
 HAWAII HEALTH SYSTEMS CORPORATION <i>Quality Healthcare for All</i> PROCEDURE	Department: Compliance	Procedure No. CMP 0059B
		Supersedes Procedure No.
Subject: WORKFORCE SANCTIONS	Approved By:  By: Edward N. Chu Its: HHSC President & CEO	Approved Date: September 1, 2024 Last Reviewed: August 22, 2024

PURPOSE:

To ensure that appropriate sanctions are consistently applied against members of the Workforce who fail to comply with the HIPAA security policies and procedures of HHSC.

DEFINITIONS:

“Workforce” as used in this procedure means any employee, part-time or full time, temporary hire, volunteer, trainee, or any other persons whose conduct, in the performance of work for HHSC, is under direct control of HHSC, whether or not they are paid by HHSC. Workforce may include medical staff members and other credentialed practitioners, academic instructors, students, residents, and board members.

“HIPAA” means the broad set of federal laws contained in the Health Insurance Portability and Accountability Act of 1996, the HITECH Act of 2009, and the subsequent Privacy and Security Rules located in 45 CFR Parts 160, 162, and 164.

“Individual of Interest” means a family member or friend or associate of a Workforce member, a co-worker, or any other individual with a similar relationship to the Workforce Member whose care or PHI is not the subject of a Workforce member’s current work product.

“Minimum Necessary / Minimum Necessary Rule” means that the PHI used or disclosed will be limited to the minimum amount of information necessary to achieve the intended purpose.

“Protected Health Information (PHI)” means information collected from an individual that is created or received by HHSC and

- relates to the past, present, or future physical or mental health or condition of the patient; the provision of health care to the patient; or the past, present, or future payment for the provision of health care to a patient ; AND
- Identifies the individual; OR
- Creates a reasonable basis to believe the information can be used to identify the individual.

“Unauthorized Access” means access, use or disclosure of PHI outside the scope of the Workforce member’s duties or level of access and/or access to the Workforce member’s own PHI, or any other individual’s PHI, including Individuals of Interest, for a non-work related purpose, without the required authorizations.

PROCEDURE:

- I. **Investigation**- The Regional Compliance Officer or Corporate Privacy Officer, with the assistance of the Chief Information Officer, as needed, shall investigate every allegation of Unauthorized Access of PHI or violation of HHSC HIPAA or Security policies and procedures and determine, to the best of their ability, whether an Unauthorized Access or a violation has in fact occurred.
 - A. If the Regional Compliance Officer or Corporate Privacy Officer finds that Unauthorized Access or violation by a Workforce member has in fact occurred, the Regional Compliance Officer or Corporate Privacy Officer shall submit a summary of their investigation to the Regional/Human Resources Office or appropriate officer, as applicable, upon completion of their investigation.
 - B. The Summary of the investigation shall include a determination of the level of violation that has occurred.
 - C. The Regional Compliance Officer shall retain all investigatory materials for a minimum of six (6) years.
 - D. Any imposed sanction on a Workforce member shall be retained in their file for a minimum of six (6) years.

- II. **Discipline**- HHSC will appropriately and consistently discipline Workforce members, in accordance with this Procedure, for any violation of HIPAA related policies or procedures, to a degree that is correlated to the gravity of violation. The Violation Matrix, included in this procedure, is meant to provide guidance on how to assess violation levels, but facts and circumstances of each individual case should be examined to see if different Level classifications are warranted. Such facts and circumstances should be noted in the relevant investigation. Nothing in this Procedure shall be interpreted to limit any rights a Workforce member might have otherwise, including rights under relevant collective bargaining agreements.
 - A. **Corporate/ Regional Human Resources Office -** HHSC's Corporate and/or Regional Human Resources Office, or appropriate regional officer, as applicable, based on the investigation, recommendation of the Regional Compliance Officer, Corporate Privacy Officer and the guidance herein, shall determine the appropriate disciplinary action to be taken. Disciplinary action may include more than one of the suggested actions from the relevant Level.

