Compliance Today

Requests for Member Records

Under the Health Insurance Portability and Accountability Act (HIPAA), members have the right to access (obtain a copy of) their protected health information (PHI).

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has launched an initiative to "vigorously enforce the rights of members to gain access" to their PHI.

A recent enforcement action involving Korunda Medical, LLC highlights the importance of properly processing member access requests. The enforcement action resulted in civil monetary penalties of $85,000 for Korunda's failure to timely provide records to a third-party, as well as charging more than the reasonably cost-based fees allowed under HIPAA.

It is critical that **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.

For more information:

- *Member Privacy: PHI and Member Rights* procedure (CO315)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)

Information Privacy & Security

Community Health Plan of Washington (CHPW) workforce members must adhere to the following safeguards for PHI and sensitive, confidential, and proprietary business information. All workforce members are required to demonstrate the same standards for protecting member and company information as they would their own.

Physical Safeguards for Workstations: Working with Printed PHI

- Keep documents containing PHI facedown when not in use;
- Store printed PHI in drawers or cabinets at the end of the day—all information must be secured;
- Lock office doors when leaving for the day;
- Dispose of printed PHI documents in a secure shred bin, never in the recycle bin;
- When sending printed PHI documents though interoffice mail, ensure the PHI is enclosed in an interoffice envelope;
- When leaving printed PHI documents on someone's desk, ensure the PHI is enclosed in an interoffice envelope or manila folder; and
- Promptly remove printed PHI from printers.

Protections of Sensitive, Confidential, and Proprietary Business Information

- Keep documents containing sensitive, confidential, or proprietary business information facedown when not in use;
- Store printed sensitive, confidential, or proprietary information in drawers or cabinets at the end of the day—all information must be secured;
- Dispose of printed sensitive, confidential, or proprietary business documents in a secure shredding bin, never in the recycle bin;
- When sending sensitive, confidential, or proprietary business information through interoffice mail, ensure the information is enclosed in an interoffice envelope;
- When leaving sensitive, confidential, or proprietary business information on someone's

desk, ensure the information is enclosed in an interoffice envelop or manila folder; and
- Promptly remove printed sensitive, confidential, or proprietary business information from printers.

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

- Encrypt ePHI stored on all portable eMedia, 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 the workstation (Ctrl-Alt-Delete + "Lock Computer," or 'Windows Button' + L);
- Always Keep laptops locked to the workstation with a cable lock when not in use; and
- When leaving work, secure thumb drives, external hard drives, and any other portable eMedia containing PHI in a drawer or cabinet.

Safeguards for Remote Workers

The workforce member and supervisor are jointly accountable for ensuring the following work environment standards are established and observed as a required element of working outside a CHPW office location or other CHPW-sponsored conference or meeting site:

- The remote worker's workspace must be private and should be dedicated to CHPW work activities. The workspace must permit effective separation of CHPW and personal business information. Remote workers must be able to protect personal and confidential information from inappropriate disclosure through audible or visible dissemination.
- Adherence to all standard information technology equipment security standards is required; specifically, equipment/device password and lockout settings and standards.
- If you have received approval to use hardcopies or removable media, all information must be stored in a locked container. This may require the employee to buy locking filing cabinets or other equipment to ensure that PHI is secure.
- Laptop computers, CD's, USB drives and/or other storage equipment (portable eMedia), are to contain no saved PHI, and are to be password protected at all times. If the employee is carrying a laptop computer from one location to another, the computer is to remain with that person at all times.
- All work documents will be stored on CHPW network drives. At no time can work documents be stored or kept on the computer hard drive.

A remote worker is required to maintain the confidentiality and security of all confidential, proprietary, medical, and sensitive information, just as if they were working from a CHPW location. Remote workers may not discuss or divulge confidential or proprietary information to any person, except as allowed or authorized by CHPW.

Quarterly Privacy/Security Walk Around Audits

The Compliance department conducts Quarterly Privacy/Security Walk Around Audits to evaluate CHPW's workforce on its understanding and compliance with general HIPAA requirements and CHPW's information and PHI privacy and security policies and procedures. The Compliance department will begin including results of the quarterly audits in each *Compliance Today* newsletter.

During the first quarter audit of 2020, the Compliance department identified the following violations:

- 1 computer screen not locked when the workforce member was not at their workstation.

For more information:

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

Cybersecurity: Portable eMedia Security

While portable eMedia allows on-the-go access to data easier, it also exposes CHPW to risk. Workforce members must take extra precautions when working with ePHI or portable eMedia to ensure the security of our members' information, as well as proprietary and confidential business information.

Securing ePHI and portable eMedia is critically important in protecting our members' information. The OCR recently announced an enforcement action against The University of Rochester Medical Center (URMC) resulting in a civil monetary penalty of $3 Million. URMC failed to employ mechanisms to encrypt ePHI or implement security measures sufficient to reduce risks and vulnerabilities; among other failures. URMC experienced the loss of an unencrypted flash drive and a laptop which resulted in impermissible disclosures of PHI.

Portable eMedia includes, but is not limited to:

- Laptops;
- Flash drives (thumb drives, memory sticks, USB storage devices, etc.);
- CDs;
- DVDs/Blu-Rays; and
- Smartphones and tablets.

CHPW utilizes a technology control mechanism which disables read/write capabilities for removable eMedia devices, except in limited circumstances. Contact the Help Desk at x8989 if you have questions.

