Oklahoma State University

Title: Sanctions	**Policy #: PRV-13.05**
Category: HIPAA Compliance	**Authority: 45 CFR § 164.530(e)(1), 164.308(a)(1)(ii)(c)**
Standard: Sanctions	**Responsibility: Health Care Components**
Effective Date: 4/14/2003	**Pages: Page 1 of 3**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

This policy covers the possible sanctions against OSU workforce members who fail to comply with the policies and procedures of this organization in regards to HIPAA.

POLICY:

OSU will apply appropriate sanctions against workforce members who fail to comply with the HIPAA policies and procedures of OSU. *§164.308(a)(1)(ii)(C)*

This policy does not cover the subject of sanctions taken by the regulating agencies against OSU. It does not apply to employees with respect to actions or disclosures of whistle blowers or victims of crime.

Sanctions will be consistent with existing OSU policy and procedures regarding discipline in the workplace. Sanctions are made at the discretion of administration and may range from a verbal warning to termination of employment.

OSU will maintain documentation of all sanction policies. Training will be provided to all employees for clarification purposes. Training records will be maintained in the HIPAA Compliance Office and/or designated locations.

Violations and sanctions will be documented and maintained in the employees' personnel file.

OSU employees are protected from intimidation, threats, coercion, discrimination, or other retaliatory actions for filing a complaint with the Secretary of Health and Human Services (HHS) under subpart C of part 160, the Enforcement Rule.

There are many types of a breach or violations of HIPAA. Some common examples that an individual may receive sanctions for, include but are not limited to:

- Discussing patient information in a public area.
- Leaving a copy of patient information in a public area.
- Leaving a computer unattended in an accessible area with Protected Health Information (PHI) unsecured.
- Accessing and viewing the record of a patient out of curiosity or concern (coworker, supervisor, public personality, own medical record, etc.).

- Releasing information without appropriate authorization, to include discussion about a patient not related to direct patient care.
- Removing any document with PHI, whether paper (including but not limited to medical record, schedules, test results, or EOB) from the premises that is not applicable to Treatment, Payment or Operations (TPO).
- Violating passwords or log-on policy.
- Removal of equipment or any computer device containing ePHI (including but not limited to disks, flash drives, or email).
- Maintaining ePHI in unsecure areas outside of a network storage drive.
- Reviewing patient records to use information for personal relationship (including but not limited to accessing birthdate or address)
- Compiling a mailing list of patients for personal use or financial gain.
- Sale of any PHI to an individual, company, or corporation.
- Caused or participated in any theft or compromise of PHI.
- Failure to report a known or suspected HIPAA violation of oneself or a coworker.

All breaches and/or violations of HIPAA and/or OSU policy are eligible for sanctions against the employee(s) involved, whether they know or should have known about the issue.

Depending on the severity of the offense all breaches and/or violations may receive any of the following sanctions:

- Verbal warning and retraining
- Plan of Corrective Action
- Warning letter with plan of corrective action with a notice of possible termination
- Revocation of system access
- Suspension without pay
- Termination
- Reports to law enforcement, licensing agencies or other officials as necessary.

The level of sanctions for all breaches/violations depends on the size, scope, intent and the employee's prior history. Employees in a supervisory role will be held to a higher standard.

PROCEDURE:

1. All employees are obligated to report any known or suspected breach or violation of HIPAA or OSU policy.

2. All reports are to be made to the HIPAA Compliance Officer either via phone, in person, email, or ethicspoint.
3. If a report is made to any other individual besides the HIPAA Compliance Officer or his/her designee, that individual must report it to the HIPAA Compliance Officer. *For example, a report is made to a supervisor; the supervisor shall report the issue to the HIPAA Compliance Officer.*
4. Upon notification of a possible or suspected breach or violation, the HIPAA Compliance Officer will conduct an investigation without unreasonable delay.
5. The HIPAA Compliance Officer may enlist the help of the Department of Information Technology, Human Resources, the HIPAA Steering Committee, OSU General Counsel, Outside Legal Counsel, Administration, the Office of the President of OSU, and the State Board of Regents if need be.
6. As part of the investigation, the HIPAA Compliance Officer will take into account the following four factors:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.
7. Upon completion of the investigation, the HIPAA Compliance Officer will write a report, detailing the events of the issue, without further disclosing any PHI, and provide recommendations as to how to resolve and mitigate the issue.
8. The report will be kept on file in the HIPAA Compliance Office and sent to Human Resources, where sanctions will be determined. *Please see above list of possible sanctions.*
9. The HIPAA Compliance Officer will then notify all affected patients following the procedures in the Breach Notification Policies.
10. The HIPAA Compliance Officer will meet with the HIPAA Steering Committee to discuss the issue and address the mitigation of the now known problem, if needed.
11. At any time throughout this process, a report to law enforcement or a licensing or regulatory agency may be made at the discretion of Administration.

REFERENCE:

SEC-01.03