## INTERIM POLICY

**Section:** HIPAA Sanction Policy for Employee Privacy and Security Violation
**Adoption Date:**
**Revision Date:**
**Sponsoring Unit/Department:** Finance and Administration

# HIPAA Sanction Policy for Employee Privacy and Security Violation

This policy outlines sanctions against employees for breaching privacy policies and procedures as promulgated under the Health Insurance Portability and Accountability Act of 1996, CFR 164.520 ("HIPAA").

The College is committed to educating and holding all employees accountable for maintaining strict confidentiality for all records and information, hard-copy or digital, that contain Personal Health Information protected under HIPAA. Any breaches of that policy will be subject to tiered sanctions as described below. The College retains the discretion to impose different or additional sanctions regardless of the level of the violation based on the totality of the circumstances.

**Exceptions:**

Sanctions as described in this policy shall not be imposed against employees or business associates for the following actions:

- Engaging in whistleblower activities,
- Submitting a complaint to the Secretary of the Department of Health and Human Services,
- Participating in an investigation, or
- Registering opposition to a violation of this HIPAA Sanction Policy.

**Level I Violation:**

A Level I violation is accidental or due to lack of privacy/security education, such as, but not limited to:

- Leaving a computer terminal unattended with privacy information accessible.
- Accessing an employee's personal health record without authorization.
- Requesting another employee to access their record.
- Sharing password(s) for computer login with other employees.

Corrective Action for Level I violation may include:

- Verbal warning and retraining in policy and procedure related to HIPAA. See General Expectations for Supervisors.
- Written warning and retraining in policy and procedure related to HIPAA.

**Level II Violation:**

A Level II violation is a purposeful disregard for the College's HIPAA privacy policy, such as, but not limited to:

- Purposefully accessing a medical record without a legitimate reason to do so.
- Using another employee's access code without the employee's authorization.
- Accessing and using aggregate data from Banner or other computer systems that contain or process Private Health Information (PHI)/Electronic Private Health Information (ePHI) without institutional approval.
- Releasing PHI/ePHI without obtaining proper identification and/or correct disclosure authorization.
- Repeat of Level I violation after appropriate training had occurred.

Corrective action for a Level II violation may include:

- Final written warning and training with a letter in personnel file related to the incident.
- One to three days suspension and additional training (dependent on severity of violation determined by the Assistant Vice Chancellor ("AVC") for Human Resources or their designee).

**Level III Violation:**

A Level III violation is a malicious disregard of the College's HIPAA privacy policy, such as, but not limited to:

- Releasing PHI/ePHI for personal gain or gain from outside an entity.
- Releasing PHI/ePHI or any data with the intent to harm an individual or the College.
- Altering or destroying PHI/ePHI or any health data.
- Repeat Level II violation.

Corrective Action for Level III violation will generally be termination of employment (determined by the AVC for Human Resources or their designee).

**Reporting:**

All reports of privacy violations regardless of level will be treated with respect and confidentiality for both the employee and the person's whose PHI/ePHI is implicated. The reports will be filed with the College's AVC for Human Resources or their designee.

**Retention and Accounting for Disclosures:**

Privacy record violations will be recorded and maintained in the Human Resource's respective personnel file. All confirmed violations will be tracked in the Disclosure Log for PHI/ePHI disclosures and authorizations.