



Subject:	<b>Data Backup Plan</b>	Policy No:	PS102
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 establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI).

**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 voice systems, data systems, networks, applications, databases, and email systems that process, store or transmit ePHI.

**Policy:**

CHP will develop the capability to secure the receipt, transport, and removal of:

- Computer Equipment
- Software
- Electronic media, such as diskettes, tapes, CD/R/RWs, USB storage devices, DVDs, zip disks, Jazz drives, removable hard drives, internal hard drives and external hard drives

CHP will document the following:

- Who has control of the hardware/software/or electronic media at all times
- Accountability, the ability to ensure that the actions of an entity can be traced back to that specific entity
- Data backup
- Data storage
- Disposal
- Retrieval
- Archiving and Retrieval testing

In developing the backup schedule, the Security Officer will consider factors such as:

- What data (systems, files, directories, folders) should be backed up?
- How frequent are backups done?
- Who is responsible/authorized to retrieve the media?

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 implementing the requirements of the data backup plan.

**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.

The Data Backup Plan is a required implementation specification defined within the Contingency Plan standard (164.308 (a)(7)) in the Administrative Safeguards category of the HIPAA Security Rule.

**Procedures:**

The Network Analyst or other designated ITI team members are responsible for ensuring that data from Community Health Plan's Production, Development and Test servers are backed up.

The information from the servers is backed up as follows:

Day Of Week	Backup Type	Tapes/Rotation	Number of Tapes Needed
Monday	Differential	Monday tapes	1-2
Tuesday	Differential	Tuesday tapes	1-2
Wednesday	Differential	Wednesday tapes	1-2
Thursday	Differential	Thursday tapes	1-2
Friday	Differential	Friday tapes	1-2
Saturday	Full	Rotate through 3 sets	9-15
1st Saturday following the last business day of the month.	Full	Archive 11 months	22 - 33
Annual – 1st Saturday following the last business day of the year.	Full	Archive 7 years	3-6 each year

- Computer backup tapes are physically transferred to Iron Mountain once per week on Monday or the next business day if Monday is a holiday. Please refer to the backup schedule found at: <T:\MIS\Documentation\Backups\ Backups-03-08-05 - Draft.doc>. **Note:** The frequency of physical transfer of computer tapes may increase to once per day, as recommended in the Business Continuity Plan.

**File Restoration**

- ITI restores files on an as-needed basis. Users should send an email to Computer Help with the complete path of the file (e.g. T:\Med Mgmt\RestoreMe.doc) and the date they would like a file restored from.
- ITI will first attempt to restore a file using the Undelete computer application. Restoring a file in this manner requires 1 business day or less.
- If using Undelete is unsuccessful, ITI will retrieve the computer tape containing the file from Iron Mountain. However, there is a fee associated with tape retrieval. The department requesting file restoration is responsible to pay the tape retrieval fee. Files can be restored within 2 business days using this method.
- Once ITI completed the restoration, they will inform the user.

**Companywide Restoration**

- Those who are authorized to request backup computer tapes from Iron Mountain and their associated security levels are included in the matrix below:

User Name	Interaction Authority	Disaster Authority Level	Last Verification or Update
Linda Blankenship	A, B, C, D, E	4	1/27/05
Brett Jones	A, B, C, D, E	1, 2, 3, 4	2/28/05
Dexter Colbert	A, B, C, D		12/29/04
Justis McLaren	A, B, C, D, E	4	1/27/05
CHP Receptionist	A, B		12/15/04
<p><b>Interaction Authority:</b>  <i>Authorization levels are mutually exclusive. A user may have a combination of letters. Combination like A, B, E, for example are acceptable.</i>  <b>A</b> May release media for off-site vaulting; may not request return of media.  <b>B</b> May receive media when returned from off-site vaulting; may request the return of media.  <b>C</b> May visit an Iron Mountain facility; may not request the return of media.  <b>D</b> May request the return of media during a declared emergency; may request the return of media, including standard special or critical special requests.  <b>E</b> May create and modify other user accounts, including security privileges.  <b>R</b> Receive only - cannot request media. May search for requests and media items.</p>			
<p><b>Disaster Recovery Authorization Levels:</b>  <i>Authorization levels are mutually exclusive. A user may have a combination of numbers. Combinations like 1, 2, 3, for example, are acceptable.</i>  <b>1</b> Confirm media to include Disaster Recovery  <b>2</b> Revise Disaster Recovery Plans  <b>3</b> Declare a Disaster Recovery  <b>4</b> Revise Disaster Recovery authorization</p>			

- The receptionists are authorized to receive computer backup tapes from Iron Mountain.
- Please refer to the (Disaster Recovery Plan or Business Continuity Plan) for companywide computer systems infrastructure restoration procedures.

**Backup and Retrieval Testing**

- ITI will test archival and retrieval processes on a quarterly basis to ensure timely response to business requirements.

**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