COMMUNITY HEALTH PLAN
of Washington™

May, 2019

Compliance Program

Compliance Today

ePHI and Access Controls

Data and health care informatics help providers better manage the health and wellness of their populations by informing clinical decision-making, promoting evidence-based care at reasonable costs, and improving quality and effectiveness. All this improved access to data increases the risk of impermissible disclosure or access of electronic protected health information (ePHI). The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) states that health information is more than ten times more valuable than credit card information and those victims of health information theft may not know that their information was stolen until years after the event.

Strong security controls and individual diligence are critical to preventing unauthorized access or disclosure of ePHI. Unauthorized access or disclosure is when an individual obtains or receives ePHI that they are not allowed to view or access. One such control is user role-based profiles and access.

CHPW uses role-based job descriptions and defined PHI Access Level Categories to limit employee access to the appropriate level of PHI, required to perform a specific function. There are four (4) categories of PHI access:

- **Frequent:** the position has frequent or daily access and responsibility for PHI. Need to know.
- **Occasional:** the position occasionally encounters PHI, often as incidental to their regular duties. Need to know determined by supervisor or manager.
- **Seldom:** the position seldom encounters PHI in the course of their regular duties and typically only as assigned. Restricted need to know.
- **Never:** the position rarely has access to PHI, in the regular course of daily duties. PHI access should be considered an exception for this position and each exception must be assessed and assigned as needed by the manager or supervisor.

Employees are granted role-based access to relevant systems at the request of their manager. To ensure that the minimum necessary rule is met, the Privacy Officer or a designee periodically reviews a random sampling of job descriptions to verify the appropriateness of assigned PHI Access Levels and compares them against the actual access levels granted in CHPW's systems.

Electronic access to PHI is limited through the use of firewalls and network/system permissions administered by the Information Services & Technology (IS&T) department. Workforce members whose positions change or terminate are tracked by the Human Resources (HR) department, and PHI access permissions are restricted or cancelled accordingly by the IS&T department.

A recent settlement between a Colorado hospital and OCR demonstrate the critical importance of managers properly completing the Move Add Change (MAC) form and process to ensure proper access to, and protection of, ePHI. Pagos Springs Medical Center (PSMC) has agreed to pay $111,4000 to the OCR and adopt a substantial corrective action plan (CAP) because it did not terminate electronic access to ePHI for a former workforce member. Following separation of employment, the former workforce member continued to have remote access to PSMC's systems. OCR Director Roger Severino says, "It's common sense that former employees should immediately lose access to protected patient information upon their separation from employment. This case underscores the need for covered entities to always be aware of who has access to their ePHI and who doesn't."

To ensure the appropriate level of access is granted to a workforce member, the hiring manager (or the business owner in the event of a vendor or auditor) is responsible for partnering with their HR Business Partner to complete and submit a *New Hire Move, Add, and Change (MAC)* form located under Quick Links in ADP at least five (5) business days prior to the workforce member or contractor start date.

When there is a change in job function, it is important that the workforce member's access be confirmed or modified based on their job description. The *Change MAC* form should be submitted at least five (5) business days prior to the workforce member's change in job function.

When a workforce member separates employment (voluntarily or involuntarily), the manager must submit a *Departure MAC* as soon as a separation date has been finalized, but no later than five (5) business days prior to the workforce member's last day of work (in the case of voluntary separation), or immediately (in the case of involuntary separation) noting same-day separation.

Failure to comply with CHPW's MAC form process or any other security policy may result in disciplinary action as described in the policy *Corrective Action and Discipline* (EE204). Disciplinary action may include termination. Legal actions may also be taken if a violation of the law has occurred.

For more information:

- *Employee Network and Facility Access Authorization (MAC Form Procedure)* procedure (CO335)
- *Discipline* policy (EE204)
- *Claims System Security Template Change Management: User Security Maintenance* procedure (IT121)
- *Claims System Security Template Change Management: Template Security Maintenance* procedure (IT122)

The 7 Elements of an Effective Compliance Program

CHPW is required to develop and maintain a comprehensive compliance program that is tailored to promote an organizational culture of ethical behavior in order to prevent, detect, and correct conduct that does not comply with federal and state laws, contractual requirements, or sound ethical business practices. CHPW's Compliance Program is designed around the 7 Elements of an Effective Compliance Program:

- Written Policies and Procedures, Standards of Conduct
- Compliance Officer, Compliance Committee, High-Level Oversight
- Effective Training and Education
- Effective Lines of Communication
- Well Publicized Disciplinary Standards
- Effective System for Routine Monitoring and Identification of Compliance Risks
- Procedures and System for Prompt Response to Compliance Issues.

Written Policies and Procedures, Standards of Conduct

The Compliance Program policies, procedures (P&Ps), and Standards of Conduct provide guidance on how to identify and report compliance violations, how to handle compliance questions and concerns, and articulate and demonstrate CHPW's commitment to legal and ethical conduct.

