SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: HIPAA SANCTIONS POLICY

PURPOSE

This policy outlines the UAMS procedures for disciplining UAMS employees for violations of HIPAA and UAMS HIPAA policies and procedures.

SCOPE

This policy applies to all UAMS employees. For purposes of this policy, "employee" does not include Faculty or Tenured-Track Positions.

DEFINITIONS

Gross misconduct means an employee's serious wrongdoing, unlawful behavior, or improper behavior justifying immediate dismissal.

Malice means the intent, without justification or excuse, to perform a wrongful act.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act, health information about UAMS employees maintained by UAMS in its role as an employer and health information regarding a person who has been deceased for more than 50 years.

Click the following link to access any other terms or definitions referenced in this policy: http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf

POLICY

It is the policy of UAMS to ensure compliance with all applicable state and federal laws providing for the privacy and security of protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"). UAMS will use a progressive disciplinary process when a UAMS employee fails to comply with HIPAA or with UAMS HIPAA policies or procedures relating to the privacy and security of PHI. The progressive disciplinary process will follow the disciplinary action provisions and guidelines set forth in this policy and

other applicable UAMS policies and procedures.

PROCEDURE

I. Levels of HIPAA Policy Violations

UAMS will use a progressive disciplinary process for violations of UAMS HIPAA policies and procedures and violations of federal HIPAA rules and regulations. The level of a HIPAA violation is determined according to the severity of the action, whether the violation was intentional or unintentional, the impact on the organization, the impact on a patient or other employee(s), and whether the violation indicates a pattern or practice of improper use or disclosure of PHI, ePHI or other confidential information by the employee. Disciplinary action will be applied based on the level of violation in conjunction with any other mitigating factors.

A. Level One – Unintentional Violation or Carelessness. A **Level One** violation occurs when an employee unintentionally or carelessly discloses confidential information to anyone who does not have a legitimate need to know the information or when an employee unintentionally or carelessly accesses, reviews or discloses confidential information outside the performance of his/her job duties.

Examples. **Level One** violations include, but are not limited to:

- Inadvertently e-mailing, faxing, mailing, or distributing PHI or other confidential information to the wrong person;
- Releasing PHI without the appropriate patient authorization;
- Leaving PHI in a public area in the workplace; Improperly disposing of PHI or ePHI; Failing to safeguard portable devices/electronic media that contain ePHI, including but not limited to having PHI on an unencrypted laptop, unencrypted portable drive or unencrypted mobile device;
- Failure to report a HIPAA breach or HIPAA violation;
- Failing to secure e-mail, text message, or other electronic transmission or storage of PHI;
- Discussing patient information in a public area without taking reasonable measures to protect the discussion;
- Failing to properly verify the identity and access rights of a person requesting PHI, whether the person is requesting in person, in writing, or by phone;
- Intentionally accessing an employee's own record using their own employee log on credentials to UAMS clinical information systems when there is no job-related need for such access;
- Failing to protect the privacy and confidentiality of medical records or other PHI or ePHI (e.g., permitting improper access or conducting improper distribution or disposal of PHI);
- Failing to lock computer screen when workstation/laptop is left unattended or failure to appropriately log off the organization's information system;
- Leaving more than the minimum required PHI on patient's answering machine;
- Carelessly handling usernames and passwords (e.g., leaving notes with passwords

written on them on or near a computer or door key pad);

- Failing to report a lost or stolen mobile device or camera containing PHI in a timely manner; or
- Committing multiple occurrences of carelessly enabling or allowing an unauthorized person or persons to gain access to UAMS information systems or other confidential information which could compromise patient confidentiality. This could include but is not limited to providing to an unauthorized person log-on credentials to UAMS information systems, clicking on a link contained in a fake, scam phishing email, or opening an attachment contained in a fake, scam phishing email designed for the purpose of gaining access to the UAMS domain.

