# COMPLIANCE NEWSLETTER

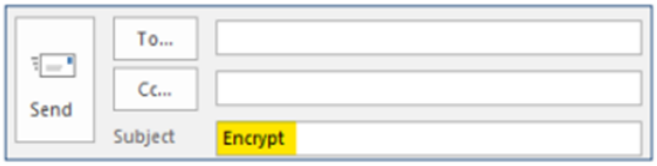
## Heritage Provider Network *Volume 10, Issue 1*

Take the Compliance Newsletter Survey for a Chance to WIN a $20 gift card!
Link Here!

## HIPAA and Email Encryption

HIPAA permits covered entities, such as HPN, to share PHI via email, but only if the email service is adequately protected. HPN uses encryption to protect PHI and requires that all emails containing PHI must be encrypted before transmission to any external sources.

When sending an email from HPN's or your Group's server (from your HPN/Group work email address), simply include the word "encrypt" anywhere in the subject line*




Before sending any emails containing PHI, double check that:

- The recipients selected are the appropriate individuals to receive the information
- The word "encrypt" is included in the subject line and is spelled correctly

*Note: The word "encrypt" works company-wide. Check with your IT department prior to using any additional terminology.

**CMP-PV-013 Confidentiality Related to PHI**
**CYB-GN-012 Protect—Protective Technology**

## HPN Compliance Training Website

To access Compliance & OSHA Training, Compliance Plan, Code of Conduct, Compliance Policies & Procedures, and archived Compliance Newsletters, please visit:
**https://www.hpnaco.com/Compliance**

### Heritage Provider Network's Group Compliance Officers

| | | |
|---|---|---|
| **ADOC/LMG/RMG** | Jeff Baron | jbaron@regalmed.com |
| **BFMC/CCPN** | Melissa Winters | mwinters@bfmc.com |
| **DOHC/HVVMG/AZPC** | Ryan Galli | ryan.galli@mydohc.com |
| **HDMG** | Thomas Viall | tviall@hdmg.net |
| **HSMG** | Sherry Connelly | slconnelly@sierramedicalgroup.com |

**Corporate Compliance Officer**: Margaret Ngo-Lee
mngo-lee@heritagemed.com
**April 2023**

## Privacy Physical Safeguards in the Office

To ensure that HPN and the Affiliated Groups are in compliance with HIPAA Privacy Safeguards, here are some physical safeguards everyone must follow within on-site facilities:

- Hard copies of Protected Health Information (PHI) are shredded and discarded in a secure manner.
- Computer Monitors are positioned away from public areas or are otherwise protected from observation by visitors.
- Supervisors regularly review facility policies that are applicable for their area work assignments with their staff to insure that current practices and procedures protect patient privacy.
- Confidential Conversations are not taking place where they can be overheard by others (Including telephone conversations, patient/provider conversation).
- Patient Information Screens are closed/locked when employees are away from their computer stations.
- Patient information (other than name) is not visible on sign-in sheets, boards, etc., and is not called out into the waiting room.

For more information, please contact your Compliance Officer and/or refer to **CMP-PV-002 Privacy Inspection Walk Through**

## REPORT FRAUD, WASTE, ABUSE & NON-COMPLIANCE

- Reports are kept confidential to the extent possible and may be made anonymously.
- Report without fear of reprisal or any other penalty, including retaliation or intimidation.
- Reports may be made 24/7, to your Compliance Officer through the Compliance Confidential Hotline, by email, or by mail.

**Refer to CMP-GN-006 Whistleblower Protection**