COMMUNITY HEALTH PLAN
of Washington™

March, 2019

Compliance Program

Compliance Today

HIPAA/HITECH Privacy and Security

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to create greater access to healthcare insurance, mandate protection of privacy of healthcare data, promote the standardization and efficiency in the healthcare industry, and outline safeguards to prevent unauthorized access to protected healthcare information (PHI).

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 to amend HIPAA civil monetary penalties for violations, extend civil and criminal liability to business associates, authorize state attorneys general to enforce HIPAA, and require health plans to notify the Department of Health and Human Services (HHS) of PHI breaches.

HIPAA and HITECH apply to covered entities. Covered entities transmit or maintain health information and include:

- Healthcare providers (doctors, facilities, nursing homes, pharmacies, etc.)
- Health plans (i.e. Community Health Plan of Washington (CHPW))
- Healthcare clearinghouses
- Schools (in limited cases)

Additionally, CHPW workforce members, as individuals who may have access to PHI and who work at a health plan, are responsible for adhering to HIPAA and HITECH.

The HIPAA and HITECH privacy and security rules require CHPW to establish administrative, technical, and physical safeguards to prevent the intentional or unintentional use or disclosure of PHI (including ePHI). In addition, the privacy rule provides rights for members related to their PHI and governs the use and disclosure of PHI.

The **minimum necessary standard**, a key protection of the HIPAA privacy rule, requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. Access to PHI should be limited to only those who need access to the information in order to carry out their job duties and limit the amount of PHI an individual may have access to, maintaining the minimum necessary to complete the task.

Non-compliance in adhering to HIPAA, HITECH, or CHPW's Privacy and Security policies and procedures places CHPW and our members at risk. The HIPAA enforcement rule contains provisions relating to compliance and investigations, the imposition of civil monetary penalties for violations, and procedures for hearings. HITECH penalties range from $100 - $50,000 per incident depending on the category and severity of the violation. There may be penalties imposed even if you can demonstrate that you did not know the law or that there was a reasonable cause for the violation.

For more information:

- Department of Health & Human Services Health Information Privacy
- *HIPAA and Privacy/Security Safeguards Violations* policy (CO325)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Member Privacy: PHI and Member Rights* procedure (CO315)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)

Compliance Today

CHPW Cybersecurity Community

Cybersecurity is a critical issue for everyone 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. 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 those 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 daily and it is important that CHPW continually manages, re-evaluates, and updates cybersecurity practices and disciplines.”

Cyber Security Task Force

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 oversee CHPW’s disciplines and practices related to cybersecurity, ensuring that CHPW 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.

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, CHPW data and computing systems. These disciplines have become increasingly important in recent years due to the proliferation of data and information mobilization. CHPW must know which 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 responsibility. This means that every CHPW workforce member 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 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 Launches New Fraud Webpage

The National Health Care Anti-Fraud Association (NHCAA) estimates that the financial losses to health care fraud are in the tens of billions of dollars each year. In fiscal year 2017, the Federal Government recovered $2.6 billion in its efforts combatting health care fraud. In addition, investigations conducted by the Department of Health and Human Services' Office of Inspector General (HHS-OIG) resulted in 788 criminal actions against individuals or entities that engaged in crimes related to Medicare and Medicaid, and 818 civil actions.

CHPW's Compliance department maintains a fraud, waste, and abuse (FWA) program to prevent, detect, and correct FWA. This integrative program is designed to address issues across divisions and departments discovered through monitoring and auditing activities and reports from workforce members, CHPW members, first tier, downstream, and related entities (FDR), other health plans, and state or federal agencies.

The Compliance department has been improving ways workforce members and external partners can anonymously report compliance-related matters and are pleased to announce the launch of an updated Fraud page on the CHPW website.

This new page is an easily accessible resource for general FWA information and an avenue for streamlined reporting. This page provides general information on FWA, links to government resources, and information on how to report suspected FWA; including a new anonymous online reporting form.

You can access the new page at: https://www.chpw.org/fraud-and-identity-theft.

For more information, visit:

- *Fraud, Waste, and Abuse policy* (CO289).
- *Fraud, Waste, and Abuse procedure* (CO290).
- *False Claims Prevention and Whistleblower Protections policy* (CO310).
- *Fraud, Waste, and Abuse Program Description*.

