


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-26	1 of 3
TITLE: EMERGENCY MODE OPERATION PLAN POLICY				

PURPOSE:

The purpose is to establish and implement as needed procedures to enable continuation of critical business processes for protection of the security of electronic protected health information (ePHI) while operating in an emergency mode. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

An emergency mode operation plan is the part of an overall contingency plan that contains a process enabling Guam Memorial Hospital Authority to continue to operate in the event of fire, vandalism, natural disaster, or system failure. In a manner similar to disaster recovery planning, budget for and schedule required resources for effective emergency mode operation plan testing.

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:

During an emergency event, the Guam Memorial Hospital Authority's business function information systems must continue to operate to support the business processes and to maintain the security and integrity of ePHI. The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for ensuring that this policy is carried out during the duration of the emergency.

The HIPAA Security Officer must consider identifying the levels of emergencies and associated responses. This may be based on the magnitude of the incident or disaster. The three levels of emergency are:

- **Level 1 Emergency** may relate to a loss of business function system or a specific part of a location/site.
- **Level 2 Emergency** may be based on an incident impacting multiple business functions systems or multiple locations/sites.
- **Level 3 Emergency** may be based on a significant disruption to several business functions systems or substantial damage at one or more locations/sites.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

During an actual emergency mode event, when the Hospital calls and implements its Emergency Operations Center also known as the Command Post, the Information Technology (IT) Department will initiate its role and respond appropriately in accordance with the Disaster Plan and this policy.

The HIPAA Security Officer will follow through to ensure that these specific components of this emergency mode operation plan are in place:

- Recall of essential Information Technology Staff for the emergency.
- Setup of required computer equipment at the Command Post was completed in a timely manner.
- Proper assignment of IT staff to monitor key business systems and provide technical support during the emergency.
- Data Backup Plan and Disaster Recovery Plan are reviewed and initiated (if needed).
- Assessment of any damaged or malfunctioning computer equipment are documented during the emergency and presented to management for emergency replacement procurement.
- Procedures and checklists to provide for the orderly transition and restoration of normal business systems operations (e.g., moving from the impacted site to the alternate site).
- Coordination and setup of available critical facilities and computer equipment for alternate processing and business workspace for continuing operations in the event of an emergency (if needed).
- Communication with key hardware and software support contractors for external support (if needed).
- Procedures to ensure that health and safety issues during the emergency are addressed.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for implementing the requirements of the Emergency Mode Operation 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.

Emergency Mode Operation 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 Emergency Mode Operation Plan standard include:

- Contingency Plan
- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operations Plan
- 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)).