

Regulatory Reference 45 CFR 164.530 (e)(1)(2)

Policy #:

Responsible Reviewer:

Originated:

Reviewed:

Revised:

Next Review Date:

**WORKFORCE DISCIPLINARY ACTIONS for
CONFIDENTIALITY and INFORMATION SECURITY VIOLATIONS**

PURPOSE: To facilitate compliance with policies and procedures regarding the confidentiality and security of protected health information (PHI).

DEFINITIONS:

Workforce: *for the purposes of this policy* includes employees, contractors, consultants, students, volunteers, other temporary staff and medical staff.

Facility specific: refers to a _____ policy.

Privacy and Confidentiality are terms used interchangeably for the purposes of this policy.

POLICY:

It is the policy of _____ (“___”) to apply sanctions consistently for privacy-related violations. The minimum recommended privacy violation level grid under the “Procedure” section of this policy provides the suggested methodology for determining the severity of the privacy violation. The grid also outlines levels of breaches, provides examples and the recommended actions.

PROCEDURE:

- A. For any suspected privacy and/or information security violation, the Privacy Officer or a member of the Compliance Department, or after normal business hours the Administrator-on-call, is to be notified immediately as described in policy _____ *Patient Protected Health Information Program*, _____ *Confidentiality of Information* and facility specific policy _____ *Complaints From Patients and Families*.
- B. The grid below is to be used as a guide for determining the severity of the privacy violation and for determining actions to be taken.

Level and Definition of Violation	Example of Violation	Recommended Action
Level I	• Improper disposal of PHI	• Retraining and re-evaluation

<p>Accidental and/or due to lack of proper education</p>	<ul style="list-style-type: none"> • Improper protection of medical records or other PHI <ul style="list-style-type: none"> - Leaving records on counters or where otherwise accessible by unauthorized individuals - Leaving any documents that contain PHI in inappropriate areas. • Not properly verifying individuals by phone, in person or in writing. • Not accounting for disclosures outside of treatment, payment or health care operations within the correct system or manual process. 	<ul style="list-style-type: none"> • Documented verbal warning with discussion of policy, procedures and requirements.
<p>Level II Purposeful violation of privacy policy or second occurrence of Level I violations.</p>	<ul style="list-style-type: none"> • Accessing or using PHI without having a legitimate job-related need to do so. • Not forwarding appropriate information or requests to the Privacy Officer for processing. 	<ul style="list-style-type: none"> • Retraining and re-evaluation. • Written warning with discussion of policy, procedures and requirement. • Possible suspension.
<p>Level III Purposeful violation of privacy policy with associated potential for patient harm.</p>	<ul style="list-style-type: none"> • Disclosure of PHI to unauthorized individual or company. • Sale of PHI to any source. • Any uses or disclosures that could invoke harm to a patient. 	<ul style="list-style-type: none"> • Termination. • Revocation of medical staff privileges. • Termination of vendor or other affiliation contract.

- C. Depending on the number and/or severity of Level I or Level II violations, recommended action for a Level III violation may be applicable. For example, the purposeful invasion of a patient’s privacy, even if not disclosed to others, may result in a Level II or III action.
- D. Violations involving contracted individuals should be referred to the General Counsel.
- E. Violations involving credentialed staff should be referred to the Chief Medical Officer.
- F. The Privacy Officer or a designee in conjunction with the employee’s manager and a representative of Human Resources will participate in the investigation and the documentation process, with all results to be reviewed by the General Counsel.

- G. Failure to report a known or suspected privacy and information security breach may result in disciplinary action.
- H. Reporting of a privacy and information security breach in bad faith or for malicious reasons may result in disciplinary action.
- I. No employee is terminated without a thorough investigation. Investigative facts are reviewed by the _____ or _____ before termination of employment may occur.
- J. Employees who disagree with a disciplinary action taken as a result of a privacy and information security breach may utilize the grievance process, as outlined in policy _____ *“Conflict Resolution for Employees.”*

APPROVED BY: _____

APPROVED BY: _____

APPROVED BY: _____