Compliance Today

The Standards of Conduct are an extension of CHPW's Mission and organizational values and reflect the expectations that CHPW's workforce members, 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.

Workforce members are required to understand and follow Compliance policies and procedures, as well as the policies and procedures related to their positions. In addition, workforce members are required to understand and follow the Standards of Conduct and attest to receiving, understanding, and following the Standards of Conduct within 90 days of hire, and annually thereafter.

Compliance Officer, Compliance Committee, High-Level Oversight

CHPW's designated Compliance Officer is Marie Zerda. Marie is responsible for the implementation of the Compliance Program and defines the Program's structure, educational requirements, reporting and complaint mechanisms, response and correction procedures, and compliance expectations.

Oversight of the Compliance Program is delegated by Community Health Network of Washington's (CHNW) Board of Directors (BOD) to the CHNW Ethics Committee, a sub-committee of the full board. The CHNW Ethics Committee exercises reasonable oversight with respect to the implementation and effectiveness of the Compliance Program. Additional oversight is provided by the Compliance Committee, which is chaired by Marie Zerda and comprised of senior management from across the organization. The Compliance Committee is tasked with reviewing and guiding Compliance Program activities and disseminating information to CHPW workforce members.

The Compliance department reports Compliance Program activities to both the CHPW Compliance Committee and the CHNW Ethics Committee, ensuring CHPW's senior management and board is knowledgeable about the content, operation, and results of the Compliance Program.

Effective Training and Education

The Compliance department maintains a Compliance Education Sub-Program in which all workforce members, Board members, and FDRs must participate as a condition of employment or contract with CHPW.

Compliance Program Training is comprehensive, covering each of the four sub-programs supporting the Compliance Program. Examples of topics covered include an overview of CHPW's Standards of Conduct; channels for reporting compliance, ethics, privacy, fraud, waste, or abuse concerns, and for asking questions; an overview of compliance policies and procedures; consequences of noncompliance; important related laws and requirements; and, CHPW's monitoring and auditing processes. Training must be completed within 90 days of employment or contacting and annually thereafter.

On a routine basis, the Compliance department communicates through intranet broadcasts educational bulletins on new Compliance Program topics or reminders about compliance topics to refresh staff knowledge. Additionally, on a monthly basis, the Compliance department reminds all staff through broadcast about its Compliance Hotline, a tool maintained for confidential anonymous reporting. The Hotline number and online report form URL is published on magnets, which have been disseminated to all staff, on CHPW's intranet, and displayed on posters in high traffic areas within CHPW's facilities.

Effective Lines of Communication

CHPW must establish and implement effective lines of communication, ensuring confidentiality between the Compliance Officer, members of the Compliance Committee, workforce members, managers, governing body (BOD), and its FDRs. Such lines of communication must be accessible to everyone and provide an avenue for compliance-related issues to be reported, including a method for anonymous and confidential good faith reporting of potential issues as they are identified. Additionally, CHPW must have an effective way to communicate information from the Compliance Officer to workforce members, such as laws, regulations, guidance, and changes to policies and procedures or Standards of Conduct.

Workforce members have a duty to report any potential violations of the Standards of Conduct or the Compliance Program, non-compliance for fraudulent behavior, or other identified or potential privacy or security risks. Workforce members can report potential violations or submit compliance-related questions or concerns to the compliance department through any of the following methods:

- Email at compliance.incident@chpw.org
- Completing the *Report Potential Fraud/ID Theft form* and sending to Compliance at the above email
- Completing the *Privacy/Security Incident Report* form and sending to Compliance at the above email
- Email the Compliance Officer at compliance.officer@chpw.org, or ext. 5091, or in person on the 9th Floor
- Your HR Business Partner, or anyone else in HR
- A member of the Executive Leadership Team (ELT)
- Any member of the Compliance department
- The Compliance Hotline at (800) 826-6762 or online at http://chpw.ethicspoint.com

CHPW prohibits retaliation for compliance-related questions or reports of potential non-compliance or potential fraud, waste, and abuse (FWA) made in good faith. Making deliberately false or malicious reports is prohibited. When you make a report, confidentiality will be maintained to the extent practical that a report can be addressed without disclosure. All reported incidents of non-compliance are taken seriously.

Well Publicized Disciplinary Standards

CHPW is required to have well-publicized disciplinary standards which encourage good faith participation in the Compliance Program by all workforce members. These standards must articulate expectations for reporting compliance issues and assist in their resolution, that workforce members participate in required training, identify non-compliance or unethical behavior, and provide for timely, consistent, and effective enforcement of the standards when non-compliance or unethical behavior is determined. In addition, the disciplinary action must be appropriate to the seriousness of the violation.

To encourage good faith participation, CHPW must publicize disciplinary standards for workforce members. The Compliance department utilizes the following methods to publicize disciplinary standards:

- Annual Compliance Program training
- Compliance Today newsletter articles
- Ad-hoc communication broadcasts
- Making Connections Orientation (new employee orientation)

- Posters posted prominently throughout CHPW's facility
- Compliance Week activities

The Compliance department works in partnership with the HR department to ensure that disciplinary actions are appropriate for the seriousness of the violation, fairly and consistently administered, and imposed within a reasonable timeframe. The HR department is responsible for working with managers and workforce members to impose disciplinary actions as needed.

