Compliance Today

Compiance 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) as a means to assist in educating workforce members on the importance of compliance and ethics. The first 'official' Corporate Compliance and Ethics Week was observed May 22-28, 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 13th annual Corporate Compliance and Ethics Week celebration. HCCA and SCCE have always co-sponsored the event, and early on took steps to sponsor a resolution in the U.S. Senate that would have allowed a National Corporate Compliance and Ethics Week to be officially recognized. Unfortunately, the senators who were shepherding the proposed resolution left office before it made its way through. By that time, Corporate Compliance and Ethics Week had taken hold among members of HCCA and SCCE, as well as compliance professionals across the country.

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 1, 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 2017 is, **"Make Good Choices."**

Join the Compliance department in celebrating.

- Educational games
  - Crossword Puzzle
  - Word Search
  - Photo Search
  - Golden Ticket Scavenger Hunt
- Department Open House

  - **Tuesday, November 7, 10:00 a.m. to 11:00 a.m.**
  - Refreshements and treats
  - Trivia Wheel
  - Test your password strength
  - Learn how to properly secure your laptop
- Daily email quizzes (based on content from this newsletter and other compliance-related information)
- Win prizes!
  - The more you play and interact, the more chances you have to win.

For more information, visit:

- Corporate Compliance and Ethics Week
- HCCA, SCCE

Cybersecurity: 5 Things Employees Should be Doing

In today's technology-driven world, everything relies on computers and the Internet to function; from communication (email, cellular phones), entertainment (streaming services such as movies, television, and music), transportation (auto engine systems), shopping (online stores, credit card processing), medicine (equipment, electronic medical records), and more. This reliance on technology and the Internet brings with it inherent risks, some more serious than others. Cybersecurity is the protection of data and systems in networks that connect to the Internet by preventing, detecting, and responding to attacks.

CHPW employs a variety of methods to respond to cybersecurity threats:

- Use of ProofPoint protection services
- Cybersecurity Taskforce
- Cybersecurity Community
- Strengthening contract language
- Auditing and Monitoring
- Ongoing education and training
- Strengthening data and systems access controls
- Solid policies and procedures
- Delegated Vendor Oversight

In addition to these corporate-level initiatives, workforce members play a critical role in CHPW's Cybersecurity Community and the protection of CHPW and members' information. Here are the five top things you, as workforce members, can do **today** to increase cybersecurity protections:

- Always report suspicious emails to the Service Desk
- Properly lock/secure your laptop computer
  - As well as any other portable eMedia
- Do not introduce unknown or unauthorized external eDevices into the CHPW computing environment, such as a flash drive
- Use secured email encryption with ProofPoint
- Use strong passwords and keep them in a secure, private location
  - Change your passwords regularly

For more information, visit:

- *HIPAA Security* policy (CO330)
- *Member Privacy: PHI Use and Disclosure* procedure (CO316)
- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Security Incident Response* policy (CO370)

Workforce Member 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 workforce members are required to wear an ID badge visibly at all times while in the building**. It is your responsibility always to swipe your badge at every secured access door; "One Swipe, One Entry." You should never tailgate another workforce member to enter a work area, for any reason. CHPW issues the following types of badges:

- Permanent (Regular Workforce Member)
- Contract (Temporary Workforce Member)
- 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 workforce member through the door (tailgate).
- Never keep your badge in your pocket or bags.
- If you lose your badge, notify the Facilities department immediately.

If you see someone without a badge, it is okay to ask them if they have one and to swipe it to gain entry. If they are a workforce member and have forgotten their badge, or if you forget your badge, check out a loaner from reception for use that day. You can check out a loaner badge up to three times per month. More than three times per month, your manager must check out and return the loaner badge for you. Continued abuse of the loaner badge may result in corrective action.

If you ever think a situation might be too confrontational, or if a workforce member is dismissive of their responsibilities, you can notify the Compliance department, or make a report through the Compliance Hotline at (800) 826-6762. **Retaliation is not tolerated** at CHPW and should be reported immediately through whichever channel you feel most comfortable with (Compliance Hotline, an Executive Leadership Team (ELT) member, Human Resources, the Compliance department, or the Compliance Officer directly).

For more information, visit:

- *Compliance department procedure CO317 Member Privacy: PHI & Workforce member Responsibilities* procedure (CO317).
- *Facility Badge Access* procedure (FA303).

Fraud, Waste, and Abuse

CHPW's Compliance department maintains a fraud, waste, and abuse (FWA) program to prevent, detect, and correct FWA. The Program ensures compliance with applicable laws, including but not limited to, 42 CFR 423.504, the Federal False Claims Act (31 USC §3729-3733), §6032 of the Federal Deficit Reduction Act of 2005 (42 USC §1396(a)(68)), and the Washington State Health Care False Claims Act (RCW 48.80).