1. **Disciplinary Action.**

    a. A **Level One** violation will be grounds for progressive disciplinary action and will generally result in the employee receiving an oral warning.
    b. **Aggravating Factors.** A **Level One** violation may be treated as a **Level Two** or **Level Three** violation, depending on the magnitude of risk created, the harm to an affected individual or entity whose privacy or security was breached, breach of particularly sensitive information, large volume of data was breached, employee involved hampers or otherwise fails to cooperate with the investigation, the employee knew or should have known he/she was violating a HIPAA policy, procedure, rule or regulation, prior violations, or other disciplinary actions imposed on an employee for any reason.
    c. **Mitigating Factors.** Disciplinary action will be applied for **Level One** violations in conjunction with any mitigating factors. Mitigating factors for **Level One** violations may include, but are not limited to, a violation that occurs as a result of attempting to help a patient or UAMS, violations that do not result in harm to an individual or to UAMS, the violation is the employee's first such violation with no prior incidents that were **Level One** violations, the UAMS employee cooperates with the investigation and appreciates the nature of the violation, the UAMS employee could not have known or reasonably did not know of the applicable policy or procedure.

B. Level Two – Intentional or Purposeful Violation or Curiosity/Concern. A **Level Two** violation occurs when an employee **intentionally or purposefully** accesses, uses, reviews and/or discloses confidential information in an unauthorized manner or for unauthorized purposes, but for reasons unrelated to personal gain.

Examples. **Level Two** violations include, but are not limited to:

- Sharing a computer password with another person or group or using a password that belongs to someone else;
- Failing to follow device and media control standards, including connecting unapproved devices (e.g., jump drives, flash drives, smart phones, PDAs) to the organization's network;
- Sharing patient information with any individual who does not have a legitimate need

to know the information to perform job duties;

- Misusing information systems or violation of security safeguards;
- Committing a second or third incident of a **Level One** violation;
- Intentionally or purposefully posting on the Internet (including, but not limited to, YouTube and social media sites such as Facebook, Instagram, Linked In, Twitter) PHI or information that is not PHI but is related to a particular patient in violation of UAMS policies and/or for unauthorized purposes, for reasons unrelated to personal gain, monetary gain, malice or gross misconduct; or
- Intentionally accessing any patient's record without a job related reason, including searching for the existence of a record or an address or phone number. (This specific action will automatically result in a written warning and may result in dismissal.)

1. Disciplinary Action.

    a. A **Level Two** violation will be grounds for progressive disciplinary action and will generally result in the employee receiving a written warning.
    b. **Aggravating Factors.** A **Level Two** violation may be treated as a **Level Three** violation, depending on the magnitude of risk created, the harm to an affected individual or entity whose privacy or security was breached, breach of particularly sensitive information, large volume of data was breached, employee involved hampers or otherwise fails to cooperate with the investigation, the employee knew or should have known he/she was violating a HIPAA policy, procedure, rule or regulation, prior violations, or other disciplinary actions imposed on an employee for any reason.
    c. **Mitigating Factors.** Disciplinary action will be applied for **Level Two** violations in conjunction with any mitigating factors. Mitigating factors for **Level Two** violations may include, but are not limited to, a violation that occurs as a result of attempting to help a patient or UAMS, violations that do not result in harm to an individual or to UAMS, the **Level Two** violation is the first such violation on the part of the employee with no prior violations, the UAMS employee cooperates with the investigation and appreciates the nature of the violation, the UAMS employee could not have known or reasonably did not know of the applicable policy or procedure.

C. Level Three – Violation for Personal Gain or Malice or Acts of Gross Misconduct. A **Level Three** violation occurs when an employee accesses, uses, reviews, and/or discloses confidential information for personal or monetary gain or with malice or engages in acts of gross misconduct. Personal gain or malice or gross misconduct includes intentional wrongful actions without justification.

Examples. Level Three violations include, but are not limited to:

- Inappropriately using or selling confidential information or PHI, such as accessing and using PHI in a court proceeding to receive personal or financial gain or stealing PHI for fraudulent purposes to open credit card accounts, file fraudulent tax returns with the Internal Revenue Service or to create a false identity;

- Committing a second instance of intentionally accessing any patient's record or information without a job related reason;
- Disclosing PHI from any source of information, verbally, written, or any other format or mechanism, for any reason other than job related;
- Posting PHI or information that is not PHI but is related to a particular patient on the Internet (including but not limited to social media sites such as Facebook, Instagram, Linked In, Twitter) in violation of UAMS HIPAA policies and/or UAMS policies regarding social media;
- Falsifying or altering patient information;
- Obtaining PHI under false representation;
- Using confidential information to harass or intimidate other individuals or to cause an individual harm, either internal or external, to the organization;
- Deliberately compromising electronic information security measures;
- Handling confidential information with gross negligence;
- Subverting network controls or escalating privileges without authorization to do so;
- Failing to cooperate during the investigation of a potential HIPAA policy violation or privacy or security incident;
- Falsifying information during an investigation or reporting in bad faith or for malicious purposes; and/or
- Repeatedly committing a **Level One** or a second **Level Two** violation.

