COMMUNITY HEALTH PLAN of Washington™

September 2020

Compliance Program

Compliance Today

HIPAA Protection Reminders While Working from Home

Remember these tips to protect PHI while working from home:

- Protect PHI from friends and family within your house by using a privacy screen on your computer, locking the screen when you walk away, restricting their access to the devices that contain PHI, and being careful not to say PHI aloud in a place where anyone could overhear.
- If you've been approved to print from home, only print information that is absolutely necessary and keep it safe. When finished, be sure to shred the material.
- Never store PHI or confidential / proprietary information on personal computers or devices. If you've been approved to use removable emedia (flash drives, etc.), be sure to only use CHPW approved equipment.
- Encrypt all PHI before it is transmitted in any form.

Conducting Risk Assessments

Risk is an event or condition that, if it occurs, could have a negative impact to Community Health Plan of Washington (CHPW), to its members, or to its providers. **Risk Management** is the process of identifying, assessing, correcting, mitigating, and ongoing monitoring of risks. **Risk Assessment** is the processes of analyzation, 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 problem 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 contractual and regulatory obligations or meeting the needs of its 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:

- *Compliance Program* policy (CO300)
- *Compliance Audit* procedure (CO364)
- *HIPAA Security* policy (CO330)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)

Cybersecurity: Ransomware

Ransomware is a type of malicious software (or malware) that attempts to deny access to a user's data, usually by encrypting the data with a key known only to the attacker. In order for a victim to obtain this key, a ransom payment is required. These types of attacks pose a serious threat to HIPAA covered entities, such as CHPW.

The FBI estimates that ransomware infects more than 100,000 computers a day globally and ransom payments are near $1 billion annually. Ransom payments are only one part of the cost of ransomware attacks. Unrecoverable data, lost productivity, damage to reputation, damaged equipment, forensic investigations, remediation expenses, and legal bills are but a few of the additional costs associated with a ransomware attack.

In recent years, ransomware attacks have become increasingly targeted, attacking specific organizations or industries. Typically, prior to initiating an attack, a hacker usually gains unauthorized access to a victim's information system for the purposes of performing reconnaissance to identify critical services, find sensitive data, and locate backups. After that is done, the ransomware is deployed, infecting as many devices and as much data as possible and encrypting backup files so that recovery is difficult.

Phishing emails and vulnerability exploitation (e.g., exploiting unpatched operating system or application vulnerabilities) are the most common attack vectors for ransomware. Ensuring proper access controls to limit access to sensitive data and adapting security measures with the advancement of technology and tactics are important steps to mitigating the threat of ransomware attacks.

CHPW is protected from ransomware by its anti-malware/anti-virus technology tool, Kaspersky. This tool, in addition to ensuring CHPW has up-to-date Microsoft security patches implemented, makes for a best-case protection scenario from ransomware attacks.

To help protect yourself, and CHPW, practice the following precautions:

- Only open emails from people you know and emails that you are expecting. The attacker can impersonate a sender or the computer belonging to someone you know and may be infected without his or her knowledge.
- Do not click on links in emails if you were not expecting them. The attacker could camouflage a malicious link to make it look like it is from your bank, for example.
- Keep your computer and antivirus tool up-to-date - this adds another layer of defense that could stop the malware (this activity is done by the IS&T Department).

For more information:

- *HIPAA Security policy* (CO330)
- *HIPAA and Privacy/Security Safeguards Violations policy* (CO325)
- *Information Privacy: Workforce Member Responsibilities procedure* (CO317)
- *Security Incident Response policy* (CO370)

FDR Oversight & Compliance Reporting

CHPW maintains a Delegated Vendor Oversight (DVO) Program to ensure CHPW meets its contractual and regulatory obligations related to vendor oversight. First Tier, Downstream, and Related Entities (FDRs) may provide administrative or health care services for members on behalf of CHPW.

The DVO Program has two parts: (I) assisting in the evaluation of potential delegated vendors and; (II) oversight/monitoring of the CHPW business owners

(BO) who have entered into a delegated contractual relationship with a vendor.

Program Oversight

The Compliance Officer and the DVO Program Manager (PM) is responsible for oversight and monitoring of the CHPW business owner (BO). This includes reviewing delegated relationships to ensure CHPW is monitoring and reporting the vendor's performance in meeting and complying with CHPW's contracts with state and federal agencies. The Compliance Officer is responsible for reporting any instances of noncompliance to the CHPW Executive Leadership Team (ELT). In addition, the Compliance Officer along with the BO reports the delegated vendor's performance results to both the CHPW Compliance Committee and the Community Health Network of Washington (CHNW) Ethics Committee.

