PROCEDURE 2202-PR3
Implementation of Corrective Actions Involving Violations of Individual's Privacy or Security

Associated Policy: 2202, Privacy and Security of Protected Health Information under HIPAA
Effective Date: 2024/11/08
Latest Revision: 2024/11/08
Category: Community Expectations
Subcategory: Records

PURPOSE & OVERVIEW

The University is committed to conducting business in compliance with all applicable laws, regulations and University policies. The University endeavors to provide a strong infrastructure that promotes a culture committed to safeguarding the privacy and security of patient, medical and research participant information. These guidelines serve a dual purpose:

1. They provide faculty, staff, trainees, students, contractors, vendors, volunteers, and other members of the USU community ("workforce members") notice of the consequences they will face for violating the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology Economic and Clinical Health (HITECH) Act, or other federal and state laws and regulations governing the confidentiality and security of patient information ("applicable laws"), or University policies relating to privacy and security of patient, medical and research participant information.

2. The guidelines provide University offices (e.g., privacy offices, human resources, academic and student affairs offices) and individual managers direction in determining appropriate consequences for workforce members who violate applicable laws or University policies that safeguard protected health information ("PHI") and other patient medical information. These guidelines should be used in conjunction with the corrective action or discipline policy applicable to the relevant workforce member including:

    - Faculty Handbook Policy 4006.1-4, Academic Due Process: Sanctions and Hearing Procedures
    - Student Code of Conduct
    - USU Policy 3001, Setting Expectations and Managing Performance

For definitions pertaining to HIPAA, see 2202-D1, Definitions that Apply to Protected Health Information under HIPAA

PRINCIPLES

1. Imposition of Appropriate Sanctions

Workforce members will be sanctioned appropriately in the event that they:

(1) access, use or disclose more than the minimum PHI necessary to complete their job-related functions;
(2) fail to adequately protect PHI in accordance with USU's information security policies;

(3) fail to promptly report a known or suspected HIPAA violation; or
(4) violate any of USU's other HIPAA policies, procedures or guidelines.

Sanctions for violations of HIPAA may include, without limitation, counseling, written warning, reprimand, suspension, and/or termination. A workforce member's compensation and eligibility to continue in an academic or training program may also be impacted in the event of a violation. These guidelines are not intended to dictate a particular consequence in any particular situation. Rather, in consultation with the appropriate Human Resources and/or Privacy Office, managers, academic affairs and student affairs administrators have the discretion to decide:

(1) at which level to start the corrective action process based on the severity of the offense, the potential or actual harm to the patient and/or the University, and any mitigating factors; and
(2) whether immediate termination is justified based on the seriousness of the offense.

2. Levels of Violations

The level of a violation is determined as provided in existing USU policy and according to the severity of the privacy or security incident, whether it was intentional or unintentional or motivated by malice or personal gain, and the impact on the patient and/or institution. The following outlines some, but not all, types of violations and categorizes them broadly according to likely severity.

Level 1: A workforce member carelessly or inadvertently accesses PHI without a job-related need to know, or carelessly or unintentionally reveals PHI to which he/she has authorized access. Examples of Level 1 violations include, but are not limited to:

(1) Leaving PHI in a public area in the workplace or disposing of it in the trash instead of shredding receptacles;
(2) Misdirecting faxes, emails or other documents that contain PHI;
(3) Discussing PHI in public areas where the discussion could be overheard;
(4) Other behaviors reflecting carelessness or lack of judgment in handling PHI.

Level 2: A workforce member intentionally accesses PHI without authorization or seriously fails to protect PHI. Examples of Level 2 violations include, but are not limited to:

(1) Intentionally accessing or asking another to access PHI, without a job-related need to know, the PHI of a friend, relative, co-worker, public personality or any other individual (including searching for the existence of a record or an address or phone number);
(2) Leaving paper files and records, computers, laptops, notebooks, smart phones or other devices containing PHI accessible and unattended;
(3) Sharing log-in IDs and passwords with others;
(4) Using personal email accounts (e.g., Hotmail, Gmail, Yahoo), cloud computing, or other media or storage devices not approved by USU for transmission or storage of PHI or not meeting required security standards (such as encryption, secure email, password protection);
(5) Removing PHI from the USU workplace without supervisor approval or failing to appropriately safeguard PHI if removed with supervisor approval or while in transit;
(6) Other behaviors reflecting intentional conduct or serious failure to safeguard PHI.

