technology world changes on a daily basis and it is important that Community Health Plan of Washington (CHPW) continually manages, re-evaluates, and updates cybersecurity practices and disciplines.

Cyber Security Task Force

In response to the increasing cybersecurity threat, CHPW established the Cybersecurity Taskforce in 2015.

This multi-disciplinary team is comprised of Human Resources, Compliance, Legal, Internal Audit, and IS&T. The group's primary objective is to watch over all CHPW disciplines and practices related to cybersecurity, ensuring that the company is well protected now and into the future. This group is responsible for sharing and implementing industry best practices related to cybersecurity protection. In addition, the group serves as a working group for discussing of, and resolution to, data and systems security opportunities relevant to CHPW business interests. Some accomplishments of the Cybersecurity Taskforce include:

- Multiple annual system and data security assessment and audits conducted by external cybersecurity experts.
- Encrypting CHPW-issued laptop computers.
- Evaluating and updating all relevant policies and procedures to include current cybersecurity language.
- Continued and ongoing enterprise-wide cybersecurity education and training for each CHPW workforce member.

Vendor Security Assessment Program

Established in early 2017, the VSAP program is designed to continually evaluate and monitor our technology vendor partners in possession of or having access to our CHPW data and computing systems. These disciplines have become increasingly important in recent years due to the proliferation of data and information mobilization. It is incumbent upon CHPW to have a continual and current understanding of what vendors are managing our sensitive data and how they protect it from cyber-attacks.

Cyber Security Community

Do you know who comprises CHPW's Cybersecurity Community? The answer is simple; you! Workforce members play a critical role in CHPW's Cybersecurity Community and the protection of CHPW and members' information. Promoting strong cybersecurity is everyone's business. This means that every workforce member of CHPW must take a part in making our enterprise cyber-safe. Activities such as using strong system passwords, locking your laptop properly, not downloading software from the internet, and encrypting emails containing sensitive information are all examples of how each individual can become a contributing member of the Cybersecurity Community here at CHPW.

For more information:

- *HIPAA Security* policy (CO330)
- *Security Incident Response* policy (CO370)
- *Access, Device, and Media Controls* procedure (IT102)
- http://www.healthit.gov

Compliance Audit Process Survey - 2017

With a focus on continuous process improvement, the Compliance department conducts an annual survey related to its audit process. The survey measures business owner experiences and satisfaction with the Compliance department’s audit tools and overall process. The survey is delivered at the end of each year to business owners whom have been audited during that year.

2017 Survey Results Summary

Overall feedback was positive. Business owners see the Compliance process as very collaborative and organized. Audit notices, univers requests, and sample selection are all clear and understandable. Communication between the Compliance department and the business owners is clear and timely. Based on results and business owner feedback, the following enhancements will be implemented:

- Implement entrance and exit conferences.
- Update audit tools and templates to align with Compliance department branding.

For more information, contact Amie Schippa, Compliance Program Manager, at x5092, or at amie.schippa@chpw.org.

Getting to Know Compliance: Andrei Barlahan

Andrei is celebrating his 5th month at CHPW and serves as the FWA Program Manager. He brings with him over 5 years experience as a FWA subject matter expert. Andrei holds a Master's in Business Administration, with an emphasis in Health Administration. In addition, he is an Accredited Healthcare Fraud Investigator (AHFI).

Andrei is passionate about working in the health care industry because it gives him the opportunity to make a difference in People's lives. As the FWA Program Manager in the Compliance department, he is able to make a difference as far as making sure government funds are appropriately being utilized. Andrei loves the culture at CHPW and can easily see that workforce members love their job and truly believe in the organization's mission.

Outside of work, Andrei and his wife enjoy spending time outdoors by hiking and fishing, and enjoy trying new foods. He has also recently taken up ice hokey. One thing people may not know about Andrei is that he loves baking and hopes to one day open his own business called Baked by Drei. In addition, Andrei and his wife blindly moved to Seattle from Long Beach, CA and now does not think they will ever move back.

Andrei and the Compliance team are located on the 9th floor. Come by and say hi!

