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 16th annual Corporate Compliance and Ethics Week celebration.

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 2020 is, "**Awareness, Recognition, Reinforcement.**"

Join the Compliance department in celebrating:

- Educational E-Games:
  - Crossword Puzzle
  - Recognizing Compliance
  - Word Search
  - Word Scramble
  - InsideCHPW Compliance Scavenger Hunt
- Daily quizzes through *insideCHPW*.
- Win Prizes!
  - The more you play and interact, the more chances for you to win.
  - This year's prizes will include e-gift cards from the following retailers:
    - Door Dash/Grub Hub/Uber Eats
    - Target
    - Walmart
    - Starbucks
    - Home Depot
    - Barnes & Noble
    - Amazon

For more information, visit:

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

Root Cause Analysis

An essential element of remediating non-compliance is effective root cause analysis. **Root cause analysis** is a systematic approach to get to the true root of a problem. It is an effective way to identify what happened, why it happened, and what changes need to be made.

Root cause is the fundamental breakdown or failure of a process which, when resolved, prevents a recurrence of the problem. Without an effective root cause analysis, an effective action plan cannot be developed, and the likelihood of the non-compliance is likely to reocurr.

An effective root cause analysis will include:

- How the issue of occurred.
    - Consider developing a timeline of events listing each step/action taken during the process that led to the failure.
- What factors contributed to the non-compliance, and at what level.
    - Review each step/action of the timeline and evaluate what factors occurred to increase the likelihood the failure would occur.
    - Were policies and procedures (P&Ps) in place or disregarded?
    - Were mitigating strategies or interventions identified prior to the issue occurring.
- Contributing factors are not root causes. Examine the contributing factors to identify the root cause(s).

Note: 'Human error' is not the conclusion of a root cause analysis, it is the beginning. A root cause is typically a finding related to a process or system that has potential for redesign to reduce risk.

Once the root cause has been identified, an improvement plan can be developed to remediate the root cause(s) of the failure(s) and ensures the failure is unlikely to reoccur.

Cybersecurity: Protecting Against Malicious Code

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. There are a variety of malicious code, such as viruses, worms, and Trojan horses.

Follow these cybersecurity practices to help reduce the risks associated with malicious code:

- Install and maintain antivirus software.
    - Be sure to download antivirus software directly from a reputable vendor's site rather than clicking a link in an advertisement or email.
    - At CHPW this is managed by IS&T and already done for you.
- Use caution with links and attachments in email. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to be from people you know.
- Block pop-up advertisements. Most browsers have a free feature that can be enabled to block pop-up advertisements that may contain malicious code.
- Disable external media AutoRun and AutoPlay features. This prevents external media infected with malicious code from automatically running on your computer.
    - In 2016, IS&T implemented a technology control mechanism which disabled read/write capabilities for removable eMedia devices, except in limited circumstances.
- Change your passwords often, using strong password passphrases, making them difficult for attackers to hack. If you believe your computer is infected, be sure to also change

any passwords for websites that may have been cached in your browser.
    - It is also recommended to use two-factor authentication (2FA/MFA) wherever possible to make it even harder for attackers to gain access to accounts and systems.
    - CHPW requires workforce members to change their passwords at set intervals and in 2019 began rolling out 2FA for access to its network and systems.
- Keep software up to date. Install software patches on your computer so attackers don't take advantage of known vulnerabilities. This is especially important for your operating system. Consider enabling automatic updates, when available.
    - At CHPW, this is managed by the IS&T department and already done for you.
- Back up data. Routinely back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your sensitive data will not be lost.
    - CHPW data, especially PHI, should never be kept on your CHPW computer's C:\ drive. Keeping data on CHPW's network ensures data is protected and backed up.
- Install or enable a firewall. Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer.
- Use anti-spyware tools. Most antivirus software includes an anti-spyware option; ensure you enable it.
- Monitor accounts. Look for any unauthorized use of, or unusual activity on, your accounts, especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.
- Avoid using public wifi. Unsecured public wifi may allow an attacker to intercept your device's network traffic and gain access to your personal information.

For more information:

- U.S. Cybersecurity & Infrastructure Security Agency (CISA)
- HIPAA Security Policy (CO330)
- Informatino Privacy: Workforce Member Responsibilities Procedure (CO317)
- Security Incident Response Policy (CO370)

Vendor Security Assessment Program

In 2017, CHPW's IS&T department implemented the Vendor Security Assessment Program (VSAP). The IS&T Technology Security Team manages the program and evaluates cybersecurity risk when CHPW shares sensitive electronic data (e.g., PHI) to a vendor or other business partners.

Any workforce member involved with sharing data to an outside entity is required to work with the VSAP team to help facilitate the evaluation of the outside entity's cybersecurity posture, disciplines, and practices such that the level of resultant risk is acceptable to CHPW. This evaluation **must** take place prior to contract execution (in the case of a new vendor) or prior to sharing any data (in the case of an established vendor that CHPW hasn't shared data with previously).

For more information, contact anyone on the VSAP team:

- Joe Saselli, Manager of Technology, Information Security at ext. 4751, or at joe.saselli@chpw.org.

Compliance Today

- Sara Crawford, Sr. Business Analyst Lead at ext. 8809, or at sara.crawford@chpw.org.
- Denise Wong, Technology Programs Coordinator at ext. 4718, or at denise.wong@chpw.org.
- Steve Swanson, VP Information Technology at ext. 4700, or at steve.swanson@chpw.org.

Compliance Anonymous Reporting

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 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

Annual Compliance Training

Reminder: annual Compliance Program and FWA training is **due by end of day, Friday, November 27, 2020**. As of October 22, 81% of workforce members have completed their training

If you have not completed training, log into *UltiPro Learning* to complete the modules. **Note:** complete training using **Chrome** not Internet Explorer or Edge.

If you have any questions related to the Compliance Program Training requirements or the modules, please contact the Compliance department at compliance.training@chpw.org.

Annual Standards of Conduct Attestation

Reminder: annual Standards of Conduct attestation is due **by end of day, Friday, November 27, 2020**. As of October 22, **only 59%** of workforce members have attested to receiving, understanding, and abiding by CHPW's Standards of Conduct.

Click here to complete your attestation.

Reporting Issues of Non-Compliance

Reminder: **Any issue of noncompliance (including not meeting a contractual obligation) must be reported to the Compliance Officer**.