Compliance Today

Getting to Know Alan Lederman

Alan is celebrating his 11th year at CHPW and current serves as the Chief Operations Officer (COO). During his tenure at CHPW, Alan has served as Chief Financial Officer (CFO) and Chief Administrative Officer (CAO). With the recent addition of the Compliance department to Alan's reporting tree, we took a moment to hear what compliance means to him.

Alan's belief is that, "Compliance isn't something separate or unique; it's something that must be woven into the fabric of an organization. It is how an organization operates with integrity and as a thoughtful steward of resources. Compliance is not only womething we *need* to do, but it is the *right* thing to do as an organization."

With a family history in health care, working as a health care provider seemed like a natural progression; however, he soon realized his passion lay more in finance. Never losing his familial interest in health care, and being drawn to the highly complex and variable nature of the industry, Alan has spent his entire career in the health care industry either working for insurance companies or integrated delivery insurance and delivery system companies. What drew Alan to CHPW its focus and dedication as a safety net, mission-driven plan and the knowledge that when CHPW does financially well, it can directly benefit the organizations it supports, as well as the community as a whole.

Outside of work, Alan and his family enjoy the outdoors and spent a lot of time working out, working in the garden or on projects around the house. He also enjoys traveling. He and his wife have two children, a son who recently graduated college and a daughter soon to graduate. One thing people may not know about Alan is that he enjoys home brewing beer.

Alan is located on the 6th floor and the Compliance department is located on the 9th floor. Come by and say hi!

Medical Identity Theft

The Office of the Inspector General (OIC) defines medical identity theft as, someone stealing personal information (name, Social Security number, or Medicare number) to obtain medical care, purchase drugs, or submit fraudulent claims in someone else's name. Medical identity theft has severe consequences wasting taxpayer dollars or having a detrimental effect on a member's credit rating.

Medical identity theft affects approximately 1.84 million people in the U.S. at a cost of approximately $12 billion dollars (McCann, 2013). The Department of Health and Human Services (HHS) estimates that more than half of the breaches are due to stolen portable eMedia; 20% of breaches are due to unauthorized access or impermissible disclosure, while 14% is due to hacking. In 2013, HHS and the Department of Justice recovered $4.3 billion from fraud, waste, abuse, and medical identity theft (HHS, 2014). The fact is that monies recovered are only a portion of what is being lost through fraud, waste, abuse, and medical identity theft. For instance, fraud accounts for approximately

Compliance Today

10% of Medicare's annual spending, equaling nearly $58 billion (Stewart, 2014); yet only $2.86 billion is actual recovered.

HIPAA and HITECH laws require CHPW to protect members' information. You can take action to help prevent exposure of members' information by doing the following:

- Verify all fax numbers before sending PHI.
- Complete proper caller verification procedures before releasing PHI.
- Encrypt (send securely) all PHI through email.
- Do not leave PHI on printers.
- Secure PHI at the end of each day.
- Work securely if you are in public or at home.
- When sending PHI or confidential/proprietary information by email, password protect the file and send the password in a separate email to the receiver.

How to Report

You can report suspected potential fraud, waste, abuse (FWA), or medical identity theft in the following ways:

- Complete the *Potential Fraud/ID Theft* form with as much information as possible and email it to compliance.incident@chpw.org.
- Contact the Compliance Officer, Marie Zerda at x5091 or by email at compliance.officer@chpw.org.
- Contact the Fraud, Waste, and Abuse Program Manager, Andrei Barlahan at x5054 or by email at Andrei.barlahan@chpw.org.
- Call the Compliance Hotline at (800) 826-6762.
- Report to the Office of the Inspector General (OIG) at (800) 447-8477, or at hhstips@oig.hhs.gov, or http://oig.hhs.gov/fraud/hotline/.

For more information, see:

- *Fraud, Waste, and Abuse* policy (CO289)
- *Fraud, Waste, and Abuse* procedure (CO290).

ePHI and Portable eMedia Security

CHPW workforce members understand the importance of securing desktop computers and printed protected health information (PHI). Just as important is securing ePHI and portable eMedia. While portable eMedia allows on-the-go access to data easier, it also exposes CHPW to risk. Workforce members must take extra precautions when working with ePHI or portable eMedia to ensure the security of our members' information, as well as proprietary and confidential business information.