 - B. **Reports to Law Enforcement**. A report to law enforcement may be warranted depending on the nature of the violation. Facility staff shall work with the Corporate Compliance Officer and General Counsel on how and when to report a violation to law enforcement.

VIOLATION MATRIX

LEVEL	DESCRIPTION OF VIOLATION	CAUSE/ MOTIVATION	Recommended List of Optional Sanctions
1	<p>-Accidental or unintentional violation- Mistakes or errors in handling PHI or in maintaining workstation or physical surroundings or failing to take appropriate measures to secure PHI:</p> <ul style="list-style-type: none"> • Mistakenly sending emails or faxes containing PHI to the wrong recipient • Discussing PHI in public areas where it can be overheard • Incorrectly identifying a patient record • Leaving an active computer screen with access to non-sensitive PHI unattended 	<ul style="list-style-type: none"> • Unintentional AND • Non-Malicious AND • Resulting harm is low 	<ul style="list-style-type: none"> • Verbal or written reprimand • Retraining on privacy/security awareness • Discussion of policies and procedures with supervisor and/or Privacy Officer
2	<p>-Failure to follow established privacy and security policies and procedures- An individual demonstrates poor job performance or lack of performance improvement. Individual, in committing the breach, is careless or negligent. Examples of Level 2 violations include:</p> <ul style="list-style-type: none"> • releasing PHI without proper patient authorization; • failure to report privacy and security violations; • improper disposal of PHI; • failure to properly safeguard password; • failure to safeguard portable device from loss or theft; or • transmission of PHI using an unsecured method. • Workforce member fails to report that his/her password has been potentially compromised (i.e. victim of phishing scheme) • accessing one's own PHI without following normal release of information request procedures • Intentionally accessing the PHI of an Individual of Interest without a need to know, which is determined by the Privacy Officer to be low risk because evidence suggests that the affected patient approved of the access or would have approved of the access; <p>-Third (3rd) occurrence of a Level 1 Violation within 3 years</p>	<ul style="list-style-type: none"> • Generally Negligent AND • Non-malicious AND • Resulting harm is moderate 	<ul style="list-style-type: none"> • Letter of Reprimand • Suspension of access to patient care systems and/or other information systems containing PHI • Suspension of employment • Subject to reoccurring electronic medical record system user access audit

<p>3</p>	<p>-Intentional violation without harmful intent. An individual intentionally violates HIPAA policies is motivated by curiosity, concern, compassion, or desire to gain information, without a legitimate need to know. Examples of this include:</p> <ul style="list-style-type: none"> • Accessing information of high profile people; • Intentionally accessing the PHI of an Individual of Interest without a need to know, which is determined by the Privacy Officer to be moderate risk; • Intentionally assisting another individual to gain unauthorized access to PHI. This includes giving another individual your unique user name and password to access PHI • Disclosing patient condition, status or other PHI obtained as a result of individual's position at HHSC to another HHSC Workforce member who does not have a legitimate need to know; • Logs into HHSC network resources and allows another individual to access PHI; • Installing unauthorized software or application with potential harm to EMR <p>-Sharing passwords or badges -Second occurrence of any Level 2 Violation within three (3) years -Level 2 violation that includes PHI that has added protections, such as information related to HIV status, psychiatric, substance abuse, and genetic data</p>	<ul style="list-style-type: none"> • Intentional AND • Non-malicious AND • Resulting harm is greater than moderate 	<ul style="list-style-type: none"> • Final written warning • Suspension of employment (without pay) • Suspension of access to patient care systems and/or other information systems containing PHI less than thirty (30) days • Subject to reoccurring electronic medical record system user access audits • Possible termination of employment, depending on factors that indicate greater damage caused by the violation
<p>4</p>	<p>-Intentional violation for malice or personal or financial gain, such as:</p> <ul style="list-style-type: none"> • Intentionally assisting another individual to gain unauthorized access to PHI to cause harm to the patient or for personal and/or financial gain. This includes giving another individual your unique user name and password to access electronic PHI that results in personal/financial benefit for the Workforce member/ and/or individual, and/or harm to the patient • Access, disclosures, or uses PHI for financial and/or personal benefit to the Workforce member or another individual (i.e. lawsuit, marital dispute, custody dispute); • Uses, accesses, or discloses PHI that results in personal, financial, or 	<ul style="list-style-type: none"> • Intentional AND • Malicious or with gross negligence (complete disregard to known serious consequences) AND/OR • Resulting harm is significant 	<ul style="list-style-type: none"> • Immediate Termination of Employment/Contract

