Compliance Today

Protecting PHI in Electronic Communications

While email is an effective communication tool, it also exposes Community Health Plan of Washington (CHPW) to increased risk of data breach. Extra diligence is required when communicating protected health information (PHI) or personally identifiable information (PII) electronically. Contractual and regulatory requirements mandate CHPW to protect private data, like PHI/PII, through technologies such as encryption.

Common examples of PHI/PII, include (but are not limited to):

- Name
- Social Security Number
- Telephone/Fax Number(s)
- Health Insurance Claim Number
- Date of Birth
- Email address
- National Provider Identification Number
- Driver's License
- Passport Number
- Biometric Information
- Medical Record Number
- Medical ID Number
- Certificate/License Numbers
- Account Numbers

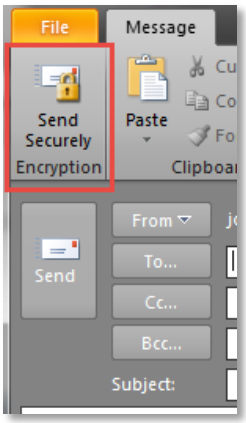
Any time you email PHI/PII to someone outside CHPW, you must either encrypt the attachment (sending the password in a separate email), or encrypt the email. If you are encrypting the email itself, CHPW uses **Proofpoint Encryption** to protect and distribute sensitive and confidential information.

Sending PHI/PII electronically without either securing the email or attachment violates CHPW's Security policies and procedures (P&Ps). Continued failure to comply with Security P&Ps will result in disciplinary action.

Encrypting with Proofpoint

Email is automatically encrypted and protected within CHPW; however, when emailing externally (outside CHPW) you must follow these simple steps to encrypt the information:

1. Write your email message and include relevant attachments (if any).
2. Click the "Send Securely" button.



   a. Alternatively, you can type "[encrypt]" (including the brackets, not quotes) anywhere in the subject line of your email message.

- To retrieve encrypted messages, the receiver must create or have an existing account through Proofpoint.

There are filters in Proofpoint to scan outbound messages for PHI/PII. If you forget to "Send Securely," Proofpoint should stop the email message and send you a notice that the email was not released from CHPW's network. Retrieve your message from "Sent Items" and resend using the "Send Securely" button.

Compliance Today

If you need to email a large file containing PHI/PII outside of CHPW, submit a ticket to the IS&T Help Desk for assistance in using secure FTP transfer or another secure option.

For more information:

- *HIPAA Security* policy (CO330)
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- Compliance Encryption Tips

Cybersecurity: Protecting CHPW Data with Vendor Partners

As you are aware, CHPW recently disclosed two data security incidents, which occurred in our vendors' computing environment (read more here). These incidents highlight the importance of protecting PHI and PII, especially when accessed or stored by a third party.

Although specific terms in our contracts outline requirements to safeguard CHPW's PHI and PII while in our vendors' possession, contractual language alone is not enough protection in the increasingly complex world of cyber-crime. It is one thing to ensure that data is transported and delivered safely from CHPW to vendors by utilizing a number of safety protocols (e.g. Proofpoint, secured FTP, encrypted data transport, dedicated private telecommunications connectivity), but once the data is safely delivered, CHPW must take additional actions to ensure the vendor is protecting CHPW's data properly.

While part of the CHPW Cybersecurity Task Force strategy has been to recognize and defend against security risks, CHPW has and will continue to proactively strengthen these disciplines by engaging an outside industry expert, Anitian Intelligent Information Security. Part of the engagement with Anitian is to assist CHPW in developing a Vendor Security Assessment Program. Once implemented, CHPW will use the Program to ensure that CHPW data in the hands of our vendors is better protected from cyber-attacks.

Things to remember in order to protect CHPW data include:

- Only use the minimum amount of PHI/PII absolutely necessary to accomplish the intended purpose of the use, disclosure, or request.
- Being aware of which vendors you work with that have access to, or store, PHI/PII in their computing environments.
    - Audit vendors that access or store PHI/PII to ensure data security protections.
- Utilize de-identified PHI/PII as much as possible; unless there is an absolute need for PHI/PII identifiers.

For more information:

- Contact the Compliance department.
- Contact the IS&T department (for assistance in securely communicating PHI/PII).
- Contact the Legal department (for assistance related to agreements or contract language).
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *HIPAA Security* policy (CO330)
- *Member Privacy* policy (CO298)

Compliance Today

Delegated Vendor Oversight: Engaging Vendors and Contract Requirements

CHPW maintains a Delegated Vendor Oversight (DVO) Program to ensure CHPW meets its contractual and regulatory obligations. The DVO Program has two parts: (1) ensure evaluation/pre-assessment of potential vendors is completed and (2) oversight/monitoring of business owners who have delegated relationships with vendors. By design, both parts of the DVO Program ensure CHPW meets contractual and regulatory requirements as though CHPW itself were performing the delegated function. CHPW remains ultimately responsible for any performance deficiencies of its First Tier, Downstream, and Related Entities (FDRs).

