Compliance Today

Data Requests and PHI

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).

Recent incidents, such as the 2015 breach at Anthem, Inc., demonstrate the increased need to and challenges of protecting ePHI. In fact, according to the Health Care Compliance Association (HCCA), 89% of health care organizations and 60% of business associates suffered data breaches in the last two years. Furthermore, the Department for 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 PHI/ePHI. Unauthorized access or disclosure is when an individual obtains or receives PHI/ePHI that they are not allowed to view or access.

Any time Community Health Plan of Washington (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 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.

For more information:

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

Cybersecurity: Protecting Against Ransomware Attacks

Ransomware can infect computers in multiple ways and can have profound negative impacts on business operations by encrypting data files on a computer and demanding a ransom for their restoration. A recent example of a worldwide ransomware attack is *WannaCry*. Launched May 12, it is estimated to have impacted home and business computer users on an unprecedented scale; infecting more than 230,000 computers in over 150 countries.

The *WannaCry* ransomware attack is an ongoing worldwide cyberattack by the *WannaCry* ransomware cryptoworm, which targets computers running the Microsoft Windows operating system. CHPW is protected from *WannaCry* by our anti-malware/anti-virus technology tool, *Kaspersky*. This tool, in addition to ensuring we have up-to-date Microsoft security patches implemented, makes for a best-case protection scenario from *WannaCry* (and other yet-to-be-known ransomware attacks).

Compliance Today

In the spirit of strengthening and upholding the CHPW Cybersecurity Community, where every employee has a role, you can help us prevent email-based ransomware attacks. Ransomware can be delivered by email through attachments or links within an email (attachments in emails can include documents, zip files, executable applications, and malicious links) that link directly to a malicious website that the attacker uses to place malware on a system.

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

- 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-to-date - this adds another layer of defense that could stop the malware (this activity is done by the IS & T Department).

Delegated Vendor Oversight: Auditing, Monitoring, and Oversight of FDRs

CHPW maintains a Delegated Vendor Oversight (DVO) Program to ensure CHPW meets its contractual and regulatory obligations. First tier, downstream, and related entities (FDR) may provide administrative or health care services for members on behalf of CHPW.

> A **First Tier Entity** is any party that enters into a written arrangement with CHPW to provide administrative services or healthcare services to our members. The term "subcontractors" is the equivalent of a first tier entity. A **Downstream Entity** is any party that enters into a written arrangement, below the level of the arrangement between CHPW and a first tier entity. The term **Related Entity** means any entity that is related to CHPW by common ownership or control and performs some of CHPW's management functions under contract or delegation.

Delegation occurs when CHPW has a contract with a vendor to provide administrative or health care services for members on CHPW's behalf, thereby granting the delegated vendor the authority to make decisions or perform an administrative function that CHPW would otherwise perform. Regardless of whether CHPW enters into an agreement with an independent contractor to perform a function, CHPW itself is ultimately responsible for the contractor's work. If the independent contractor does not meet its obligations, its places CHPW's contracts with the Centers for Medicare and Medicaid Services (CMS), the Washington State Health Care Authority (HCA), and others—as well as CHPW's standing with the Washington State Office of the Insurance Commissioner (OIC)—at risk.

The business owner (the CHPW workforce member who would otherwise be responsible for the function had it not been delegated) is responsible for evaluating the delegated vendor and completing the pre-assessment, as well as ongoing monitoring and auditing of those activities delegated (if applicable).

CHPW business owners are responsible for conducting routine auditing and monitoring activities to ensure the delegated vendors are and remain compliant, as well as

ensuring they meet performance requirements and providing Compliance with monthly performance reports. 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. When a delegated vendor performs its own audit, it is a best practice for the CHPW business owner to obtain a summary of the audit workplan and audit results that relate to the services the delegated vendor performs.

Delegated vendors that do not meet their contractual obligations with CHPW must provide the business owner with a corrective action plan (CAP) detailing how and when they will be compliant. The business owner must forward a copy of the CAP to the Delegated Vendor Oversight Program Manager.

For more information:

- *Delegated Vendor Oversight* policy (CO321).
- *Delegated Vendor Oversight Program* description.
- DVO Toolkit for business owners, on Compliance SharePoint site.
- Josh Martin, Delegated Vendor Oversight Program Manager, ext. 8805, josh.martin@chpw.org.

Getting to Know the Compliance Department: Wensy Robles

Wensy is celebrating her 10th year at CHPW and serves as Compliance Specialist II. Wensy brings operational experience from Customer Service, Appeals and Grievances, and Provider Operations to the Compliance department.

Wensy is passionate about health care and CHPW because she gets such a great feeling knowing that someone is able to see a doctor, get their meds, or just get taken care of, and to know that she had something to do with it. She enjoys the opportunity to work for an organization that strives to deliver quality and accessible health care to the less fortunate community. Aside from what the mission stands far, the think Wensy loves best about CHPW are her co-workers. “I love coming to work knowing that the people I work with are amazing at what they do.”

Compliance Today

Outside of work, Wensy enjoys swimming, getting lost in a good book, traveling, and spending time with her family (her husband, 2 daughters (6 and 4) and son (2)). Another of Wensy's passions is ceramic painting, although she does not get to do it as often as she would like.

Wensy and the Compliance team are located on the 9th floor. Come by and say hi!

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

CMS 2017 Parts C & D Program Audit Protocols

CMS announced the release of the final 2017 Medicare Parts C and D Program Audit Protocols. CHPW highly recommends all business owners with the responsibility of Medicare Advantage review these protocols, including the data and documentation requests, in preparation for future audits. As you are aware, CHPW will be expected to fully comply with the audit protocols and the associated data collection efforts during a CMS Program Audit.

To view the protocols, please use the following link:

Compliance Today

https://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/ProgramAudits.html.

CMS 2017 Medicare Advantage & Prescription Drug Plan Spring Conference

The 2017 MA & PDP Spring Conference occurred on May 10 and 11. Materials can be found at the following link: T:\Public\Medicare\2018 MA Renewal\Guidance and Resources\2017 Spring Conference\2017 Spring Conference Final Presentations

Compliance P&Ps Recently Updated:

- *Fraud, Waste, and Abuse* procedure (CO290).
- *Advance Directives* procedure (CO292).
- *Compliance Education Program* policy (CO293).
- *Identity Theft Prevention* procedure (CO303).
- *Member Privacy: PHI & Member Rights* procedure (CO315).
- *Member Privacy: PHI Use & Disclosure* procedure (CO316).
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317).
- *Delegated Vendor Oversight* policy (CO321).
- *HIPAA & Privacy/Security Safeguards Violations* policy (CO325).
- *Cooperation with Auditors & Investigators* policy (CO327).
- *Employee Network and Facility Acess Authorization MAC Form* procedure (CO335).
- *Responding to Threats of Physical Violence* procedure (CO336).
- *Exclusion Screening* procedure (CO337).
- *Compliance Audit* policy (CO363).
- *Substance Use Disorder Records Use & Disclosure* policy and procedure (CO367).
- *Compliance Program* description.
- *Privacy and Security Program* description.