Compliance Today

CHPW Delegated Vendor Oversight Program

The Compliance department is responsible for administering CHPW's corporate Delegated Vendor Oversight (DVO) Program, which is a sub-program supporting CHPW's Compliance Program. Josh Martin, Delegated Vendor Overisight Program Manager, is responsible for managing the Program.

The Delegated Vendor Oversight Program and its standards, requirements, and processes apply to *all* CHPW lines of business. The DVO Program has two parts: (1) ensure correct identification and evaluation/pre-assessment of potential vendors is completed by the CHPW Business Owner (BO) and (2) oversight/monitoring of the BOs that have entered into a delegated contractual relationship with a vendor.

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 an administrative function that CHPW would otherwise perform.

The CHPW BO that owns the function/activity is responsible for fully understanding the delegated vendor relationship and must be in a position to enforce the delegated vendor's contractual obligations to CHPW. The BO is responsible for evaluating the delegated vendor.

When considering a potential delegated vendor relationship, the BO must engage subject matter experts (SMEs), including (but not limited to) the Compliance Officer, DVO Program Manager, Business Analyst, the Legal team, and other decision makers. More specifically, BOs must:

- Conduct a Pre-Assessment;
- Identify reporting and monitoring activities to be performed;
- Define and Audit schedule;
- Obtain required approval to enter into a contractual relationship;
- Provide the delegate with CHPW's Standards of Conduct and General Compliance/Fraud, Waste, and Abuse (FWA) training materials, and applicable CHPW Policies and Procedures relevant to the function/activity.

Each delegate signs a Delegated Services Agreement (DSA), Service Level Agreement (SLA), and a Business Services Agreement (BAA), as applicable.

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).

HIPAA, Disclosure of PHI, and Care Coordination

The HIPAA Privacy Rule allows **covered entities** to share protected health information (PHI) **without a member's authorization for the purposes of treatment, payment, and health care operations (TPO)**.

Covered Entities

The Privacy Rule applys to health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of the Department of Health and Human Services (HHS) has adopted standards under HIPAA (referred to as covered entities).

Health Plans: individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare Advantage and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies).

Health Care Providers: every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.

Health Care Clearinghouses: health care clearinghouses are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa, such as: electronic claims transactions.

Treatment, Payment, and Operations (TPO)

Since CHPW is a covered entity it may use and disclose PHI for its own TPO activities. CHPW may disclose PHI for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

Treatment: the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

Payment: encompasses activities of a health plan(CHPW) to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.

Health care operations: any of the following activities: (a) quality assessment and improvement activities, **including case management and care coordination**; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of CHPWas the covered entity.

As a result, CHPW is not required to obtain an Authorization to Disclose PHI in order to disclose PHI to anyone who is part of the member's Individual Care Team (ICT) for case management and care coordination activities.

Minimum Necessary Standard

Although such disclosures are permitted, they are still subject to the minimum necessary standard. CHPW (a covered entity) must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

The minimum necessary requirement is not imposed in any of the following circumstances: (a) disclosure to or a request by a health care provider for treatment; (b) disclosure to an individual who is the subject of the information, or the individual's personal representative; (c) use or disclosure made pursuant to an authorization; (d) disclosure to HHS for complaint investigation, compliance review or enforcement; (e) use or disclosure that is required by law; or (f) use or disclosure required for compliance with the HIPAA Transactions Rule or other HIPAA Administrative Simplification Rules.

Substance Use Disorder (SUD) Records

It is important to note that SUD records do not have the same authorization exceptions for TPO as other PHI. SUD records use and disclosure **always** requires authorization by the member.

Authorization to Disclose PHI vs. Appointment of Representative (AOR)

When required, CHPW must obtain from the member an Authorization to Disclose PHI form in order to disclose any PHI to someone other than the member (outside of the exceptions noted above). The Authorization to Disclose PHI form **does not** grant any decision-making authority to anyone, nor does it allow for anyone to act on behalf of the member. The form simply allows CHPW to disclose PHI to someone other than the member. The Authorization to Disclose PHI form is located on all CHPW's external websites on the "Member Rights" pages.

