



**COMMUNITY HEALTH PLAN**  
of Washington

*Committed to your health.*

Subject:	<b>Security Awareness and Training Policy</b>	Policy No.: AS109
Signature		Original Issue: 4/12/05
SEC Approval:	Marilee McGuire	Date: 4/12/05
Prepared By:	Carrie Hardie	Effective Date: 4/20/05

**Purpose:**

The purpose is to implement a security awareness and training program for all Community Health Plan (CHP) workforce members, including management.

CHP understands that “people”, not necessarily technology, are often the largest threat to the security of sensitive information, such as electronic protected health information (ePHI) in the organization.

**Scope:**

This policy applies to all CHP workforce members including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive information, such as ePHI, by CHP.

**Policy:**

CHP will ensure that all workforce members have been trained in and understand the security policies and procedures. In addition, all workforce members will be trained how to identify, report, and prevent potential security incidents.

Security training will be an ongoing activity at CHP. Periodic security reminders will keep workforce members up to date with new threats, such as computer viruses or “scams” to watch out for. The frequency and form these reminders take will be determined by the Security Officer but should include things like security-related flyers or posters in break rooms, reminders in paycheck stubs or emails, and verbal updates at staff meetings.

CHP will run anti-virus software on all computers that connect to the Internet and/or are networked together. Members of the workforce must be trained how to use the software and how to spot unusual activity that might indicate the presence of a virus. The anti-virus software must be kept up to date, as new viruses (and other types of malicious code) are discovered daily.

CHP will develop security policies to identify core activities in the areas of security reminders, protection from malicious software, log-in monitoring, and password management.

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 workforce members are responsible for understanding and following all security related policies and procedures, and asking their manager or the Security Officer for clarification when needed.

Managers are responsible for ensuring that all workforce members under their supervision complete all mandatory security training and serving as a resource for security-related questions.

The Security Officer is responsible for:

- Ensuring all workforce members understand and follow security related policies and procedures
- Maintaining an ongoing security awareness program at CHP
- Ensuring all workforce members understand and use the installed anti-virus software
- Keeping all anti-virus software up to date

The Security Officer is responsible for leading compliance activities that bring the CHP into compliance with the HIPAA Security Rule implementation specifications of:

- Security reminders
- Protection from malicious software
- Log-in monitoring
- Password management

**Compliance:**

Failure to comply with this or any other 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.

Security Awareness and Training is a standard (164.308 (a)(5)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

**Procedures:**

1. New workforce members are required to complete mandatory new hire security training within 60 days of hire.
2. Human Resources is responsible for notifying the Compliance Department of a new hire immediately, so that the new workforce member can be scheduled for training within the required timeframes.
3. All workforce members are required to complete ongoing security training as required by the Security Officer.
4. IT will issue periodic security awareness reminders to workforce members. All workforce members are responsible for reading the information and implementing any instructions contained in the security awareness reminders.

**Form(s):**

None

**Definition(s):**

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

**References:**

- 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