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

"Touching Lives Every Day"

COMPLIANCE ALERT 10-12

HIPAA Expansion under the American Recovery and Reinvestment Act of 2009

The American Recovery and Reinvestment Act of 2009 (ARRA)'s HITECH Act expanded the administrative portion of the Health Insurance and Portability Accountability Act (HIPAA) to ensure further compliance by Hospitals with the privacy and security safeguards underlying HIPAA when dealing with protected health information (PHI).

No Changes in Past HIPAA administrative Requirements: The basic tenets of the HIPAA privacy and security portions remain intact and include:

- Implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security tracking reports.
- Mandatory reporting of suspected or known security incidents.
- Institution of security measures needed to reduce risk of data breaches with PHI
- Application of appropriate sanctions against employees and vendors who fail to comply with PHI security and notification procedures and policies
- Implementation of a training program for all members of the Hospital's workforce.
- Development of appropriate policies and procedures to prevent, detect, contain, report, and correct data breaches and security violations.

NEW Key Changes in HIPAA include: The HITECH Act of the ARRA did expand and provide clarity to various portions that "apply to HIPPA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information."

- Clarifies the definition of "breach" and provides mandated notification processes depending on the type of breach and number of individuals involved.

- Applies rules, treatment, and penalties to all contracted business associates of the Hospital. Business Associates are those companies that handle or have access to PHI on behalf of a Hospital.
- Applies HIPAA compliance to vendors, contractors, trainees—not just employees.
- Provides clear date and timeline for Hospital response after a breach is discovered.
- Implements penalties for unintentional breaches. Penalties for willful neglect increased.
- Allows the State Attorney General to bring civil actions against a Hospital for data breaches.
- Requires Hospitals to provide an accounting of disclosures for the past three (3) years when requested.
- Mandates that Facilities provide Federal Government notification of all breaches each year.
- Provides patients new right to restrict disclosure of PHI in specific situations.

Definition of Breach. Breach is defined as the unauthorized access, use or disclosure that compromises the privacy and security of data in a manner not authorized under the Privacy Rule. Furthermore, the new changes say that the breach must cause significant risk of financial, reputational, or other harm to the individual whose data was involved.

The expansion of HIPAA includes three main statutory exceptions that *exclude* a disclosure from the definition of a breach:

1. Unintentional acquisition or use in good faith in the course and scope of a person's official job duties provided there is no further unauthorized use of the information.
2. Inadvertent disclosure by an authorized person to another authorized person within the same covered entity or business associate provided there is no further unauthorized use of the information.
3. If there is a good faith belief that the disclosure was to an unauthorized person who would not be able to retain the PHI.

Most importantly, the new rules stipulate that if data is encrypted (secured) or appropriately destroyed using specified methods by HHS then PHI is classified as protected from definitions of "breach."

Breach Notification. Breach notification rules only apply to "unsecured" PHI. Unsecured PHI is that which is not encrypted or "that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals though the use of a technology or methodology" specified by the government.

Other factors will mitigate whether an actual breach has occurred. These include who had access to and received the unauthorized PHI, whether the Hospital has taken immediate action to minimize the risk of harm, and if the unauthorized PHI was returned to the Hospital prior to it being accessed or used by unauthorized persons. The burden of proof that a breach has or has not occurred is on the covered entity. The process for risk determination and discovery must be documented.

Once a breach has been identified, Hospitals and other covered entities must notify individuals of a data breach without unreasonable delay and no later than 60 days after the breach was discovered or would have been discovered with due diligence. Notifications must be sent out by first class mail to the patient (or next of kin if applicable) at the last address of record. Email notification may only be used if the patient has previously given permission for email notices or if email is requested.

<u>The notification must include:</u>

1) a brief description of what happened, including the date of the breach and the date of the discover of the breach, if known;
2) a description of the types of unsecured protected health information that were involved in the breach;
3) any steps individuals should take to protect themselves from potential harm resulting from the beach;
4) a brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches, and;
5) contact procedures for individuals to ask questions or learn additional information which must include a toll-free telephone number, an email address, website or postal address.

Other notification requirements:

- Telephone or other means must be used if there is imminent danger to the patient. Written notice must still be provided.
- If more than 500 residents of a state or region are affected then appropriate media outlets must be utilized as well as written means for notification.
- If more than 500 patients are involved, the Secretary of Health and Human Services must be notified immediately in addition to other required notification procedures.
- An annual report to the Secretary of Health and Humans Services must be sent for breaches less than 500 patients. This report is submitted electronically and is due by March 1 following the end of the previous calendar year.
- If the Hospital does not have accurate contact information for some of the affected individuals or if the mail is returned, the covered entity must provide substitute notice for the unreachable individuals. Substitute notification may be a phone call (for less than 10 patients), email, or a web site with a toll-free number for at least 90 days (if more than 10 individuals).
- Hospitals' notifications must also comply with Title VI of the Civil Rights Act of 1964 that requires reasonable steps to ensure meaningful access for Limited English Proficient persons.

HIPAA Applicability, Enforcement, and Penalties. The new rules expand the applicability of HIPAA requirements. Business associates (those vendors and contractors that handle PHI on an entities' behalf) now must comply with many of the HIPAA privacy and security rules. Business associates are required to notify the Hospital if a data breach occurs. These new rules also expand to volunteers and trainees as well as business associates and employees.

The HIPAA criminal provisions now apply to individuals not just the covered entities. And there are changes that allow civil penalties to be levied against individuals and Hospitals by a state's attorney general.

Penalties for HIPAA violations are specified within four tiers: A) Inadvertent disclosure through lack of knowledge about violation; B) Unauthorized disclosure due to reasonable cause but not willful neglect; C) Corrected disclosures due to willful neglect; D) Uncorrected disclosures due to willful neglect. Fines range from $100 per violation due in Tier A up to $1.5 million per year maximum for Tier D violations.

Increased Patient Rights. Patients can restrict disclosure of PHI if: 1) the disclosure is to a health plan for purposes of carrying out payment or healthcare operations but is not treatment, AND; 2) the PHI pertains solely to a healthcare

service for which the patient has paid out of pocket in full to the provider. Patients may also request an accounting of disclosures for treatment, payment, and healthcare operations back for three years.

Sources: Federal Register, 74, 162, August 24, 2009, 42740-42770.
Federal Register, 74, 209, October 30, 2009, 56123-56131.