HAWAII HEALTH SYSTEMS
C O R P O R A T I O N

"Touching Lives Every Day"

COMPLIANCE ALERT 10-3

Implementation Recommendations for the HITECH Act of 2009

The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009 mandates new requirements for notification of all parties whose information has been compromised through unauthorized release. This information refers specifically to protected health information (PHI). HITECH also requires HHSC business associates notify us of any breaches involving HHSC PHI being handled by the business associate.

HITECH strongly advises but does not require encryption. However, notification is not required if technology (encryption) consistent with the National Institute of Standards and Technology (NIST) are used or if the data has been destroyed using techniques approved by NIST. Security of PHI should be a focus of all HHSC regions and includes data being stored and actively used, stored on paper or electronically. HITECH includes data accessed by appropriate users and by transmission to other entities.

This rule went into effect on September 23, 2009. Sanctions as a result of violation of the rule go into effect on February 22, 2010. Willful neglect carries the most severe penalties.

HHSC Hospitals and Regions should continue implementing necessary measures to comply with HITECH. Preparation should include:

1. Develop, implement, and enforce a Breach Notification Policy with resulting process in the event a breach does occur.
2. Review "Notices of Privacy Practices" and HIPAA policies to reflect new policy and security measures as implemented to comply with HITECH.
3. Train all staff on HIPAA and new data breach notification requirements under HITECH. Staff should also be trained on the Region's data breach notification process.

4. Notify all business associate agreements using the HHSC business associate addendum developed by HHSC legal office. Notify existing business associates of new requirements for data notification on their part since there is no "grandfathering" of the HITECH data breach notification requirements.
5. Special review and consideration of vendors outside the U.S. that might handle PHI to ensure compliance with HITECH and encryption standards of NIST.
6. Consider a review a risk analysis for data breach of all potential data storage and use sites at each facility. For instance, data generated from computers and stored on someone's desk, for instance, are covered under HITECH.
7. Work with the HHSC Corporate Information Security Officer to explore alternative architectures, devices, systems, etc. the Region may consider to comply with HITECH.

HITECH will require additional scrutiny, diligence, and cost. Remote support by business associates and others is now more complicated. However, the security and guarding of PHI is important to all of us. Data breach notification not only can be costly financially but also affects our reputation.

Sources: NIST "Guidelines for Media Sanitization"
"HITECH Risk for LTC Data Systems," December 1, 2009, D. M. Oatway.
American Recovery and Reinvestment Act of 2009