This integrative program is designed to address issues across divisions and departments discovered through monitoring and auditing activities and reports from workforce members, CHPW members, first tier, downstream, and related entities (FDR), other health plans, and state or federal agencies. In the interest of ensuring quality, integrity, and sound business practices, the Compliance department investigates and seeks resolution of irregular billing practices, suspected cases of identity theft, and reports of suspected FWA. CHPW is committed to collaborating with the Washington State Healthcare Authority (HCA), the Centers for Medicare and Medicaid Services (CMS), other state and federal agencies, other health plans,

and providers to identify and correct FWA.

CHPW utilizes multiple avenues for the prevention, detection, and correction of FWA, including:

- Oversight;
- Standards, policies and procedures;
- Education and training;
- Systems and processes to detect and prevent FWA, and medical identity theft;
- Mechanisms for reporting suspected FWA;
- Processes for addressing and correcting at-risk business practices or noncompliant behaviors related to FWA, and;
- Processes for referring and reporting credible allegations of fraud to state and federal agencies.

The Compliance Officer, directly supported by the Fraud, Waste, and Abuse Program Manager and Compliance department staff, oversee the application of CHPW's FWA policies and procedures as well as auditing and monitoring activities, ensuring appropriate action is taken when processes, systems, and protections are violated or prove insufficient. The Compliance Officer reports FWA Program activities each quarter to the Compliance Committee and to CHPW's Board of Directors through the Ethics Committee. The Compliance Officer may, as appropriate, escalate risks of a serious nature directly to CHPW's ELT and the Board of Directors.

The Fraud, Waste, and Abuse Program Manager manages the day-to-day operations and administrative aspects of the FWA Program, supported by the Compliance Program Manager and the Compliance Specialist. Record review and investigation support are provided by the Fraud, Waste, and Abuse Program Manager, and the Claims Recovery team.

For more information, visit:

- *Fraud, Waste, and Abuse* policy (CO289).
- *Fraud, Waste, and Abuse* procedure (CO290).
- *False Claims Prevention and Whistleblower Protections* policy (CO310).
- *Fraud, Waste, and Abuse Program Description*.

Provider Billing Trends

Auditing and monitoring activities are one of the Seven Elements of an Effective Compliance Program and aid CHPW in detecting and preventing FWA. The Compliance and Claims Recovery department collaborate to initiate review of claims and CHPW member explanation of benefits (EOB) to ensure that diagnosis, evaluation, and management or procedure codes submitted for payment are supported by the medical record documentation for a member.

An investigation may be triggered as a result of the targeted review for any of the following:

- Post payment review of claims
- Medical claims review
- Pre-payment medical record review
- Claims trend reviews
- Ad hoc reviews requested by Medical Management or other workforce members
- Reports of suspected FWA
- Reports of suspected identity theft
- Up-coding
- Unbundling
- Services not rendered
- Kickback referrals
- Lack of medical necessity
- Phantom billing/ghost billing
- Falsifying diagnosis

In an effort to avoid inappropriate billing practices, the

following common billing issues were identified by CHPW and communicated to our provider network:

- Modifiers on Medicare Advantage (MA) claims(s): the Centers for Medicare and Medicaid Services (CMS) requires specific modifiers to be submitted on **all** claims for **all** MA plans. CHPW has a new claim edit in place, effective September 18, 2017) to deny claims that do not have the required modifiers.
- Inappropriate and overuse of modifier 59 and X modifiers: CHPW identified incidences of inappropriate use of modifier 59 instead of x modifiers.
- Upcoding and down coding: claims paid incorrectly for services billed due to either upcoding or down coding. The provider's medical record documentation must support and align with the procedure codes reported and billed for payment.
- Evaluation and Management (E&M) codes billed within 90 Day Global Surigical Period: providers incorrectly billed E&M services provided by a surgeon the day before, the day of, and up to 90 days after surgery.
- New vs. established patient E&M: new patient E&M codes were reported in members' claim history by a provider of the same specialty within the last three years of the current date of service. An established patient E&M code should have been used instead.
- Inpatient orders: valid inpatient admission orders must alwys be submitted and must include: date and time admitted; where admitted and why (medical necessity); signature by an admitting provider (orders entered by a resident must be cosigned by an attending provider); decision to admit; "Order entered by" and doctor's signature; order status must be completed.

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 FWA from workforce members, plan members, and FDRs. 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

Annual Compliance Training:

- Reminder: training must be completed no later than end of day on **Friday, November 17.**

Compliance P&Ps Recently Updated:

- *Compliance Education Program* procedure (CO294).
- *Compliance Program* policy (CO300).
- *Compliance Department and Legal Counsel* policy (CO313).
- *Exclusion Screening* policy (CO318).
- *Compliance Hotline* policy (CO319).
- *Verification of Services (VOS)* policy and procedure (CO356).