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

"Touching Lives Every Day"

COMPLIANCE ALERT 11-24

HIPAA VIOLATION GUIDELINES

I. **PURPOSE:**

The purpose of this document is to comply with legal requirements relating to the imposition and notification of disciplinary actions for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA limits the access, use, or disclosure of protected health information (PHI) only to *authorized individuals who require access to such information*.

II. **DEFINITIONS**:

"PHI" refers to any individually identifiable health information, including demographic data, relating to: (1) an individual's past, present, or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual. PHI includes information in any form, whether electronic, paper, or oral.

III. **GENERAL PROVISIONS**:

A. Should an investigation confirm that an employee of HHSC has committed a violation of HIPAA, the following disciplinary guidelines shall be considered in the determination of appropriate disciplinary action for said violation.

B. Each violation will be considered on a case-by-case basis to determine the seriousness of the violation and appropriate sanction. These guidelines are not intended to replace or preclude the application of existing disciplinary standards and principles such as just cause or progressive discipline.

C. An employee who is found to have violated HIPAA may, in addition to any personnel action taken, be referred to an outside entity (e.g., US Attorney's Office, Prosecuting Attorney's Office) for possible prosecution or other sanction.

D. These guidelines are not intended to diminish an employee's right to challenge adverse personnel action pursuant to applicable collective bargaining agreements or other applicable laws or procedures.

IV. **DISCIPLINARY GUIDELINES**:

Violations of HIPAA that are substantiated through investigation shall be addressed in the same manner as violations of the HHSC Code of Conduct, with a range of possible sanctions up to and including termination of employment. Reference is made to the Code of Conduct, Section VI. The type of sanction imposed will depend to a large extent upon the intent of the employee when the HIPAA violation occurred, as well as the severity of the violation.

The following are categories of HIPAA violations, reflecting increasing severity. These categories, while not all-inclusive, shall serve as a guide in determining appropriate sanctions and/or other necessary corrective action to be taken in response to a confirmed violation.

Category 1 Violations: Inadvertent, improper access or disclosure of PHI. This occurs when an employee unintentionally or carelessly accesses or reveals PHI to himself/herself or to others without a legitimate need to know. Examples include leaving medical records unattended in an accessible area; discussing PHI in a public area where others may overhear the conversation; leaving a computer unattended when PHI is displayed; failing to properly dispose of PHI, or mistakenly mailing a patient billing statement to the wrong guarantor. Appropriate sanctions for category 1 violations may include required HIPAA refresher training; verbal reprimand; written reprimand; or, depending upon the circumstances, suspension.

Category 2 Violations: Deliberate, unauthorized access or disclosure of PHI, but without personal gain. This occurs when an employee intentionally accesses or discloses PHI without a legitimate business reason, but not for personal gain. Examples include looking up birth dates or addresses of friends/relatives; sharing computer access codes; or accessing PHI out of curiosity, such as reviewing a public personality's medical records. Appropriate sanctions for category 2 violations may include required HIPAA refresher training; verbal reprimand; written reprimand; suspension; or, depending upon the circumstances, termination.

Category 3 Violations: Willful, unauthorized access or disclosure of PHI. This occurs when an employee intentionally accesses, reviews, or discloses PHI for personal gain or with malicious intent. Examples include reviewing a patient's records in order to use the information in a personal relationship; using patient information to open credit card accounts; or gathering patient information to be

sold to tabloids. An appropriate sanction for category 3 violations would be termination, with reporting to other appropriate agencies.

V. **MITIGATING FACTORS**:

In determining sanctions for HIPAA violations, mitigating factors, if any, should be considered. Examples include:

- Victim(s) suffered no harm
- The breach occurred as a result of trying to help a patient
- The offender admitted the breach and was cooperative
- The offender was remorseful
- The action was taken because of pressure from an authority figure
- The offender was not adequately trained

VI. **EXACERBATING FACTORS**:

In determining sanctions for HIPAA violations, exacerbating factors, if any, should be considered. Examples include:

- The breach required notification to the Department of Health and Human Services as mandated by the HITECH Act
- Large number of people affected
- Breach of particularly sensitive or specially protected information, such as HIV-related, psychiatric, of substance abuse information
- Large organizational expense involved, such as for breach notifications
- Harm to the victim(s)
- The offender hampered the investigation
- The offender committed prior HIPAA violations

VII. **APPLICABILITY:**

These guidelines shall apply to all employees of the HHSC.

VIII. **REFERENCES:**

A. HRS Chapter 323F
B. HRS Chapter 487N
C. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, August 21, 1996.
D. Health Information Technology for Economic and Clinical Health Act (HITECH), American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Div. A, Title XIII, § 13001 *et seq.*, Div. B, Title IV, § 4001 *et seq.*, Feb. 17, 2009.