


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

| APPROVED | RESPONSIBILITY | EFFECTIVE DATE | NUMBER | PAGE |
|---|---|----------------|---------|--------|
|  | Information Technology Administrator (HIPAA Security Officer) | 12/2004 | 6420-24 | 1 of 2 |
| TITLE: DATA BACKUP PLAN POLICY | | | | |

PURPOSE:

The purpose is to establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI). This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit ePHI.

POLICY:

Guam Memorial Hospital Authority will develop the capability to secure the receipt, transport, and removal of:

- Hardware
- Software and
- And electronic media, such as diskettes, tapes, optical platters, CD-ROMs, Zip Discs, and Flash Drives

Guam Memorial Hospital Authority 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
- Data and System Recovery
- Disposal

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

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

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

In addition, the HIPAA Security Officer will ensure that plans and procedures are in place for:

- Retention and Recycling of Backup Media for System and Data backup utilizing Grandfather, Father, Son concept.
- High Availability System that Mirrors the Hospital's Production System and Data to the backup system has seamless switch over procedures that will minimize user and system downtime.
- Testing of Retention and Recycling, and Switch over to High Availability System are performed regularly.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be 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 per the Sanction Policy 6420-8. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

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:

Procedures related to the Data Backup Plan standard include:

- Contingency Plan Procedure
- Disaster Recovery Procedure
- Emergency Mode Operations Procedure
- Testing and Revision Procedures

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.
- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.
- International Standards Organization (ISO/IEC 17799:2000(E)).