> 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 delegated vendor to provide administrative or health care services for members on CHPW's behalf, thereby granting the FDR the authority to make decisions or perform a core administrative function that CHPW would otherwise perform.

The CHPW business owner is responsible for the function if it were to be performed by CHPW (i.e., not be delegated), is responsible for fully understanding the delegated vendor relationship and be in a position to influence and enforce the delegated vendor's contractual obligations to CHPW.

The business owner remains responsible for evaluating the delegated vendor, including conducting the pre-assessment, reviewing and approving the delegated vendor contract language, ongoing monitoring and auditing activities, initiating and monitoring Corrective Action Plans (CAPs), and providing the Compliance department with monthly status reports of the delegated vendor.

Prior to contracting with any delegated vendor, business owners must conduct a pre-assessment to evaluate the FDR's ability to: (1) meet CHPW's obligations under its contracts with CMS, HCA, or other payors, and; (2) meet all regulatory obligations applicable to CHPW, as well as NCQA accreditation standards.

When considering a potential delegated vendor relationship, the business owner is responsible for engaging subject matter experts (SMEs), including (but not limited to) the Compliance Officer, DVO Program Manager, analysts, the Legal department, and other decision makers. More specifically, business owners are responsible for:

- Conducting a pre-assessment;
- Identifying reporting and monitoring activities to be conducted;
- Defining audit schedules;
- Obtaining necessary approval to enter into a delegated vendor relationship;
- Providing the delegated vendor with CHPW's Standards of Conduct and Compliance/FWA training materials, as well as CHPW P&Ps relevant to the delegated function.
    - Alternatively, obtaining, reviewing, editing, and approving the delegated

vendor's P&Ps relevant to the delegated function (these materials must meet CHPW's procedural, contractual, and regulatory requirements).

Each delegated vendor signs a Delegated Services Agreement (DSA), Service Level Agreement (SLA), or other contractual instrument ("Agreement"), and, as applicable, a BAA. The agreement(s) detail CHPW's performance standards for the activities or functions delegated and protections for PHI.

For more information:

- Contact Josh Martin, DVO Program Manager at ext. 8805, or at josh.martin@chpw.org.
- *Delegated Vendor Oversight* policy (CO321).
- *Delegated Vendor Oversight Program* description.
- DVO Toolkit:
    - *Delegated Vendor Criteria* (to assist in identifying whether a vendor is a delegate).
    - *Delegated Vendor Requirements* (outlines pre- and post-contracting requirements and detailed contract provisions).

Getting to Know the Compliance Department: Meg O'Connor

Meg is celebrating her 10th year at CHPW and serves as Compliance Specialist I. Meg brings with her many years of experience in health care; working in the Emergency Department of a hospital and at Blue Cross Blue Shield of Denver.

Meg is passionate about health care because she believes that every human has a basic right to health care. "When we help our community/tribe become as healthy as possible, we ALL benefit," she says. She feels that people should not have to choose between paying bills, eating, or getting the basic health care they need. The best part about her job at CHPW is that, "I get to help all departments be compliant, which means we have more room to grow and are successful as a plan of choice because we do it right."

Outside of work, Meg enjoys spending her time crafting, gaming, and with her two cats (Varric and Pumpkin). Those who know Meg, know that she is a huge trivia buff and finds the etymology of language

Compliance Today

fascinating. She is also very versed in French.

Meg 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**.**

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

2017 CMS Audit Protocols

CMS has released the 2017 Audit Protocols, which are located at: T:\Public\Medicare\CMS Audit Protocols\2017 CMS Audit Protocols. CHPW Medicare Advantage (MA) business owners must use these updated protocols to conduct MA audits of their operational areas to ensure compliance.

HPMS Memos

Did you know you can receive Health Plan Management System (HPMS) memos without gaining access to the HPMS system? If you need HPMS memo guidance, visit the CMS website and follow the instructions to join the "PLAN listserv." You must also include our Medicare Advantage contract number (H5826) in your request.

Compliance Today

Compliance P&Ps Recently Updated

- *Privacy Incidents & Breach Notifications* policy (CO311)
- *Privacy Incidents & Breach Notifications* procedure (CO312)
- *Cooperation with Auditors & Investigators* procedure (CO328)
- *Filing Forms B, C, and D with the OIC* policy (CO362)
- *Compliance Audit* procedure (CO364)
- ****New**** *Security Incident Response* policy (CO370)
- *Compliance Education Program* description
- *Delegated Vendor Oversight Program* description