Business Owner Responsibilities

The BO is the CHPW workforce member who would be best qualified to manage the delegated function, if the function were to be performed by CHPW (i.e., not delegated). The BO must fully understand the delegated vendor relationship and be in a position to influence and enforce the delegated vendor's contractual obligations.

The business owner remains responsible for evaluating the delegated vendor including conducting and completing the pre-assessment, reviewing and approving the delegated vendor contract language, ongoing monitoring and auditing activities, initiating and monitoring Corrective Action Plans (CAPs), and providing the Compliance Officer and DVO PM monthly status reports of the vendor's performance.

The BO must have monitoring and auditing activities in place with its delegates to ensure compliance with CHPW's contractual and regulatory obligations. CHPW BOs are responsible for conducting routine auditing and monitoring activities to ensure the delegated vendors are and remain compliant. Monitoring of delegated vendors for compliance with contractual requirements must include an evaluation to confirm that the delegates are applying appropriate oversight and monitoring of any downstream/subcontracted entities with which the delegated vendor contracts. A delegated vendor that fails to meet contractual obligations must be placed on a CAP detailing how and when the noncompliance will be corrected. A copy of any CAPs issued to FDRs must be forwarded to the Compliance Officer and DVO PM.

Compliance Reporting

To ensure appropriate oversight and monitoring of business owners and FDRS, as well as effective reporting, the Compliance department requires business owners to provide the following types of ongoing reporting to the Compliance Officer and DVO PM:

- Monthly reports of the delegated vendor's performance in meeting its contractual obligations.
- Any instances of non-compliance.
- DVO Oversight Narratives for Ethics and Compliance Committees.
- Copies of CAPs and routine updates of remediation.
- Copies of auditing and monitoring activities outside of day-to-day auditing/monitoring, including, at a minimum, an annual audit of the delegate.
- It is a best practice for business owners to obtain, and forward to Compliance, copies of new downstream contracts, pre-delegation assessment(s), and auditing/monitoring activities of any downstream entities.

- It is a best practice for business owners to obtain, and forward to Compliance, copies of delegated vendors' own audits, to include a summary of the audit work plan and audit results that relate to the services the delegated vendor performs.

For more information:

- *Delegated Vendor Oversight* policy (CO321).
- *Delegated Vendor Oversight Program* description.
- DVO Toolkit for business owners.
- Committees Toolkit for business owners (CHNW Ethics and CHPW Compliance Committees reporting tools).
- Josh Martin, DVO Program Manager, ext. 8805, josh.martin@chpw.org.

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 InsideCHPW 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 & Updates

Reporting Issues of Noncompliance

Reminder: **any issues of noncompliance or any instance of missing a contractual obligation (whether internally or by a CHPW FDR) must be reported to the Compliance department**.

Request to Access PHI

Reminder: all requests to access a member's PHI (whether from the member or a third-party) are forwarded to the Compliance department for vetting and processing. The Compliance department will reach out to other departments for assistance as needed.

Annual Training

Reminder: annual Compliance Program and FWA training is due **by end of day, Friday, November 27, 2020.** As of September 22, 65% of workforce members have completed their training.

If you have not completed training yet, be sure to log into UltiPro Learning and complete the six modules. **Note:** be sure to complete training using **Chrome** not Internet Explorer or Edge.

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.

Annual Standards of Conduct Attestation

Reminder: annual Standards of Conduct attestation is due **by end of day, Friday, November 27, 2020**. As of September 22, 41% of workforce members have attested to receiving, understanding, and abiding by CHPW's Standards of Conduct.

If you have not already done so, visit the article on InsideCHPW to complete your attestation. **Note:** workforce members hired in 2020 complete this in UltiPro as part of their 90-days training requirements.

Recently Updated Compliance P&Ps

- *Privacy Incidents and Breach Notifications* policy (CO311)
- *Compliance Hotline* procedure (CO320)
- *HIPAA Security* policy (CO330)
- *Fraud and Provider Payment Suspension* procedure (CO339)
- *Compliance Audit* policy (CO363)
- *Compliance Audit* procedure (CO364)
- *Substance Use Disorder (SUD) Records Use and Disclosure* policy and procedure (CO367)