The Appointment of Representative (AOR) form also has a very limited scope of use. The AOR form is **only** used when a Medicare Advantage member wishes to appoint a relative, friend, advocate, doctor, or another person whom the member authorizes to act on their behalf in obtaining a Medicare Advantage **grievance, coverage determination, or appeal**.

For more information:

- *Member Privacy: PHI Use and Disclosure Procedure* (CO316)
- *Substance Use Disorder Records Use and Disclosure Policy and Procedure* (CO367)
- *Information Privacy: Workforce Member Responsibilities Procedure* (CO317)

Printing of PHI/PII in Remote Environment

CHPW workforce members working remotely are required to maintain the confidentiality and security of all confidential, proprietary, medical, protected health information (PHI), personally identifiable information (PII), and other sensitive information, just as if they

were working from a CHPW location. Workforce members may not discuss or divulge confidential or proprietary information to any person, except as allowed or authorized by CHPW.

Workforce members may not at any time download ePHI to their computers. ePHI may be accessed and stored only on CHPW's network using its secure virtual private network (VPN). CHPW workforce members are prohibited from using personal email accounts to conduct CHPW business, including forwarding information from their CHPW account to their personal account. In addition, workforce members are prohibited from printing PHI or PII while working remote.

Other HIPAA standards for working remote include:

- Workspaces must be private and 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. Privacy screens and locking the screen when you walk away.
- 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 print or use hardcopies or removable media, all information must be stored in a locked container or file cabinet. This may require the workforce member to purchase a locking filing cabinet, shredder, or other equipment to ensure that PHI and PII is protected and secure.
- PHI or PII is not to be saved on laptop computers, CD's, USB drives, or other storage equipment unless there is a specific work requirement that has been approved by the IS&T Information Security team. All sensitive data must be protected according to CHPW's data classification and protection standards, including password protection and encryption.
- If the employee is transporting a laptop computer, or approved hardcopies and removable media from one location to another, the asset must remain with that person at all times unless it is stored in a locked and secure location (i.e. trunk of vehicle).
- 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, unless an explicit exception has been granted by Information Security.
- Never store PHI or confidential/proprietary information on personal computers or devices.
- Encrypt all PHI before it is transmitted in any form.

For more information:

- *HIPAA Security Policy* (CO330)
- *Information Privacy: Workforce Member Responsibilities Procedure* (CO317)

Anonymous Compliance Hotline

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

Compliance Today

Employee Quick Links on the InsideCHPW home page, and from a link on the Compliance Page on Inside CHPW.

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

Compliance Annual Training

Annual Compliance Training will be assigned to workforce members sometime in April, with completion due by November 2021. As with previous years, workforce members will have the ability to "test out" of the training with a passing score of 90% or greater on each module. In addition, the annual Standards of Conduct attestation will be assigned as part of the annual training package.

Recently Updated Compliance P&Ps

- *Fraud, Waste, and Abuse Procedure* (CO290)
- *Advance Directives Procedure* (CO292)
- *Compliance Education Program Procedure* (CO294)
- *Identity Theft Prevention Procedure* (CO303)
- *CHPW Policy and Procedure Process Procedure* (CO305)
- *Privacy Incidents & Breach Notification Procedure* (CO312)
- *Member Privacy: PHI & Member Rights Procedure* (CO315)
- *Member Privacy: PHI Use & Disclosure Procedure* (CO316)
- *Information Privacy: Workforce Member Responsibilities Procedure* (CO317)
- *Exclusion Screening Policy & Procedure* (CO318)
- *Compliance Hotline Procedure* (CO320)
- *Delegated Vendor Oversight Policy* (CO321)
- *HIPAA & Privacy/Security Safeguards Violations Policy* (CO325)
- *Cooperation with Auditors & Investigators Procedure* (CO328)
- *Employee Network and Facility Access Authorization (MAC Form) Procedure* (CO335)
- *Responding to Threats of Physical Violence Procedure* (CO336)
- *Compliance Audit Procedure* (CO364)
- *Compliance Program Description*
- *Compliance Education Program Description*
- *Fraud, Waste, and Abuse Program Description*
- *Delegated Vendor Oversight Program Description*