Portable eMedia includes, but is not limited to:

- Laptops
- Flash drives (thumb drives, memory sticks, USB storage devices, etc.)
- CDs
- DVDs/Blu-Rays
- Smartphones and tablets

Note: beginning in September, 2016, CHPW implemented a technology control mechanism disabling read/write capabilities for removable eMedia devices, except in limited circumstances. Contact the Help Desk at x8989 if you have questions.

Workforce members with read/write access **must encrypt all portable eMedia** containing ePHI or proprietary and confidential business information using an approved method of encryption (note: CHPW laptops are automatically encrypted). Contact the Help Desk at x8989 if you need assistance encrypting portable eMedia. ePHI and other sensitive information

should never be stored on your laptop, but rather on CHPW's secured network. As with printed PHI and your laptop, workforce members **must secure all portable eMedia when away from your desk and at the end of each workday.**

Disposing of Portable eMedia

Portable eMedia such as CDs or DVD/Blu-Rays must be placed in specific secure shredding bins for destruction, just as with printed PHI. Secure shredding bins for portable eMedia are found on the 10th floor. Workforce members must return portable eMedia (such as flash drives or mobile phones) to IS&T when no longer in use, for cleaning and proper disposal.

Loss of Portable eMedia

If you lose a device, **immediately** report the loss to the Compliance Officer, Marie Zerda, at compliance.officer@chpw.org, and the VP of IS&T, Steve Swanson, at steve.swanson@chpw.org. After you notify the Compliance Officer and VP of IS&T, complete a *Privacy/Security Incident Report* and forward to the Compliance department at compliance.incident@chpw.org.

For more information, see:

- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Removale Media Device* policy (IT111)

Reporting Privacy/Security Incidents & Potential FWA

Any CHPW workforce member, contractor, or agent who knows of an impermissible disclosure or acquisition of PHI, or who suspects that one has occurred, or who suspects potential fraud, waste, and abuse or identity theft must **immediately** report that information to their supervisor and to the Compliance, Privacy and Security Officer (or to their designee). Failure to report privacy and security incidents or potential FWA may result in disciplinary action, up to and including termination.

Reporting Privacy/Security Incidents

- Complete a *Privacy/Security Incident Report* form with as much information as possible.
- Email the completed form to the Compliance department at compliance.incident@chpw.org.
- Contact the Compliance Officer, Marie Zerda at x5091 or by email at compliance.officer@chpw.org.
- Contact the Compliance Program Manager, Amie Schippa at x5092 or by email at amie.schippa@chpw.org.
- Call the Compliance Hotline at (800) 826-6762.

Reporting Potential FWA

- Complete the *Potential Fraud/ID Theft* form with as much information as possible and email it to compliance.incident@chpw.org.
- Contact the Compliance Officer, Marie Zerda at x5091 or by email at compliance.officer@chpw.org.
- Contact the Fraud, Waste, and Abuse Program Manager, Andrei Barlahan at x5054 or by email at Andrei.barlahan@chpw.org.
- Call the Compliance Hotline at (800) 826-6762.
- Report to the Office of the Inspector General (OIG) at (800) 447-8477, or at

hhstips@oig.hhs.gov, or
http://oig.hhs.gov/fraud/hotline/.

No retaliation of any kind is permitted against any workforce member who makes a report in good faith.

For more information, see:

- *Member Privacy: Workforce Member Responsibilities* procedure (CO317)
- *Fraud, Waste, and Abuse* policy (CO289)
- *Fraud, Waste, and Abuse* procedure (CO290).
- *Corrective Action and Discipline* policy (EE204)

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 required visibly to display their ID badge at all times while in the building**. It is your responsibility always to swipe your badge at every secured access door.

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).

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 (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 both the CHPW VP of Talent and Business Process Management, as well as the Compliance Officer 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 and using the unique identification number and PIN provided during the initial report.

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, you have multiple avenues to report such retaliation, for example: an ELT member, the Hotline, or the HR, Legal, or Compliance departments.

Recently Updated Compliance Policies & Procedures

- *Advance Directives* procedure (CO292)
- *Member Privacy: PHI Use & Disclosure* procedure (CO316)
- *Member Privacy: Employee PHI Responsibilities* procedure (CO317)
- *Responding to Threats of Physical Violence* procedure (CO336)
- *Exclusion Screening* procedure (CO337)