Enhanced Compliance Hotline Reporting

Community Health Plan of Washington (CHPW) is committed to conducting business with the highest degree of ethics, integrity, and compliance with laws. Our Standards of Conduct set forth these commitments and provide standards for our conduct across our CHPW workforce, governing body, and our first tier, downstream, and related entities (FDRs).

CHPW's Standards of Conduct are an extension of our Mission and organizational values, and go beyond complying with laws; the standards reflect our expectations that CHPW's staff, governing body, and contracted partners (FDRs) will conduct all business with honesty, dignity, and respect for our members, and that all activities are conducted with the utmost degree of integrity. It is important that each of us understand and follow CHPW's Standards of Conduct, comply with all applicable laws, and refrain from business situations that would place CHPW at risk or jeopardize CHPW's integrity and reputation in the community.

In an ongoing effort to improve current processes for anonymous reporting, the Compliance department is happy to announce the expansion of the Compliance

Hotline reporting to include an online report form option.

You can still report concerns by calling the Compliance Hotline at (800) 826-6762, or by completing the new online form. Both the Compliance Hotline and online reporting form are managed by NAVEX Global. The Hotline and online reporting form are available 24 hours a day, 7 days a week.

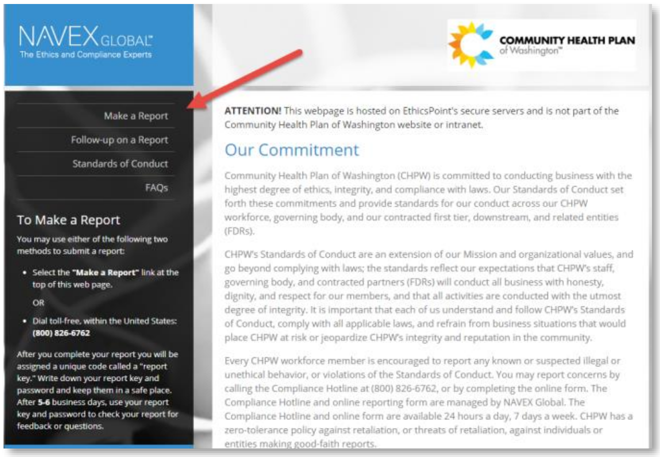
As a reminder, CHPW has a zero-tolerance policy against retaliation, or threats of retaliation, against individuals or entities making good-faith reports.

In order to ensure confidentiality and comfort in reporting, NAVEX does not trace or record calls. If you choose to remain anonymous, no one will attempt to identify you. All reports of suspected violations will be thoroughly investigated in a discrete and confidential manner. Reports of suspected violations are forwarded to CHPW's Compliance Officer and the Vice President, General Counsel.

You can visit the new Compliance Hotline reporting site at: http://chpw.ethicspoint.com. You can access the online reporting site with the link above, visiting the 'Compliance Reporting' button from the Employee Quick Link on the InsideCHPW home page, and from a link on the Compliance department page on InsideCHPW.

How to Make an Online Report

Select the 'Make a Report' link on the left side navigation menu.



To Make a Report

You may use either of the following two methods to submit a report:

- Select the **"Make a Report"** link at the top of this web page.

OR

- Dial toll-free, within the United States: **(800) 826-6762**

After you complete your report you will be assigned a unique code called a "report key." Write down your report key and password and keep them in a safe place. After **5-6** business days, use your report key and password to check your report for feedback or questions.

ATTENTION! This webpage is hosted on EthicsPoint's secure servers and is not part of the Community Health Plan of Washington website or intranet.

Our Commitment

Community Health Plan of Washington (CHPW) is committed to conducting business with the highest degree of ethics, integrity, and compliance with laws. Our Standards of Conduct set forth these commitments and provide standards for our conduct across our CHPW workforce, governing body, and our contracted first tier, downstream, and related entities (FDRs).

