COMMUNITY HEALTH PLAN of Washington™

September, 2018

Compliance Program

Compliance Today

Quarterly Compliance Security Audits

The Compliance department conducts a Privacy and Security Audit quarterly. The audit evaluates Community Health Plan of Washington's (CHPW) workforce on its understanding and compliance with general HIPAA requirements and CHPW's privacy and security policies and procedures.

The audit consists of:

- Random workforce member interviews.
- Checking for compliance with privacy and security policies and procedures during and outside regular business hours.

In addition, these audits provide workforce members the opportunity to introduce themselves to Compliance department team members, as well ask any questions they may have related to CHPW's Compliance Program.

Quick reminders to maintain privacy and security:

Physical Safeguards for Workstations: Working with Printed PHI

- All CHPW workforce members, contractors, and agents are required to adhere to the following when working with PHI:
- Keep documents containing PHI facedown when not in use;
- Put printed PHI away in drawers or cabinets at the end of the day;
- Lock office doors when leaving for the day;
- Printed PHI documents should be placed in a secure shredding bin or stored securely;
- When sending printed PHI documents though interoffice mail, ensure the PHI is enclosed in an interoffice envelope; and
- Promptly remove printed PHI from printers and fax machines.

Physical Safeguards for Workstations: Working with Electronic PHI and Mobile Devices6

All CHPW workforce members, contractors, and agents are required to adhere to the following:

- Encrypt ePHI stored on all portable devices, such as laptops, thumb drives, flash drives, and external hard drives;
- Never share usernames or passwords;
- Never leave usernames or passwords visible;
- Lock computer screens when leaving their desk (Ctrl-Alt-Delete + "Lock Computer," or ⊞ L);
- Keep laptops locked to the workstation; and
- When leaving work, secure thumb drives, external hard drives, and any other portable device containing PHI in a drawer or cabinet.

For more information:

- Basics for Privacy and Security
- *HIPAA Security* policy (CO330)
- *Member Privacy* policy (CO298)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)

Cybersecurity: Tips to Prevent Phishing

Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information through electronic communications by impersonating a trustworthy source. For example, an individual may receive a message informing them that their password may have been hacked. The phishing email may instruct the individual to click on a link to reset their password. This link directs the individual to a website impersonating and organization's real website (e.g.,

bank, government agency, email service) and asks for the individual's login credentials (username and password). When entered into this fake website, the person initiating the phising attack records these login credentials and can begin other malicious activities. Alternatively, the link in the phishing message may download malicious software onto the individual's computer. Phishing messages may also include attachments, such as a spreadsheet or document, containing malicious software that executes when the attachment is opened. Phising is one of the primary methods used to distribute malicious software, including ransomware. As a member of CHPW's Cybersecurity Community, every workforce member plays a role in preventing successful phishing attempts.

Ways you can protect yourself, and CHPW, from phishing attempts:

- Only open up 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 for your bank, for example.
- Keep your computer and antivirus tool up-todate - this adds another layer of defense that could stop the malware (this activity is done by the IS & T Department).Be wary of unsolicited third party messages seeking information.
- Contact the Help Desk at ext. 8989 with any questions or to discuss any suspicious messages you've received.

For more information:

- *HIPAA Security* policy (CO330)
- *Member Privacy* policy (CO298)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)

Protecting PHI: Faxing Accuracy

Always make sure you have the correct number before sending.

Remember, only the minimum amount of PHI should be disclosed to accomplish the task. When faxing to a provider or facility, you **must** confirm that you are faxing to the correct number and location for the intended recipient.

Faxes Containing PHI by Conventional Fax Machine

To send a fax by conventional fax machine, the following sequence must be followed:

1. Ensure the information being sent contains the minimum necessary PHI to accomplish the intended purpose;
2. Attach a completed External Fax Cover Sheet for PHI (Appendix B) containing the appropriate disclaimer and CHPW contact information;
3. Enter the fax number and visually verify before the fax is sent; and
4. Collect the fax confirmation sheet and:
    a. The destination fax number matched to the intended recipient's fax number;
    b. The confirmation sheet is stapled to the faxed document; and
    c. The faxed document with confirmation sheet is appropriately filed and locked away.

