HAWAII HEALTH SYSTEMS
CORPORATION

"Quality Healthcare for All"

COMPLIANCE ALERT 13-24

*REMINDER: Use ZIX *Secure* when Emailing Protected Health Information (PHI)*

EXECUTIVE SUMMARY: HHSC employees and staff should ensure that all protected health information (PHI) is encrypted when it is sent via email outside of the HHSC email system. Encryption is done through utilization of the ZIX software that is under contract with HHSC.

SUMMARY: Sending email within HHSC (to "hhsc.org" addresses) does not require encryption because our system is secure. However, encryption IS required when sending PHI outside of HHSC (to a non-hhsc.org address).

Utilization of the ZIX system ensures that your email message is encrypted. However, it is important to remember that the "Subject" line of the email is NOT encrypted so no PHI should be included in the "Subject" line.

<u>Directions for utilizing ZIX:</u>

1. Include the word and asterisks: *Secure* in the "Subject" line. This tells our servers to encrypt the message.
2. Recipients will receive an email stating that they have a secure email and give them a link to go to for retrieval.
3. Remember: Even with the *Secure* in the subject line, the "Subject" line itself is NOT encrypted. The message in the body of the email is encrypted if the *Secure* is used.

ACTION NEEDED: HHSC facilities utilizing the OPPS should review rule to gain familiarity with this new rule. Other payers may follow CMS's lead but that is unknown at this time.

Source: Contact your Regional Compliance Officer and/or your IT department if you have further questions.