Workforce members with read/write access **must encrypt all portable eMedia** containing ePHI or proprietary and confidential business information using an approved method of encryption (note: CHPW laptops are automatically encrypted). Contact the Help Desk at x8989 if you need assistance encrypting portable eMedia.

ePHI and other sensitive information should **never** be stored on your laptop, but rather on CHPW's secured network. As with printed PHI and your laptop, workforce members **must secure all portable eMedia when away from your desk and at the end of each workday.**

Disposing of Portable eMedia

Portable eMedia such as CDs or DVD/Blu-Rays must be placed in specific secure shredding bins for destruction, just as with printed PHI. Secure shredding bins for portable eMedia are found on the 10th floor. Workforce members must return portable eMedia (such as flash drives or mobile phones) to IS&T for cleaning and proper disposal when no longer in use.

Loss of Portable eMedia

If you lose a device, **immediately** report the loss to the VP, Compliance Officer, Marie Zerda, at compliance.officer@chpw.org, and the VP of IS&T, Steve Swanson, at steve.swanson@chpw.org. After you notify the VP, Compliance Officer and VP of IS&T,

complete a *Privacy/Security Incident Report* and send to the Compliance department at compliance.incident@chpw.org.

For more information:

- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Removable Media Device* policy (IT111)

Workplace Violence

According to the Occupational Safety and Health Administration (OSHA), approximately 75% of nearly 25,000 workplace assaults reported annually occurred in healthcare and social service settings. Workers in healthcare are four times more likely to be victimized than workers in private industry.

CHPW is responsible for providing a safe and secure environment and requires all workforce members and visitors to take reasonable measures to ensure their own personal safety and security, as well as the safety of all others while on CHPW premises.

For immediate and urgent threats of physical violence, call 9-1-1.

- Anyone on CHPW premises who receives a threat of physical violence from a workforce member, enrollee/member, or visitor **must immediately** report it to their supervisor. If a supervisor is not available, they may report it to any member of management who is available.
- Any supervisor or member of management receiving such a report **must immediately** communicate it to the VP, Compliance Officer and the Executive Leadership Team (ELT). If the situation warrants immediate action, contact the Receptionist.
    - If contacted, the receptionist will immediately engage the locking mechanism for the door to the main reception area and notify building security, Facilities, and HR, as well as (if warranted) call 9-1-1.
- The VP, Compliance Officer will decide the best course of action for addressing the threat in consultation with the ELT and the Facilities Manager. This may include locking down the affected floor(s), calling 9-1-1, contacting building security, law enforcement agencies, etc.
- If the VP, Compliance Officer is not available or is offsite, a member of management, or the ELT should be contacted immediately.

Important numbers:

- CHPW Compliance Officer: ext. 5091, or (206) 799-1406 (mobile)
- 1111 3rd Ave Building Security: (206) 515-2462
- Reception: ext. 0, or ext. 8833

For more information:

- *Responding to Threats of Physical Violence* procedure (CO336)
- *Workplace Violence Prevention and Employee Safety* policy (EE107)

Anonymous Compliance 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 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 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 and Updates

Alert: HHS OIG Telephone Numbers Used in Scam

The HHS Office of the Inspector General (OIG) issued an alert that official HHS OIG telephone numbers are being used as part of a spoofing scam. The OIG encourages the public to be vigilant and guard against providing personal information during calls that purport to be from the HHS OIG.

If you believe you may have been the victim of the telephone spoofing, report the information to the HHS OIG Hotline at 1-800-HHS-TIPS (1-800-447-8477) or online. Individuals may also file a complaint with the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357).

NAVEX Global Publishes Definitive Ethics and Compliance Program Benchmark Report

Leading ethics and compliance software and services company, NAVEX Global (the same company that manages CHPW's Anonymous Compliance Hotline), publishes its first consolidated *Definite Corporate Compliance Benchmark Report*. Disciplines covered in the report include policy and procedures management, employee training, third-party risk management, and hotline and incident management. Visit their site for more information and to obtain a copy of the report.

Recently Updated Compliance P&Ps

- *Fraud, Waste, and Abuse* policy (CO289)
- *Advanced Directives* policy (CO291)
- *Compliance Education Program* policy (CO293) and procedure (CO294)
- *Member Privacy* policy (CO298)
- *Compliance Program* policy (CO300)
- *Identity Theft Prevention* procedure (CO303)
- *False Claims and Whistleblower Protections* policy (CO310)
- *Privacy Incidents & Breach Notifications* policy (CO311)
- *Compliance Department and Legal Counsel* policy (CO313)
- *Member Privacy: PHI and Member Rights* procedure (CO315)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)

- *Exclusion Screening* policy (CO318) and procedure (CO337)
- *Compliance Hotline* policy (CO319)
- *Delegated Vendor Oversight* policy (CO321)
- *HIPAA and Privacy/Security Safeguards Violations* policy (CO325)
- *Cooperation with Auditors and Investigators* policy (CO327) and procedure (CO328)
- *HIPAA Security* policy (CO330)
- *Employee Network and Facility Access Authorization* procedure (CO335)
- *Verification of Services (VOS)* policy and procedure (CO356)
- *Security Incident Response* policy (CO370)
- *Compliance Program* description
- *Compliance Education Program* description
- *Fraud, Waste, and Abuse Program* description
- *Privacy and Security Program* description
- *Delegated Vendor Oversight Program* description