



COMMUNITY HEALTH PLAN
of Washington

Committed to your health.

Subject:	Accountability Policy	Policy No:	PS103
Signature		Original Issue:	4/12/05
SEC Approval:	Marilee McGuire	Date:	4/7/05
Prepared By:	Jeff Cains	Effective Date:	4/20/05

Purpose:

The purpose is to maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Scope:

This policy applies to Community Health Plan (CHP) in its entirety, all workforce members, including consultants, contractors, business associates and vendors. Further, the policy applies to all systems, networks, and applications, as well as all facilities, which process, store or transmit electronic protected health information (ePHI).

Policy:

CHP will ensure that a record is maintained to identify movements of ePHI-related hardware and devices. The movement of hardware, electronic media and devices includes the receipt, removal, storage and/or disposal of ePHI systems. Such information will also include the identity of responsible persons associated with the movement.

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:

The Security Officer will be responsible for ensuring the implementation of the requirements of the Accountability Policy.

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.

Accountability is an addressable implementation specification defined within the Device and Media Controls standard (164.310 (d)(1)) in the Physical Safeguards category of the HIPAA Security Rule.

Procedures:

The Desktop Support Analyst or other designated ITI team members are responsible for the movement of hardware, electronic media and devices. The procedures for handling the movement of hardware, electronic media and devices are as follows:

- Document all CHP owned desktop computers, laptop computers and other devices containing ePHI in the Configuration Management database.
- Document in the Inventory Control Access database whenever a user receives a desktop computer, laptop computer or other device.

- Update the Inventory Control Access database whenever a user no longer requires a desktop computer, laptop computer or other device, such as when the user's job function changes or the user is no longer employed by CHP.
- Refer to the Media Re-Use Policy for procedures related to reusing storage media.
- Complete the Retired Assets Donation form whenever a desktop computer, laptop computer or other device containing CHP information is donated or sold to an individual or organization for non-CHP business use.
- Completely remove all company information from desktop computers, laptop computers or other devices containing ePHI by overwriting the storage media in such devices as follows:

The storage media will be securely overwritten (sanitized) using Norton Ghost 8.0's GDisk in conformance with U.S. Department of Defense NISPOM (National Industrial Security Program Operating Manual), DoD 5220.22-M, January 1995. The NISPOM document is available at:

<http://www.dss.mil/isec/nispom.htm>

GDisk performs a sanitize operation, when performing a disk wipe operation with the following cycle occurring six times:

1. All addressable locations are overwritten with 0x35.
 2. All addressable locations are overwritten with 0xCA.
 3. All addressable locations are overwritten with a pseudo-random character.
 4. All addressable locations are verified in hardware using the Verify Sectors command to the disk.
- Deposit all storage media that cannot be overwritten, such as bad hard drives, which contain ePHI in a locked and secure location for later destruction. In order to ensure secure destruction of storage media that cannot be overwritten, CHP will contract with a vendor to perform these destruction services.
 - All individuals that work for CHP in any capacity are to store any portable media (for example flash drives, thumb drives, floppy diskettes, CDR/W discs, etc.) and portable devices (for example laptops and Blackberry handhelds) that contain ePHI in a locked drawer or cabinet when the individual is away from the storage media or devices.

Form(s):

Retired Assets Donation form

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

Revision History		
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