



COMMUNITY HEALTH PLAN
of Washington

Committed to your health.

Subject:	Media Re-Use Policy	Policy No:	PS104
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 implement procedures for removal and destruction of electronic protected health information (ePHI) from electronic media before the media are made available for re-use.

Scope:

This policy applies to Community Health Plan (CHP) in its entirety, including consultants, contractors, business associates and vendors. Further, the policy applies to all voice and data systems, network, and applications, as well as all facilities, which process, store or transmit ePHI.

Policy:

CHP will ensure the Configuration Management Database is appropriately updated upon the re-use of media components containing ePHI. This policy also applies to the following media:

- USB storage devices
- CD/R/RWs *
- DVDs *
- Floppy disks
- Zip disks
- Jazz drives
- Removable hard disk drives
- Internal hard disk drives
- External hard disk drives
- Tapes *
- Optical disks

* **These media types will not be re-used but will be destroyed by breaking or shredding. However computer tapes used for backing up data and voice systems tapes used for the voicemail system will be overwritten as needed, until such time as they become unusable in which case the tapes will be shredded.**

CHP will ensure that prior to re-using the media, it is securely overwritten and that such action is verified and documented.

CHP will ensure that the previous label on such media that is to be overwritten is removed and destroyed.

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 is responsible for ensuring the implementation of the requirements of the Media Re-use 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.

Media Re-use is a required implementation specification defined within the Device and Media Controls standard 164.310 (d)(1) in the Physical Safeguards category of the HIPAA Security Rule.

Procedure(s):

Procedures address the following media:

- USB storage devices
 - CD/R/RWs *
 - DVDs *
 - Floppy disks
 - Zip disks
 - Jazz drives
 - Removable hard disk drives
 - Internal hard disk drives
 - External hard disk drives
 - Tapes *
 - Optical disks
- * **These media types will not be re-used but will be destroyed by breaking or shredding. However computer tapes used for backing up data and voice systems tapes used for the voicemail system will be overwritten as needed, until such time as they become unusable in which case the tapes will be shredded.**

In regard to USB storage devices, floppy disks, zip disks, jazz drives, removable hard disk drives, internal hard disk drives, external hard disk drives and optical disks, the Desktop Support Analyst will do the following tasks before the storage media containing ePHI will be re-used by CHP or for non-CHP business use:

Re-Used by CHP

- All storage media will be reformatted except for hard disk drives
- Hard disk drives will be re-imaged using the following steps:
 1. The hard disk drive partitions and data will be deleted
 2. A basic set of data and application will be overwritten on to the hard disk drive
- Before re-use, the Configuration Management Database will be updated to reflect reassignment of devices that contain storage media or standalone storage media devices to another CHP employee.

Re-use For non-CHP business use

Per the Disposal Policy, the following steps will be taken when storage media is purchased or donated:

- 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/ise/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.
- Asset Control tags will be removed, destroyed and documented in the Configuration Management Database.
 - The Configuration Management Database will be updated to reflect that the storage media has been securely overwritten.
 - The Configuration Management Database will be updated to reflect that the device has been purchased by or donated to a person or organization for non-CHP business use.

Forms:

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

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