Level 3: A workforce member intentionally accesses, uses or discloses PHI without authorization, possibly motivated by willful disregard, malice or personal gain. A Level 3 violation is considered serious misconduct. Examples of Level 3 violations include, but are not limited to:

(1) Intentionally using or disclosing without a job-related need to know the PHI of a friend, relative, co-worker, public personality, or any other individual's PHI;
(2) Accessing, using or disclosing PHI for personal purposes or gain, or with an intent to harm the patient or any third party;

(3) Discussing or disclosing PHI with any third party either directly or via social networking or blogging sites, such as Twitter and Facebook.
(4) Intentionally assisting an individual in gaining unauthorized access to PHI.
(5) Jeopardizing the integrity of USU's systems.
(6) Failing to cooperate during the investigation of a privacy or security incident.
(7) Falsifying information during a privacy investigation or reporting in bad faith or for malicious purposes.
(8) Other behaviors reflecting personal purpose or gain, malice or misconduct.

3. Considerations in Evaluating Violation for Appropriate Sanctions

Factors in determining appropriate disciplinary action shall follow existing USU policy for the type of workforce members involved and may include, but are not limited to:

(1) Whether the breach was intentional or inadvertent;
(2) The nature of the incident, including whether it involved specially protected information such as HIV, psychiatric, substance abuse, or genetic data;
(3) The magnitude of the disclosure, including the number of patients and the volume of Protected Health Information accessed, used or disclosed;
(4) The workforce member's motive in accessing, using or disclosing PHI, and whether there was an element of malice or desire for personal gain;
(5) Whether the workforce member has committed prior HIPAA violations;
(6) The workforce member's response or conduct during investigation;
(7) Risk of harm to the victim(s) of the breach or to the University;
(8) The existence of any compelling, aggravating or mitigating factors.

PROCEDURES

1. Prompt Reporting and Investigation

Each workforce member must report any alleged, apparent, or potential violations of HIPAA or applicable privacy and security laws promptly (within no more than twenty-four hours) to his/her supervisor/designee or to the supervisor's supervisor. Suspected violations shall be investigated appropriately and in coordination with the relevant supervisor, Human Resources officer, and the Privacy Officer. Matters involving faculty, students or trainees should also be brought to the attention of the appropriate dean(s) or division director(s). Initial determination of the level of each violation shall be recommended by the direct supervisor based on these guidelines, unless the supervisor is also involved in the violation. In such cases, the recommendation shall be made by the individual at the next level above the supervisor.

Results of the investigation and any decision regarding discipline will be documented as appropriate and disciplinary actions will be made part of the workforce member's personnel, training or student file. Discipline will be issued in accordance with existing discipline or corrective action policies applicable to the particular workforce member, including grievance procedures available to workforce members. Final authority concerning sanctions resides with university officers as set forth in policy. Such individuals will review any sanction involving suspension, dismissal, or termination before it is implemented. In most cases sanctions for level 1 violations shall be determined and carried out within the workforce members unit. Level 2 and 3 violations shall be determined by the supervisor, appropriate Human Resource representative, the assigned privacy officer, and the USU HIPAA Privacy or Security Officer.

2. Guidelines for Sanctions

The following will serve as guidelines for appropriate sanctions for violations of HIPAA or other applicable laws or policies.

Faculty:
Appropriate sanctions will be imposed in accordance with the Statement on Faculty Discipline, Faculty Handbook section 4006.1-4 and 11-12, as applicable.

Employees, post-doctoral fellows, volunteers:

- *Level 1.* Violations shall, in most cases, result in oral or written counseling and/or retraining. Repeat Level 1 violations shall be subject to further disciplinary action up to and including termination.
- *Level 2.* Violations shall, in most cases, result in a written disciplinary warning with or without an unpaid suspension, and retraining shall be required. Disciplinary action up to and including termination may be taken for repeat Level 2 violations.
- *Level 3.* Violations, in most cases, shall result in immediate termination of employment, academic appointment or ending of a volunteer assignment.

Students enrolled in undergraduate or graduate degree programs:

- *Level 1:* Violations shall, in most cases, result in oral counseling and/or retraining. Repeat Level 1 violations shall be subject to progressive disciplinary action up to and including termination from the program of study.
- *Level 2:* Violations shall, in most cases, result a written reprimand in the student's file and retraining. The student may also be suspended from the program of study.
- *Level 3:* Violations, in most cases, shall result in immediate termination from the program of study.

Contractors/Vendors:
Violations of any level may result in termination of the contract/business relationship and disqualification from future contractual/business relationships.

HISTORY

2019/02/01	Reformatted, minor corrections, added history, pending policy number assignment.
2019/07/30	Provided new numbering, minor edits.
2022/11/03	New number assigned.

ADDITIONAL INFORMATION

Workforce members are responsible for following policies and procedures and complying with regulations. For assistance to report possible violations or address concerns, you may contact your supervisor, the USU Privacy Official or the Legal Affairs Office, or a USU Healthcare Plan Privacy Officer within the unit. For questions or concerns about the application of these procedures, you may also contact Human Resources.