Compliance Today

Compliance Week

Corporate Compliance and Ethics week is an annual event sponsored by the Health Care Compliance Association (HCCA) and the Society of Corporate Compliance and Ethics (SCCE) to increase awareness of compliance and ethics issues. The first 'official' Corporate Compliance and Ethics Week was observed in 2005; however, its roots can be traced back as early as 2002, when two HCCA members, Gene DeLaddy and Cheryl Atkinson, wrote an article for *Compliance Today* telling others about an awareness program at their facility. Gene and Cheryl's event was called Compliance Awareness Week and was celebrated at the Carolinas HealthCare System in Charlotte, NC.

This year marks the 15th annual Corporate Compliance and Ethics Week celebration. Historically, Corporate Compliance and Ethics Week was observed the first week in May. In 2015, HCCA and SCCE moved the celebration to the first full week in November to better align with the implementation of the Federal Sentencing Guidelines; November 2004.

Community Health Plan of Washington (CHPW) has celebrated Corporate Compliance and Ethics Week since 2012. The Compliance department leads activities and educational opportunities throughout the week to interact, educate, and engage with workforce members.

The theme for 2019 is, "**Awareness, Recognition, Reinforcement.**"

Join the Compliance department in celebrating:

- Educational Games:
  - Photo Search
  - Golden Ticket
  - Crossword Puzzle
  - Recognizing Compliance
- Department Open House
  - **Tuesday, November 5, 10:00 a.m. to 11:30 a.m.**
  - Refreshments and treats
  - Trivia Wheel
  - Recognizing Compliance Ball Drop
  - Phishing Pond
- Daily quizzes through *InsideCHPW*.
- Win Prizes!
  - The more you play and interact, the more chances for you to win.

For more information, visit:

- Corporate Compliance and Ethics Week
- HCCA, SCCE
- Compliance Department on InsideCHPW

Cybersecurity: Identifying and Reporting Suspicious Emails

Not sure if an email is genuine or a phishing attempt? These steps may help you better identify suspicious solicitations for information before you submit a security incident.

If the email has not been identified by our secure mail gateway, ProofPoint, as having potentially malicious

content, you may discover emails that could either be from a trusted source asking for information beyond the normal scope of your business operations, or from a new contact requesting updated information. These scenarios happen for a variety of reasons, including but not limited to:

- Updates and changes to financial information from third party vendors.
- Initiating new lines of business.
- Inquiries involving sharing sensitive information.

If you suspect an email to be suspicious, follow these guidelines:

- Is the sender a new contact?
- Are they asking for sensitive information?
- Are they requesting information in a new format than previously agreed upon?
- Are there generic links with minimal explanation?
- Are there any spelling errors or word usage that seem awkward?
- Are there any attachments?
- Are there multiple recipients?

After reviewing this information, if you feel the message contains potentially malicious intent, please report the incident to the Help Desk so that we can update our security vendors and inform other potentially exposed users.

When reporting a potentially malicious email, do not download, forward, or respond to the message. Please collect the following information, email it to service.desk@chpw.org, and delete the email immediately to minimize accidental exposure:

- Sender's email address (username@domain.com);
- Recipient's email address (Individual, Shared, or Distribution list address);
- Time and date of the message, and;
- Subject.

No further action will be required unless otherwise requested. We will investigate the issue and notify appropriate parties as necessary. Your reports help keep others safe. Thank you for your assistance.

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)

Vendor Oversight & Delegated Vendor Oversight Programs

CHPW's Vendor Oversight Program

In 2015, CHPW developed and implemented a Vendor Oversight Program (VOP) to provide support to business owners with consistent end-to-end processes, tools, and resources to effectively procure and manage the life cycle of CHPW's vendors. The VOP outlines requirements for vendor procurement, oversight, and termination practices for vendors that classify, use, handle, transmit, store, retain, dispose, and manipulate CHPW electronic data.

All CHPW workforce members involved with the selection of new vendors and oversight of existing vendors, including full time employees, contractors, temporary employees, and project-based consultants/employees, must comply with the CHPW policies and requirements governing the CHPW VOP.

There are six (6) phases of the Program to help guide business owners through the procurement and management lifecycle of their vendors:

1. Identify Business Need for Vendor Selection
2. Vendor Identification and Selection
3. Vendor Contracting
4. Vendor Implementation
5. Vendor Sustainment Cycle
6. Terminate Vendor Contract

The VOP allows CHPW to proactively manage its vendor portfolio in the following ways:

- Monitoring business owner sustainment activities;
- Providing consultation/education;
- Maintaining procurement and management materials;
- Maintaining Vendor Management Resource site;
- Monitoring renewals and terminations;
- Identifying economies across portfolio;
- Overseeing vendor procurement activities;
- Providing status of portfolio performance;
- Providing tools to support Program activities, and;
- Providing continuous Program improvement.

For more information on the VOP:

- Contact Steve Cook, Director of Enterprise Services, at ext. 4725 or at steve.cook@chpw.org.
- *CHPW Vendor Oversight Program Data Security* policy (IT126)

While the programs may be separate, the VOP and CHPW's Delegated Vendor Oversight (DVO) Program support each other. During Phase II of the VOP, business owners are referred to the DVO Program to ensure proper identification and classification of delegates, and the ongoing oversight and monitoring provided by the DVO Program support VOP's goals of proactively managing the lifecycle of CHPW's vendors.

Delegated Vendor Oversight Program

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 the Centers for Medicare & Medicaid Services (CMS), the Washington State Health Care Authority (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 VP, 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/Fraud, Waste, and Abuse (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).

Workforce Badge Use and Access

Secured access and proper badge use are important parts of protecting our members' privacy and the security of CHPW's facility. **All individuals are always required visibly to display their ID badge while in the building**. It is your responsibility to always swipe your badge at every secured access door.

Compliance Today

CHPW issues the following types of badges:

- CHPW Employees (Regular or Temporary)
- Contingent Worker (Contractor)
- Board
- Vendor
- Visitor
- Loaner

Proper use of your ID badge is mandatory and ensures we maintain a secure facility. Some things to keep in mind are:

- Always make sure your badge is visible;
- Always keep your ID (image and name) visible on the badge;
- Never follow another employee through the door (tailgate), and;
- Never keep your badge in your pocket, bags, or wallet.

All visitors, including children, must be checked in with reception and receive a visitor badge before entering CHPW's facilities. Visitors **must be escorted at all times** while in CHPW's facilities.

If you observe someone attempting to tailgate, gently remind them to use their access badge.

If you forget your badge, you can check out a loaner badge from reception, for a period of up to three days. If reception is not open yet, **you must wait** until someone is able to issue you a loaner badge before you can enter CHPW's facilities. You can obtain a loaner badge up to two-times per month. More than two-times per month, your manager must obtain and return the loaner badge for you. Continued abuse of the loaner badge may result in corrective action.

For more information see:

- *Member Privacy: Workforce Member Responsibilities* policy (CO317).
- *Facility Badge Access* procedure (FA303).

Reminders and Updates

Annual Compliance/FWA Training

Reminder, on August 12, 2019, annual training was assigned in LearningConnect to workforce members employed in 2018.

All modules must be completed **no later than end of day, Friday, November 29, 2019.**

Recently Updated Compliance Policies and Procedures

- *Compliance Program* policy (CO300)
- *Compliance Department and Legal Counsel* policy (CO313)
- *Information Privacy: Workforce Member Responsibilities* procedure (CO317)