1. Disciplinary Action

a. Unless extenuating circumstances can be identified, **Level Three** violations will be treated as grounds for immediate dismissal under this Policy.

b. **Aggravating Factors.** In addition to dismissal, the employee may be subject to other sanctions and disciplinary actions, including but not limited to notifying law enforcement, reporting the violation to the appropriate regulatory or governmental authority, reporting the violation to the appropriate licensing board, or monetary fines and penalties in accordance with state or federal law. Such additional sanctions and disciplinary actions may be imposed based on such factors as the magnitude of risk created, the harm to an affected individual or entity whose privacy or security was breached, breach of particularly sensitive information, large volume of data was breached, employee involved hampers or otherwise fails to cooperate with the investigation, the employee knew or should have known he/she was violating a HIPAA policy, procedure, rule or regulation, prior violations, or other disciplinary actions imposed on an employee for any reason.

c. **Mitigating Factors.** Disciplinary action will be applied for **Level Three** violations in conjunction with any mitigating factors. Mitigating factors for **Level Three** violations may include, but are not limited to, a violation that occurs as a result of attempting to help a patient or UAMS, violations that do not result in harm to an individual or to UAMS, the UAMS employee cooperates with the investigation and appreciates the nature of the violation, the UAMS employee could not have known or reasonably did not know of the applicable policy or procedure.

II. Other Disciplinary Actions

A violation of HIPAA or UAMS HIPAA policies or procedures may result in suspension without pay or administrative leave in accordance with UAMS Policy 4.4.02 Employee Discipline.

A. Suspension Without Pay: If immediate dismissal for cause is not appropriate for repeated infractions or a single serious offense, a supervisor may place an employee on suspension without pay in addition to issuing a written warning. This means while immediate dismissal for repeated offenses or a single serious offense is too severe, suspension without pay is appropriate. An employee may be suspended without pay for one to five workdays, but a suspension period may not exceed 40 work-hours. While on suspension without pay, an employee may not use accrued leave.

B. Administrative Leave: An employee may be placed on administrative leave during investigations of suspected gross misconduct. Administrative leave is appropriate when an employee's absence during an investigation of gross misconduct is in the best interest of the employee and UAMS. At the conclusion of the investigation, the employee may either be dismissed (effective the last day worked) or reinstated without loss of pay.

C. Approval of Office of Human Resources Required. Supervisors must consult with OHR Employee Relations and receive approval from OHR Employee Relations before placing an employee on suspension without pay or administrative leave. OHR Employee Relations will provide instructions regarding appropriate documentation of suspension without pay and administrative leave.

III. Determination of Level of Violation and Disciplinary Action

The Office of Human Resources will make a final determination as to the level of the violation, the appropriate disciplinary action, whether the employee is eligible for rehire and whether the employee should not have future access to UAMS information systems. Managers and supervisors must contact the Office of Human Resources, Employee Relations prior to issuing a written warning and prior to terminating an employee. The HIPAA Privacy Officer and/or Security Officer, in cooperation with the employee's manager or supervisor, may make a recommendation to the Office of Human Resources as to whether an employee's behavior constitutes a **Level One, Level Two,** or **Level Three** violation. A recommendation may also be made as to whether the employee is eligible for rehire and/or whether the employee should not have future access to UAMS information systems.

IV. Training

Any UAMS employee whose relationship with UAMS is not terminated may be required to complete training through the UAMS HIPAA Office and/or UAMS IT Security Office in order to continue working at or attending UAMS. Such training may include, but is not limited to, an online training module through the UAMS HIPAA Office. Such training may be required in addition to

or in lieu of a disciplinary action issued as a result of a violation of HIPAA or UAMS HIPAA policies and procedures.

V. Documenting Disciplinary Actions for HIPAA Violations

Disciplinary actions resulting from violations of HIPAA or UAMS HIPAA policies or procedures must be documented in accordance with UAMS Administrative Guide Policy 4.4.02 Employee Discipline.

VI. References

UAMS Administrative Guide Policy 4.4.02 Employee Discipline
University of Arkansas System Board of Trustees Policy 405.1 Appointments, Promotion, Tenure, Non-Reappointment, and Dismissal of Faculty

Signature:  **Date: January 9, 2018**