Compliance Today

HIPAA: Minimum Necessary Requirement

Under the Health Information Portability and Accountabiliyty Act (HIPAA), protected health information (PHI) should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a specific function. The minimum necessary standard requires Community Health Plan of Washington (CHPW) to evaluate practices and implement safeguards to limit unnecessary or inappropriate access to and disclosure of PHI. In addition, the minimum necessary standard requires that access to PHI be limited to only those employees who have a need to know that specific information to do their job. Access to PHI and the amount of PHI accessed must be limited to only that which is absolutely necessary to accomplish the given purpose.

Specific exceptions to the minimum necessary standard may be needed to facilitate care or to cooperate with an investigation by the Department of Health and Human Services (HHS). The minimum necessary standard does not apply to:

- Disclosures to or requests by a health care provider for treatment purposes;
- Uses or disclosures to the member who is the subject of the information (or to their authorized representative);
- Use or disclosures made pursuant to a member's authorization;
- Use or disclosures required for compliance with the HIPAA Administrative Simplification Rules;
- Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes; or
- Use or disclosures that are required by other laws or regulations.

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. Employees and contract employees 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.

For more information:

- *Member Privacy: PHI Use and Disclosure* procedure (CO316).
- *Employee Network and Facility Access Authorization* procedure (CO335).
- *Facility Badge Access* procedure (FA303)
- *HIPAA and Privacy Security Safeguards Violations* policy (CO325).
- *HIPAA Security* policy (CO330).
- *Privacy Incidents and Breach Notifications* policy (CO311).
- *Privacy Incidents and Breach Notifications* procedure (CO312).

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 abailable 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 releatives, employers, or household members of the individual are removed:

1. Names;
2. All geographic subdividsions 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 he 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 peole 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 universial 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).
- *Member Privacy: Workforce Member Responsibilties* procedure (CO317).

Protecting PHI

To ensure workforce members follow CHPW's privacy and security requirements, the Compliance department conducts quarterly privacy and security audits. As a reminder, all workforce members, contractors, and agents are required to adhere to the following:

- Encrypt ePHI stored on all portable devices, such as 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
    - Work with IS&T for keys or locks as needed.
- When leaving work, secure thumb drives, external hard drives, and any other portable device containing PHI in a drawer or cabinet.

Extra precautions must be taken to protect confidential and proprietary information stored on portable electronic media. Portable electronic media include CDs/DVDs, thumb drives (USB flash drives), PDAs, mobile phones, and tablets.

- **All** portable electronic media must be **secured** when not in use; either in a drawer, cabinet, secure room, or with a laptop cable lock.
    - Work with Facilities or IS&T for keys or locks as needed.
- When working on your laptop in a public space, ensure others cannot see your screen.
- Never leave your laptop, printed PHI, or company confidential or proprietary information unattended while in public spaces.
- Never connect CHPW devices to free, public, or unsecured wireless networks.
- Never store PHI or company confidential or

proprietary information on your computer's hard drive (C:\); and
- Only use CHPW's secured network folders/drives.

Note: 'Unsecured Laptops' continue to be the most common CHPW workforce member violation.

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 the CHPW VP of Talent and Business Process Management 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 (even if reported confidentially; you will receive a tracking number).

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, notify the HR department or the Compliance Officer.

Reminders/Updates

Compliance P&Ps Recently Updated:

- *Fraud, Waste, and Abuse* policy (CO289).
- *Advance Directives* policy (CO291).
- *Advance Directives* procedure (CO292).
- *Compliance Program* policy (CO300).
- *CHPW Policy & Procedure Approval Process* procedure (CO305).
- *False Claims and Whistleblower Protections* policy (CO310).
- *Compliance Hotline* policy (CO319).
- *Compliance Hotline* procedure (CO320).
- *Delegated Vendor Oversight* policy (CO321).
- *HIPAA & Privacy/Security Safeguards Violations* policy (CO325).
- *Cooperation with Auditors & Investigators* policy (CO327).

Compliance Today

- *HIPAA Security* policy (CO330).
- *Responding to Threats of Physical Violence* procedure (CO336).
- *Exclusion Screening* procedure (CO337).
- *Fraud and Provider Payment Suspension* procedure (CO339).
- *Verificaion of Services (VOS)* policy and procedure (CO356).
- *Compliance Audit* policy (CO363).
- *Compliance Audit* procedure (CO364).
- *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367).