April 2017 Volume 4, Issue 2

COMPLIANCE NEWSLETTER

Heritage Provider Network

Compliance Officer Forum

Building a Culture of Compliance

by Kelly Karaniuk, AZPC Compliance Officer, and Carlos Schroeder, DOHC Compliance Officer

A culture of compliance requires everyone's participation to example ethical conduct and a commitment to comply with regulations and laws.

Employees work together to behave ethically and with integrity. One way of doing so is by following the policies and procedures, and by reporting to their supervisors any actions that are contrary to the Compliance Program.

One of the most critical elements of a Compliance Program is to build a culture of compliance.

Compliance Officers team up with leadership to establish or enhance a corporate culture that will support collaboration and consensus building.

Compliance should be viewed as a benefit versus a burden and can be simplified by creating a culture that starts with the Three C's of Compliance*:

Communication	Confirmation	Correction
• Education on our commitment to do the right thing.	• Monitoring and auditing processes; checks & balances.	• Identifying and resolving root causes to issues.

The Three C's are imperative in creating and maintaining compliant processes, policies and procedures throughout the organization.

What are some of the other tools that help assist with promoting a culture of compliance?

- **Transparency** – promoting accountability and providing information
- **Openness** – including others in the decision making process
- **Respect** – honoring someone by showing positive feelings
- **Honesty** – being fair and truthful
- **Reliability** – doing what is expected or promised
- **Flexibility** – being able to adapt to circumstances or challenges, and being able to consider multiple options
- **Resiliency** – recovering quickly from setbacks

Building a culture of compliance allows for employees to feel confident about their role, enhances stakeholder value, and maintains the integrity of our organization.

*Grand, C. (2005). Building a culture of compliance. *International Business Strategy*. Retrieved from www.qualitymag.com/ext/resources/qual/home/files/pdfs/building%20a%20culture%20of%20compliance.pdf

Standards/Code of Conduct

INTEGRITY · RESPECT · HONESTY · PRIVACY · ETHICS

- HPN's Standards/Code of Conduct state the company's overarching principles and values. They describe expectations of ethical behavior and how to report non-compliance and potential Fraud, Waste, and Abuse (FWA).
- Everyone who conducts business with or for HPN shares the responsibility of upholding and enforcing HPN's Standard/ Code of Conduct.

Compliance is everyone's responsibility!

The Standards/ Code of Conduct are distributed within 90 days of hire, upon updating, and annually.

The Compliance Program, including the Standards/Code of Conduct, Compliance Training, and Policies and Procedures, are located on your group's website or at www.heritageprovidernetwork.com/?p=compliance

Stay Tuned! Upcoming! 2017 Compliance Training

- Code of Conduct
- Cultural & Linguistics
- Fraud, Waste & Abuse
- Model of Care
- Harassment
- HIPAA/HITECH
- Injury & Illness

Keep a look out when to begin training! All training materials may be found on your group's website or at heritageprovidernetwork.com.

REPORT Compliance Concerns

- **Report to your Supervisor, HR, or Compliance Officer if you suspect any issues of non-compliance.**
- **You are protected from retaliation whenever you speak up in good faith; and always have the option of reporting anonymously.**

Corporate Hotline:
855-682-4127

Corporate Compliance
P.O. Box 7007, Lancaster, CA 93539

RANSOMWARE & HIPAA BREACHES

Ransomware is a type of malicious software created to restrict access to a computer system network and its informational contents until a sum of money is paid.

Although an organization may choose to pay the sum demanded, there are risks to consider:

- ! Those withholding information may have already shared or copied the information on a separate device;
- ! There is no guarantee that the information is secure.
- ! Additionally, the information is **NOT** guaranteed to be released after paying the ransom.

REMEMBER! Any compromised PHI is a HIPAA breach! Be aware of the consequences! !!!

- If you notice a rogue process/program running on your device, disconnect from the internet *immediately* and contact your IT department.

The best protection is Prevention! !!!

- Be mindful when opening emails with attachments. *These attachments may actually contain malicious software such as ransomware or even a Trojan virus!*
- If you receive a suspicious email and/or attachment, refer to your IT department to ensure your computer is safe from hackers and their tricks!

COMPLIANCE OFFICERS			
HPN	Sandy Finley sdfinley@hdmg.net Corporate Compliance Officer	**DOHC**	Carlos Schroeder cschroeder@mydohc.com
ADOC/GCMG/ LMG/RMG	Jeff Baron jbaron@regalmed.com	**HDMG**	Kathy Litel kslitel@hdmg.net
AZPC	Kelly Karaniuk kelly.karaniuk@azprioritycare.com	**HVVMG**	Denise Rock drock@hdmg.net
BFMC/CCPN	Debbie Zamora dzamora@bfmc.com	**SMG**	Sherry Connelly slconnelly@sierramedicalgroup.com