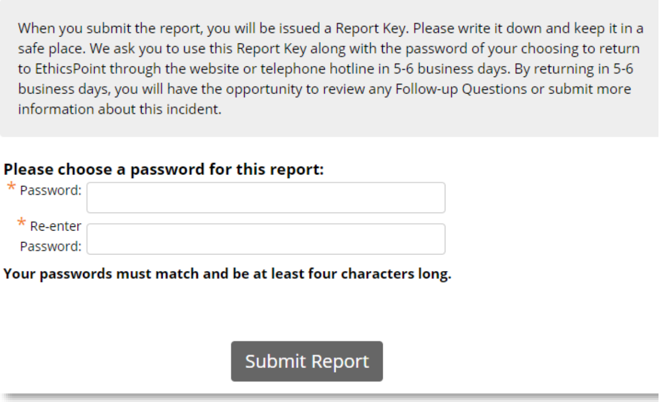
CHPW's Standards of Conduct are an extension of our Mission and organizational values, and go beyond complying with laws; the standards reflect our expectations that CHPW's staff, governing body, and contracted partners (FDRs) will conduct all business with honesty, dignity, and respect for our members, and that all activities are conducted with the utmost degree of integrity. It is important that each of us understand and follow CHPW's Standards of Conduct, comply with all applicable laws, and refrain from business situations that would place CHPW at risk or jeopardize CHPW's integrity and reputation in the community.

Every CHPW workforce member is encouraged to report any known or suspected illegal or unethical behavior, or violations of the Standards of Conduct. You may report concerns by calling the Compliance Hotline at (800) 826-6762, or by completing the online form. The Compliance Hotline and online reporting form are managed by NAVEX Global. The Compliance Hotline and online form are available 24 hours a day, 7 days a week. CHPW has a zero-tolerance policy against retaliation, or threats of retaliation, against individuals or entities making good-faith reports.

On the following page, select the appropriate category for the report you wish to make. Complete all required fields marked with an '*' and provide as much detail as you can to facilitate investigation.

When you have completed inputting the information, create a password for your report and hit submit. The system will issue you a 'Report Key' that you can use to log in and follow up on the status and resolution of your report.

- **Note:** you must retain this password and 'Report Key' the system issued. Without these, you will not be able to follow up on your submission. NAVEX is unable to recover this information for you.



When you submit the report, you will be issued a Report Key. Please write it down and keep it in a safe place. We ask you to use this Report Key along with the password of your choosing to return to EthicsPoint through the website or telephone hotline in 5-6 business days. By returning in 5-6 business days, you will have the opportunity to review any Follow-up Questions or submit more information about this incident.

Please choose a password for this report:

* Password:

* Re-enter Password:

Your passwords must match and be at least four characters long.

ETHICSPOINT IS NOT A 911 OR EMERGENCY SERVICE. Do not use this site to report events presenting an immediate threat to life or property. Reports submitted through this service may not receive an immediate response. If you require emergency assistance, please contact your local authorities.

Contact the Compliance department at compliance.training@chpw.org if you have any questions.

Compliance Audit Process Survey – 2018

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

2018 Survey Results Summary

Overall feedback was positive. Business owners see the Compliance audit process as very collaborative and organized. Audit notice, universe requests, and sample selections are clear and understandable. Communication between the Compliance department and the business owner is clear and timely. Comparing results to the prior year, respondents' experience illustrates improvement in the quality of content in the forms, reports, and communication providing a better experience than in previous years.

In 2019, the Compliance department will phase in an online review process to review samples as part of the audit.

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

Reminders and Updates

Recently Updated Compliance Policies and Procedures

- *Fraud, Waste, and Abuse* procedure (CO290)
- *Advanced Directives* policy (CO291)
- *Compliance Education Program* policy (CO293)
- *Compliance Program* policy (CO300)
- *Privacy Incidents and Breach Notifications* procedure (CO312)
- *Compliance Department and Legal Counsel* policy (CO313)
- *Member Privacy: PHI & Member Rights* procedure (CO315)
- *Exclusion Screening* policy (CO318)
- *HIPAA Security* policy (CO330)
- *Employee Network and Facility Access Authorization MAC Form* procedure (CO335)
- *Verification of Services (VOS)* policy and procedure (CO356)

- *Filing Forms B, C, and D, with the OIC* policy (CO362)
- *Privacy and Security Program* description
- *Delegated Vendor Oversight Program* description