	<p>reputational harm or embarrassment to the patient;</p> <ul style="list-style-type: none"> • Utilizes HHSC computing resources, including the network, that are either related to or result in events that are reportable to the FBI; <p>-Second occurrence of any Level 3 violation within three (3) years -Third occurrence of any Level 2 violation within three (3) years -A Level 1 or 2 or 3 occurrence that affects more than 100 patients -A Level 3 occurrence, relating to snooping or curiosity, that affects more than five (5) patients - A Level 3 occurrence that includes PHI that has added protection such as information related to HIV status, psychiatric, substance abuse and genetic data</p>		
--	--	--	--

III. **Whistleblowers and Victims of a Crime.** A Workforce member shall not be disciplined if they are either a whistleblower or a victim of a crime and disclosed PHI in accordance with this section:

- A. **Whistleblowers-** If a Workforce member was acting in good faith while engaging in the following conduct:
- i. A Workforce member believed that HHSC has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or believes that the care, services, and conditions provided by HHSC potentially endangers one (or more) patients, Workforce members, or other members of the general public and discloses such information to appropriate authorities; and
 - ii. Discloses PHI to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of HHSC; or
 - iii. Discloses PHI to an appropriate healthcare accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by HHSC; or
 - iv. Discloses PHI to an attorney retained by or on behalf of the Workforce member for the purposes of determining the legal options of the Workforce member with regard to the alleged unlawful conduct.
- B. **Victims of a Crime-** If the Workforce member was a victim of a crime and disclosed PHI to a law enforcement official only if:
- i. The PHI disclosed is about the suspected perpetrator of the criminal act; and
 - ii. The PHI disclosed is limited to:
 1. Name and address;
 2. Date and place of birth;
 3. Social security number;
 4. ABO blood type and RH factor;
 5. Type of injury
 6. Date and time of treatment;
 7. Date and time of death, if applicable; and

8. Description of distinguishing physical characteristics, including height, weight, gender, race, hair, eye color, presence or absence of facial hair, scars, and tattoos.

- IV. **Non-Retaliation and Non-Retribution Policy.** In accordance with HHSC's "Non-Retaliation and Non-Retribution Policy" CMP 0018, a Workforce member shall not be subject to intimidation, threats, coercion, or discrimination from any other HHSC employee if that the Workforce member:
- A. Files a HIPAA related complaint with HHSC or the Secretary of Health and Human Services or testifies, assists, or participates in an investigation, compliance review, proceeding, or hearing as it relates to alleged HIPAA violations at HHSC; OR
 - B. Opposes any act or practice unlawful under state and federal regulations; AND
 - C. Provided that the Workforce member acted in good faith believing that the practice was unlawful, the manner of opposition was reasonable, and the Workforce Member's opposition did not involve disclosure of patient PHI in violation of regulations.

AUTHORITY:

- Hawaii Revised Statutes (HRS) Chapter 323F-7

RELATED POLICIES:

- CMP009A and B - Compliance Investigations
- CMP0058A - HIPAA Policy
- ITD0016A - Sanctions

REFERENCE(S):

- 45 C.F.R. § 164.308(a)(1)(ii)(C)
- 45 C.F.R. § 164.502 (j)
- 45 C.F.R. § 164.512(f)(2)(i)
- 45 C.F.R. § 164.530(e)