Effective System for Routine Monitoring and Identification of Compliance Risks

CHPW is required to have an effective system for routine monitoring and identification of compliance risks that includes internal monitoring and audits, as well as external audits to evaluate FDR compliance with regulatory and contractual requirements and the overall effectiveness of the Compliance Program.

CHPW must conduct monitoring and auditing activities to validate compliance with regulations, guidance, contractual obligations, state and federal laws, and internal P&Ps to protect against non-compliance and potential FWA.

The Internal Audit department conducts an annual risk assessment to assess CHPW's compliance and FWA risk areas. Based on the annual risk assessment, the Compliance department develops a Monitoring and Auditing Workplan.

The Compliance department utilizes dashboards, self-assessment tools, and business owner reports to document CHPW's monitoring and auditing efforts. In addition, CAPs are tracked and monitored for areas identified to be non-compliant in order to ensure non-compliant areas are corrected and the non-compliance is unlikely to reoccur. All monitoring, auditing, and corrective action activities are reported to both the Compliance and Ethics Committees.

Procedures and System for Prompt Response to Compliance Issues

CHPW is required to establish and implement procedures and systems for promptly responding to compliance issues, investigating potential compliance program issues as identified in the course of self-evaluations and audits, correcting such problems promptly and thoroughly to reduce the potential for recurrence, and ensuring ongoing compliance with regulatory and contractual requirements.

The Compliance department tracks and logs potential risks/concerns reported by workforce members, state and federal agencies, and FDRs, including risks identified through auditing and monitoring activities.

If CHPW discovers evidence of misconduct related to payment or delivery of items or services under its contracts, it must conduct a timely, well-documented, and reasonable inquiry into that conduct. CHPW must investigate any compliance incident or issues involving potential FWA.

CHPW must conduct appropriate corrective action in response to the potential violation, such as recovery of overpayments or disciplinary action against responsible individuals. Corrective action must be designed to correct the underlying problem that resulted in violations and to prevent future noncompliance. A root cause analysis determines what caused or allowed the FWA, problem, deficiency, or noncompliance to occur.

CHPW must have procedures to voluntarily self-report potential FWA, misconduct, or other compliance issues and concerns. Self-reporting is an important practice in maintaining an effective compliance program.

Cybersecurity: Ransomware Attack Threats

The Department of Health and Human Services (HHS) defines ransomware as, "a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so." It is important to note that paying the ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data.

Ransomware attack threats may incorporate tactics or techniques that are the same as or identical to other threats (e.g., successful phishing attacks may lead to the installation of ransomware).

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.

Most ransomware attacks are sent in phishing emails asking the recipient to either open an attachment or click on an embedded link. 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 for 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).

HIPAA: De-Identification of PHI

Any time CHPW receives a request for data that includes PHI, business owners must understand the purpose of the request and for what the information will be used. HIPAA requires that CHPW always provide the minimum necessary amount of information needed to fulfill the purpose of the request.

Whenever possible, aggregate, or de-identified information is preferred for disclosure. Even if disclosing to another covered entity, it is important only to disclose the minimum necessary needed to fulfill the intended purpose, as all electronic PHI (ePHI) is at risk. The more individuals or entities with access to health care data increase the risk of that data being impermissibly accessed or disclosed.

Once PHI has been de-identified, it is no longer PHI. There are two methods of de-identification: 1) use of statistical methods proven to render information not individually identifiable, and 2) deletion of the 18 specified PHI identifiers.

Statistical Method

A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable may de-identify data by:

1. Applying such principles and methods and determining that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
2. Documenting the methods and results of the analysis that justify such determination.

Deletion of 18 PHI Identifiers

To de-identify PHI using this method, the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
    - Currently, 036, 059, 063, 102, 203, 556, 592, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893 are all recorded as "000."
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail (email) addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Device identifiers and serial numbers;
13. Vehicle identifiers and serial numbers, including license plate numbers;
14. Web universal resource locators (URLs, website addresses);
15. Internet protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

For more information:

- *Member Privacy* policy (CO298).
- *Member Privacy: PHI and Member Rights* procedure (CO315).
- *Member Privacy: PHI Use and Disclosure* procedure (CO316).
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317).

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 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 now 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 department page on InsideCHPW.

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 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 and Updates

Recently Updated Compliance P&Ps

- *Advanced Directives* procedure (CO292)
- *CHPW Policy and Procedure Approval Process* procedure (CO305)
- *Responding to Threats of Physical Violence* procedure (CO336)
- *Exclusion Screening* procedure (CO337)
- *Fraud and Provider Payment Suspension* procedure (CO339)
- *Compliance Audit* policy (CO363)
- *Compliance Audit* procedure (CO364)