HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	*Quality Through Compliance*	Policy No.: **CMP 0014**
		Revision No.: N/A
Policies and Procedures	Issued by: Corporate Compliance Committee	Effective Date: February 12, 2010
Subject: ***Data Breach Response***	Approved by: Alice M. Hall Alice M. Hall Interim President & CEO	Supersedes Policy:
		Page: 1 of 2

I. **PURPOSE:** To satisfy applicable federal and state legal and regulatory requirements, including HIPAA, the HITECH Act, HRS Chapter 487N and associated regulations, regarding response to breaches of certain types of protected health and personal information. This policy is intended for system-wide implementation prior to the February 22, 2010 current enforcement date for the HITECH Act.

II. **DEFINITIONS:**

Breach – the unauthorized acquisition, access, use, or disclosure of Unsecured Protected Health Information ("UPHI") or Personal Information ("PI"), subject to certain exceptions. Breach of UPHI includes, for example, "snooping" into a patient's medical record without a "need to know."

Business Associate – "Business Associate" as defined in 45 CFR 160.103, including but not limited to vendors who perform claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, or repricing, or who provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to HHSC.

HIPAA – Health Insurance Portability and Accountability Act of 1996, as amended (45 CFR part 160).

HITECH – Health Information Technology for Economic and Clinical Health Act, enacted February 17, 2009 (Section 1176(b) of the Social Security Act, 42 U.S.C1320d-5(b)).

Personal Information ("PI") – An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account; as defined in HRS Section 487N-1.

Protected Health Information ("PHI") – Information created or received by HHSC which relates to an individual's health or condition; the provision of health care to an individual; or payment for the provision of health care to an individual, which identifies the individual or

with respect to which there is reasonable basis to believe the information can be used to identify the individual; as defined in 45 CFR[1] Section 160.103.

Unsecured PHI ("UPHI") – PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5 on the Department of Health & Human Services Web site.

Workforce – All HHSC employees, volunteers, trainees, healthcare providers, and any other persons under the direct control of HHSC.

III. POLICY:

Upon discovery or notification that a member of HHSC's workforce or a Business Associate of HHSC has actually or potentially committed a breach of Unsecured Protected Health Information ("UPHI") and/or a breach of Personal Information ("PI"), HHSC shall promptly review the matter and shall comply with all applicable federal and state laws and regulations, including but not limited to obligations for notification of affected individuals and/or reporting to appropriate authorities.

IV. PROCEDURE:

Any HHSC workforce member who discovers, is notified of, or otherwise becomes aware of an actual or potential breach of UPHI and/or PI committed by an HHSC workforce member or an HHSC Business Associate shall report it within one (1) business day to the appropriate Regional Compliance & Privacy Officer ("RCPO"). In the absence of the RCPO or for breaches involving the HHSC Corporate Office, such reports shall be made to the Chief Compliance & Privacy Officer ("CCPO"). Reports may be made through the Regional or Corporate Compliance Hotline if the reporter wishes to remain anonymous.

The RCPOs shall maintain a log of all such reports and shall be responsible for reviewing and analyzing all reported matters to determine what action, if any, is required. The RCPOs shall retain documentation of their investigation if any, analysis, and conclusion regarding whether further action is required. The CCPO shall do the same for reports to the extent they involve the corporate office.

Violations of this policy and other HIPAA/HITECH policies will be addressed in accordance with established HHSC disciplinary protocol (in accordance with the respective collective bargaining agreements and the HHSC Human Resources and Civil Service System Rules, as applicable) and reference to ITD 0016.

Each HHSC Region and the Corporate Office will establish further procedures for implementation of this policy as needed.

V. REFERENCES:

HRS Chapter 323F; HRS Chapter 487N; 45 CFR 160 and 164; H.R. 1, S.1, American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act (the HITECH Act), § 13001, et seq. (Feb. 17, 2009).

---

[1] Code of Federal Regulations.