



Subject:	<b>Sanction Policy</b>	Policy No.: AS112
Signature		Original Issue: 4/12/05
SEC Approval:	Marilee McGuire	Date: 4/11/05
Prepared By:	Carrie Hardie	Effective Date: 4/20/05

**Purpose:**

The purpose of this policy is to establish appropriate sanctions for workforce members who fail to comply with the privacy or security policies and procedures of Community Health Plan (CHP).

CHP will ensure all workforce members comply with CHP's privacy and security policies as well as state and federal regulations such as HIPAA by applying sanction and disciplinary actions appropriate to the breach of policy.

**Scope:**

This policy applies to all CHP workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, and temporary workers.

**Policy:**

CHP will appropriately and consistently discipline employees and other workforce members for any violation of privacy or security policies or procedures to a degree appropriate for the gravity of the violation.

CHP will record all disciplinary actions taken in the employment records of the employee.

CHP will investigate all privacy or security incidents or violations and mitigate to the extent possible any negative effects that the incident may have had in a timely manner.

CHP and its workforce members will not intimidate or retaliate against any workforce member or individual that reports a privacy or security incident.

A copy of this Policy will be retained for a minimum period of six (6) years from the date it was created or, if revised, for a minimum period of six (6) years from the date it was last in effect.

**Responsibilities:**

All individuals identified in the scope of this policy are responsible for compliance with any sanction that is applied to them under this policy.

The CHP Privacy Officer is responsible for reviewing and investigating reported privacy incidents and violations of privacy policies.

The CHP Security Officer is responsible for reviewing and investigating reported security incidents and violations of security policy.

CHP Human Resources, Privacy and Security Officers are responsible for acting as a resource to the management when recommending appropriate discipline. Each case will be reviewed to

ensure fair and consistent application of sanctions for violations to policy. Human Resources will also document any applied discipline in the employee's personnel file.

**Compliance:**

Failure to comply with this or any other privacy or security policy will result in disciplinary actions as described in the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Sanction Policy is a required implementation specification defined within the Security Management Process standard (164.308 (a)(1)) in the Administrative Safeguards category of the HIPAA Security Rule.

**Procedure(s):**

1. **Violation of CHP privacy or security policies or procedures.** Failure to comply with the CHP privacy or security policies or procedures will result in disciplinary action against the individual committing the violation.
  - a. CHP privacy and security policies and procedures will be enforced consistently across the organization.
  - b. Sanctions that are imposed as a result of a violation of a CHP privacy or security policy or procedure will be imposed consistently across the organization.
  - c. The following types of conduct on the part of a member of CHP's workforce will result in disciplinary action against the individual engaging in the conduct:
    - i. Accessing a member's PHI out of curiosity or for any purpose outside of treatment, payment or health care operations.
    - ii. Discussing a member's PHI in a public area or outside of CHP.
    - iii. Failing to logoff or leaving a computer monitor on and unsecured.
    - iv. Using a member's PHI for personal reasons (such as developing a personal relationship with the member) rather than for legitimate and authorized business reasons.
    - v. Copying or compiling PHI with the intent to sell or use the PHI for personal or financial gain.
    - vi. "Hacking" into or otherwise attempting to gain unauthorized access into the CHP computer systems, network devices and/or applications.
    - vii. Failing to follow procedures to ensure secure transmission of PHI across an open network.
    - viii. Downloading unauthorized software to CHP systems, including workstations, laptops, PDAs, BlackBerrys, and USB storage devices.
2. **Disciplinary action that may be taken.**
  - a. Will be recommended by Human Resources and management, in consultation with the Privacy or Security Officer, as appropriate. It will be determined on a case by case basis, taking into consideration the specific circumstances and severity of the violation; and

- b. May be up to and including termination of employment, or of the business relationship as appropriate.
  - c. Sanctions that may be imposed include, but are not limited to:
    - i. Verbal reprimand by the employee's immediate supervisor, with summary documentation to the employee's personnel file;
    - ii. A written warning letter to the employee's personnel file;
    - iii. Administrative leave without pay;
    - iv. Attendance and successful completion of additional training;
    - v. Reimbursement of expenses incurred by CHP to resolve the matter; or
    - vi. Immediate termination of employment.
3. **Violations of state or federal confidentiality laws and regulations.** Workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of an individual's information are subject to criminal investigation and prosecution or civil monetary penalties.
4. **Duty to report.** Any workforce member who observes or becomes aware of or suspects a wrongful use or disclosure of PHI maintained by CHP is required to report his or her suspicion or the wrongful use or disclosure as soon as possible to his/her supervisor or the HIPAA Privacy Officer. Workforce members who become aware of security breaches must notify the Security Officer of the breach.
  - a. A workforce member who makes a report of a suspected or actual improper use or disclosure in good faith will not be retaliated against for making the report.
  - b. A workforce member who fails to report either a suspected or actual violation will have violated this Policy, and may be subject to disciplinary action, up to and including termination.
5. **No retaliation for good faith reports.** CHP will not retaliate against a member of its workforce who acts in good faith believing the practice he or she reports is unlawful or violates CHP policy. Any employee that believes that he or she has been subject to retaliation should immediately notify Human Resources.

**Form(s):**

None

**Definition(s):**

Definitions for all policies are included in the glossary section of the Appendix.

**References:**

- HIPAA Final Privacy Rule, 45 CFR Parts 160 through 164
- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.

- Getting Started with HIPAA, Uday O. Ali Pabrai, Premier Press, April 2003.
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E))

**Contact:**

See Master Contacts List

<b>Revision History</b>		
Revision Date	Revision	Revision Made By
10/24/05	Removal of Contacts and consolidation in Master Contact List	Carrie Hardie
3/22/06	Changed all references from "Community Health Plan of Washington" to "Community Health Plan" and "CHPW" to "CHP"	Carrie Hardie