Regulatory Resources

As a Managed Care Organization (MCO), CHPW has a number of state and federal regulations, as well as contractual requirements to which it must adhere. Often, the hardest part about our roles is knowing where to go to find information on these requirements. Below are a number of regulatory resources that may be useful:

- Medicare manuals: https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Internet-Only-Manuals-IOMs.html

- Washington State regulations (WAC/RCW): http://leg.wa.gov/CodeReviser/Pages/default.aspx
- Federal regulations (CFR): http://www.ecfr.gov/cgi-bin/ECFR?page=browse
- Department of Health and Human Services (HHS): http://www.hhs.gov/
- Centers for Medicare & Medicaid Services (CMS): https://www.cms.gov/
- CMS National Training Program: https://www.cms.gov/Outreach-and-Education/Training/CMSNationalTrainingProgram/index.html
- CMS National Coverage Determinations: https://www.cms.gov/medicare-coverage-database/indexes/ncd-alphabetical-index.aspx
- Local Coverage Determinations: https://med.noridianmedicare.com/web/jfb/policies/lcd/active
- Medicare Learning Network (MLN): https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNGenInfo/index.html
- CMS Outreach & Education Medic: http://medic-outreach.rainmakerssolutions.com/

Compliance Hotline (800) 826-6762

Effective Lines of Communication is one of the Seven Elements of an Effective Compliance Program. In this element, CHPW must have a system in place to receive, record, respond to, and track compliance-related questions, reports of suspected or detected non-compliance, and potential fraud, waste, or abuse (FWA) from workforce members, plan members, and first tier, downstream, and related entities (FDR). Mechanisms for reporting must maintain confidentiality and allow anonymity if desired.

Each workforce member has a duty to report any potential compliance or ethics concerns, potential non-compliance or FWA. CHPW provides access to a confidential **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)**.**

In order to ensure confidentiality and comfort in reporting, the Hotline vendor does not trace or record calls. 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 Compliance Hotline representative documents your concern(s) and comment(s). The Hotline vendor then forwards the report to both the CHPW VP of Talent and Business Process Management, as well as the Compliance Officer for investigation and resolution. Investigation and resolution may involve other departments, including Compliance, Legal, or other CHPW management. 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 the initial report.

CHPW prohibits retaliation for compliance-related questions or reports of potential non-compliance or potential FWA made in good faith. Making deliberately false or malicious reports is prohibited. If you feel you have been threatened or intimidated after making a report, or prior to making a report, you have multiple avenues to report such retaliation, for example: an ELT member, the Hotline, or the HR, Legal, or Compliance departments.

Recently Updated Compliance Policies & Procedures

- *Fraud, Waste, and Abuse* policy (CO289)
- *Advance Directives* policy (CO291)
- *Compliance Education Program* policy (CO293)
- *Member Privacy* policy (CO298)
- *Identity Theft Prevention* procedure (CO303)
- *CHPW Policy and Procedure Process* procedure (CO305)
- *False Claims and Whistleblower Protections* policy (CO310)
- *Privacy Incidents & Breach Notifications* policy (CO311) and procedure (CO312)
- *Member Privacy: PHI & Member Rights* procedure (CO315)
- *Compliance Hotline* procedure (CO320)
- *Delegated Vendor Oversight* policy (CO321)
- *HIPAA & Privacy/Security Safeguards Violations* policy (CO325)
- *Cooperation with Auditors and Investigators* policy (CO327) and procedure (CO328)
- *HIPAA Security* policy (CO330)
- *Employee Network and Facility Access Authorization* procedure (CO335)
- *Filing Forms B, C, and D with the OIC* policy (CO362)
- *Compliance Audit* policy (CO363)
- *Security Incident Response* policy (CO370)
- *Health Plan Management System (HPMS) Memo Intake* policy and procedure (CO372)
- *Compliance Program* description
- *Compliance Education Prograom* description
- *Privacy and Security Program* description
- *Fraud, Waste, and Abuse Program* description
- *Delegated Vendor Oversight Program* description