POLICY INFORMATION

Document # **201**	Title: **Sanctions**	Print Date: **11/15/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **11/10/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 12/1/2016

I. POLICY STATEMENT

The purpose of this policy is to impose appropriate, consistent and equitable responses to confirmed HIPAA Privacy and Security violations regardless of an individual's or entity's status with CEHS, in accordance with 45 CFR §164.530 and 164.308(a)(1)(ii)(C).

II. DEFINITIONS

See HIPAA Policy 100

CEHS HCC Workforce Members means faculty, employees, students, volunteers and other persons whose conduct, in performance of work for CEHS is under the direct control of CEHS, whether or not they are paid by CEHS. This does not include Business Associates or their employees and agents.

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Components "HCC" (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the Health Care Components of CEHS.

IV. PROCEDURES TO IMPLEMENT

1. Responsibility to Report
    a. Workforce members and Business Associates have a responsibility to report suspected and known HIPAA violations. Reports may be made to any of the following:
        i. HCC Privacy Officer
        ii. HCC Director
        iii. CEHS Privacy Officer;
        iv. CEHS Security Officer; or
        v. USU ISO Security Officer
        vi. Incident Reporting Tool as available

    b. Failure to report a known HIPAA violation may result in disciplinary action in accordance with USU policies.

c. No one shall be retaliated against for making a good faith report.

2. Investigation
   a. If the clinic director receives the report, they will pass the information to either the HCC Privacy Officer, or the CEHS Privacy Officer, or CEHS Security Officer.
   b. When the appropriate Privacy or Security Officer receives the report, they will log the allegation and gather preliminary information. If that allegation is classified as level 1 or 2, has a low severity, and is the workforce member's first violation, they can document and close the incident. All other allegations must be reported to the CEHS Privacy and/or Security Officer who will be responsible to conduct a timely and confidential investigation.
   c. All investigations and incidents will be managed in accordance with CEHS Policy **700 - Security Incident Procedures** and USU policies.
   d. All investigations shall be documented. Documentation will be retained for six years.
   e. Access to HCC areas and systems may be revoked during the investigation.

3. Levels of HIPAA violations

   The level of HIPAA violation is determined based on the severity of the violation, whether it was intentional or unintentional, and whether the violation indicates a pattern of improper use, disclosure or release of PHI and/or misuse of computing resources. The degree of discipline could range from verbal warning up to and including termination of relationship with CEHS HCC. The following (4) levels of violations will be utilized in recommending the disciplinary action and/or corrective action to apply:

   a. **Level 1: Unintentional/Negligent.** This violation is mistaken access or disclosure of information. This is an unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error. Examples of Level 1 violations include, but are not limited to:
      - Directing PHI via mail, email, or fax to the wrong party.
      - Incorrectly identifying a patient record.

   b. **Level 2: Failure to follow established privacy and security policies and procedures.** This is a violation due to poor job performance or lack of performance improvement. Examples of level 2 violations include, but are not limited to:
      - Release of PHI without proper patient authorization.
      - Leaving detailed PHI on an answering machine.
      - Failure to properly safeguard password.
      - Failing to lock computer when leaving a work station.

c. **Level 3: <u>Deliberate or purposeful without harmful intent.</u>** This is an intentional violation due to curiosity or desire to gain information for personal use. Examples of level 3 violations include, but are not limited to, the following:
   - Looking at a coworker or neighbor's medical record.
   - Accessing or using PHI for personal gain (i.e., lawsuit, marital dispute, custody dispute).
   - Disclosing PHI for financial gain.

d. **Level 4: <u>Willful and malicious violation with harmful intent.</u>** This is an intentional violation causing patient or organizational harm. Examples of this type of violation include but are not limited to:
   - Unauthorized intentional disclosure and/or delivery of PHI to anyone;
   - Intentionally assisting another individual to gain unauthorized access to PHI;
   - Using, accessing or disclosing PHI resulting in personal, financial or reputational harm or embarrassment to the patient;
   - Utilizing CEHS computing resources, including the network, that either relates to or results in events that are reportable to HHS/OCR;

4. <u>Severity</u>
   There are three categories of severity across the four areas of risk levels. The categories should be utilized in recommending the disciplinary action and/or corrective action to apply:

Category	Potential harm done	Example purpose of Violation
Low	Little to no harm done to patient and HCC. No harm to CEHS or USU	Ignorance or lack of education
Medium	Some harm done to patient and only affects HCC involved	Snooping or curiosity
High	There is high probability violation cause harm to patient, HCC, CEHS and/or USU	Malice, sale or personal gain

5. <u>Response to Confirmed HIPAA Privacy or Security Violations</u>
   When it is determined that a violation has occurred, a sanctioning body will be convened to review the results of the investigation and decide appropriate sanctions.

   a. The following personnel may comprise a sanctioning body:

- CEHS Security & Privacy Officer
- Clinic Director
- Supervisor of workforce member in question
- HCC Privacy Officer
- Department Head over HCC
- CEHS Dean
- Director of Human Resources
- University Counsel
- Director of Information Security Office
- Vice President for Research
- Faculty Senate

b. The sanctioning body will uphold or modify the Risk Level determined in the initial investigation:
    i. Level 1
    ii. Level 2
    iii. Level 3
    iv. Level 4

c. The sanctioning body will uphold or modify the level of Severity determined in the initial investigation:
    i. Low
    ii. Medium
    iii. High

d. The sanctioning body will determine the appropriate sanctions.

6. Additional Factors

Sanctions may be modified based on additional factors that could either lessen or heighten the penalty:

a. Factors that might lessen the penalty:
    - Violator knowledge of privacy and security practices (e.g., inadequate training)
    - HCC is found to have inappropriate practices
    - Violation occurred as a result of attempting to help a patient
    - Victim(s) suffered no financial, reputational, or other personal harm
    - Action was taken under pressure from an individual in a position of authority

b. Factors that might heighten the penalty:
    - Violation of specifically protected information such as mental health records, substance abuse, or genetic data
    - High volume of people or data affected
    - High exposure for the HCC, CEHS, and/or USU
    - Large organizational expenses incurred for the HCC, CEHS, and/or USU
    - Hampering the investigation, lack of truthfulness
    - History of performance issues and/or violations

7. Notification of State or Federal Agencies
   Depending on the circumstances of the violation, notification to State or Federal agencies may be required. Notification to these agencies should be under the direction of the Dean of CEHS, University President, counsel, public relations and the Information Security Office. See **CEHS Privacy Policy 202: Breach Notification**. Certain violations may also be reported to law enforcement officials and/or regulatory, accrediting and/or licensure organizations.

V. ATTACHMENTS

N/A

VI. REFERENCES

CEHS HIPAA Privacy Policy 106: Patient Right to Request an Accounting of Disclosures

CEHS HIPAA Privacy Policy 202: Breach Notification

CEHS HIPAA Privacy Policy 700: Security Incident Procedures

CEHS HIPAA Privacy Policy: Minimum Necessary 117

USU Policy 311: Corrective Action (Exempt & Non-Exempt Staff)

USU Policy 407: Academic Due Process; Sanctions & Hearing Procedures

Utah State Board of Regents Policy R345

CFR 164.308(a)(1)(ii)(C)