Compliance Today

Faxes Containing PHI by Digital Fax Solution (JIVA or RightFax)

To send a fax digitally, the following sequence must be followed:

1. Ensure the information being sent contains the minimum necessary PHI to accomplish the intended purpose;
2. The recipient is called and the fax number is verified. If faxes are routinely sent to the same number and a staff member is certain that the number is correct, verification is not necessarily required;
    a. In the event that a fax number is incorrect in JIVA or Xcelys, a request must be sent to Medical Management's Operations Manager to have the number updated.
3. The intended recipient is selected from a pre-populated contact list or entered as a contact; Note: In JIVA: Workforce members must select "OTHER" from the dropdown list for a selected provider's fax number and never "Provider Default" unless it is listed on corresponding documentation supplied by a provider.
    a. Workforce members may add a new contact fax number using the "OTHER" category from the dropdown list. Fax number verification is required when entering a new fax number.
4. The fax number is visually verified before the fax is sent; and
5. The send function is selected, and the fax is verified as queued to be sent.

If you discover a fax containing PHI has been sent to an incorrect fax number, complete a *Privacy/Security Incident Report* form and email the completed form to compliance.incident@chpw.org.

For more information:

- *Member Privacy* policy (CO298)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)

Conflicts of Interest

A conflict of interest can occur when a person or a member of a person's family has an existing or potential interest, or relationship which impairs, or might appear to impair, the person's independent judgement. Family members include a spouse, parents, siblings, children, and others living in the same household.

Workforce members at Director level or above must complete a *Conflict of Interest Statement* and a *Disclosure Statement* upon hire, promotion, when a new conflict arises, and at least annually thereafter. Statements are maintained by the HR department.

Certain relationships with an entity which does business with or directly/indirectly competes with CHNW/CHPW may create a conflict of interest or appearance of conflict of interest. A few examples include:

- Serving as an officer, director, employee, or independent contractor of such an entity.
- Owning or controlling (directly or indirectly) 5% or more of the equity interests of such an entity.
- Reciept of gifts or other favors from such an entity.

A conflict of interest is not inherently illegal or unethical and does not necessarily mean the conflict is

damaging for CHNW/CHPW. Each of the following examples may be permissible given the appropriate disclosure and approval:

- A Board member owns a business that provides print servies for CHPW member materials.
- A Board member leases real estate to CHPW.
- A Board member applies for employment with CHPW.

These examples can be managed with appropriate disclosure and decision-making. Workforce members should seek clarification from their supervisor, HR or the Compliance Officer any time they have questions regarding whether a situation presents a potential conflict of interest.

For more information:

- *Conflict of Interest* policy (EE105)

Compliance Hotline (800) 826-6762

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)**.**

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 (at NAVEX) documents your concern(s) and comment(s). The Hotline vendor then forwards the report to both the CHPW VP of HR and the Compliance Officer 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.

Reminders and Updates

Annual Compliance Program Training

CHPW's annual Compliance Program Training was assigned to workforce members on August 20, 2018. If you were hired before 2018 and have not been assigned this training, contact HR.

Workforce members have until the end of day, Friday, November 23, 2018 to complete training.

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

Note: for best results, complete training using the Chrome browser, not Internet Explorer.

Compliance on InsideCHPW

In the coming months, the Compliance department will be launching and updated page on InsideCHPW. Some features and information you can expect include:

- Who's Who in Compliance
- Forms
- DVO Business Owner Toolkit
- Committee Reporting Toolkit
- More TBD

Compliance Today

Recently Updated Compliance Policies and Procedures

- *CHPW Policy and Procedure Approval Process* procedure (CO305)
- *HIPAA Security* policy (CO330)
- *Responding to Threats of Physical Violence* procedure (CO336)
- *Exclusion Screening* procedure (CO337)
- *Fraud and Provider Payment Suspension* procedure (CO339)
- *Compliance Audit Procedure* (CO364)
- *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367)