


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-25	1 of 6
TITLE: DISASTER RECOVERY PLAN POLICY				

PURPOSE:

The purpose is to establish and implement a plan to restore and recovery of any loss of Systems and Data, most especially electronic Protected Health Information (ePHI), from a disaster or catastrophe. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

The disaster recovery plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. A disaster recovery plan refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.

A disaster recovery plan provides a blueprint to continue business systems operations in the event that a catastrophe occurs. The disaster recovery plan must include contingencies for the period of time of the disaster and until the recovery plan can be completely implemented. The price for not developing a disaster recovery plan is that the Guam Memorial Hospital Authority may find it difficult to continue to be in business or potentially suffer a significant loss.

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 assign final responsibility of security to one individual who will be referred to as the "HIPAA Security Officer". The HIPAA Security Officer is to ensure the development of a Disaster Recovery Plan document.

The major objective of this policy is to define procedures for recovery of the Hospital business systems and disruption of computer and/or network services from a catastrophic disaster as delineated in the Contingency Plan Policy 6420-23. This disruption may come from total destruction of the main hospital campus or from minor disruptive incidents. There is a great deal of similarity in the procedures to deal with the different types of incidents affecting different areas supported by Information Technology Department. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the hospital, including providing support to departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

All major computing systems that are vital for the daily operation of the hospital and under the stewardship of Information Technology Department are maintained under service contracts with the equipment and software support contractors. This ensures that routine maintenance problems will be addressed in a timely way with adequate resources. These contracts range from telephone support, remote access support to full hardware replacement.

This plan is limited to the computing support given to departments from the Information Technology department, including systems under the stewardship of Information Systems. Individual departments should develop their own plan to deal with manual operations within their departments should computer and/or network services be disrupted.

ASSUMPTIONS:

This section contains some general assumptions, but does not include all special situations that can occur. Senior Information Technology staff members on site will make any special decisions for situations not covered in this plan needed at the time of an incident and will coordinate efforts with the HIPAA Security Officer.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first on site following an incident will contact the HIPAA Security Officer for a determination of the need to declare an incident. The Hospital Administrator/CEO, the Associate Administrator of Operations, and the Chief Financial Officer overseeing the Information Technology department will also be notified.

The senior Information Technology staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have resulted or may occur as a result of the incident, immediate attention will be given to those persons injured. The Guam Memorial Hospital Authority Facilities Maintenance Department will be notified if necessary. If the situation allows, attention will be focused on shutting down systems, turning off power, etc., but evacuation to ensure health and safety is the highest priority.

Once an incident that is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper hospital authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable computer and/or remote access and telephone support to the hospital has been re-established.

INCIDENTS REQUIRING ACTION:

The disaster recovery plan will be invoked under one of the following circumstances:

- An incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of 24 hours.
- An incident that has impaired the use of computers and/or networks managed by Information Technology department due to circumstances that fall beyond the normal processing of day-to-day operations. This includes all systems that the Guam Memorial Hospital Authority considers to be mission critical. These systems include:

- AS/400 Primary and Backup Systems
- Network Infrastructure

- Keane Patient Accounting, Clinical, Financial and Operations Applications
- Cerner-DHT Laboratory Information System
- Hospital Enterprise Exchange Servers
- Connect Imaging Radiology PACS Imaging System
- 3M Coding and Reimbursement System
- Computermart EMC and EMR Electronic Billing System
- Internet and Email access system

- * An incident, which was caused by problems with computers and/or networks, managed by Information Technology department and has resulted in the injury of one or more persons.

CONTINGENCIES:

General situations that can destroy or interrupt computer and telephone services usually occur under the following major categories:

- * Power Interruption
- * Fire
- * Water/Flooding
- * Weather and Natural Phenomenon
- * Sabotage and Interdiction

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

- * Partial recovery - operating at an alternate site on campus and/or off campus at the Skilled Nursing Facility.
- * Full recovery - operating at the current central site or at the Skilled Nursing Facility, possibly with a degraded level of service for a period of time.

DISASTER RECOVERY TEAM:

In case of a disaster, the emergency recall list will be used to contact and notify the Disaster Recovery Team. Recovery team leaders have been assigned in each major area and general duties given. The team leaders will activate the teams and make assignment of personnel in the major areas to specific tasks during the recovery stage over that area.

Organization of the Disaster Recovery Team:

Recovery Management Team:

Manager, Information Technology - Team Leader
HIPAA Security Officer - Alternate
Systems Operations Supervisor - Disaster Recovery Coordinator

Command Center Recovery Team (if needed):

Hospital Administrator/CEO - Team Leader
Associate Administrator of Operations - Alternate
Chief Financial Officer – Recovery Coordinator with Recovery Team
HIM and Business Office staff as necessary

Computer Operations Recovery Team:

System Operations Supervisor - Team Leader
Systems Analyst/Administrator - Alternate
Computer Operations staff as necessary
Applications Analysts as necessary

Damage Assessment and Restoration Team:

Senior Network Communications Analyst - Team Leader
Network Communications Analyst - Alternate

Functions of the Disaster Recovery Team:

Recovery Management Team

The Recovery Management Team is responsible for providing leadership for the Information Technology group, including review, modification, and implementation of the pre-planned recovery strategies. These responsibilities include overseeing the processing of critical hospital information systems at alternate processing facilities until the restoration of normal processing at the restored, renovated or new production facility. To support recovery operations, a Command Center will be established in the Hospital Boardroom in accordance with existing Disaster Policies and Procedures.

While processing of critical applications is being performed at the alternate processing facility, another alternate processing facility such as the Skilled Nursing Facility or other designated hospital space or off-site cold site will be set up to enable the Recovery Management Team to acquire replacement mainframe hardware and other servers in a "grow fast" recovery strategy. The services of hardware support contractor IBM and other software support vendors will be needed to repair or replace damaged systems.

Command Center Recovery Team

If needed, the Command Center will be activated only in the event a disaster has occurred, resulting in a decision by the Hospital Administrator/CEO and his Management staff to initiate the Disaster Recovery Plan. The Command Center will be activated in the Hospital Boardroom and will provide centralized and coordinated management and control of all communications during disaster recovery. When a disaster is declared, and during subsequent recovery operations, all disaster teams and other hospital personnel will be in continuous contact with the Command Center. All Teams will report their status to the Command Center to permit the Command Center Recovery Team Leader to allocate the existing and externally available resources.

It is expected that the Skilled Nursing Facility in Barrigada Heights or other available non affected areas within the Hospital will be used as an alternate processing location at time of disaster to provide access to critical applications. The Command Center Recovery Team will maintain contact between the Command Center and the remote processing location.

Computer Operations Recovery Team

The Computer Operations Recovery Team will be activated only in the event a disaster has occurred, resulting in a decision by the Hospital Administrator/CEO and his Management staff to initiate the Disaster Recovery Plan. The responsibility of the Computer Operations area is

to continue providing and overseeing processing of all production applications, printing reports and ensuring data and on-line access is available to the end users. The most critical computer applications will be restored at the alternate processing facility as soon as humanly and logistically possible. Help desk support will be re-established at the Command Center immediately thereafter. Most other functions will subsequently be resumed within three to ten days or sooner if resources permit.

Once the new or repaired permanent production system becomes available, the Computer Operations Recovery Team will take the necessary actions to make final backups of the systems being recovered at the alternate processing facility, clear applications from the recovery equipment, transport the final backups to the production location, and restore the data files to the new production equipment. Then bring as much end users back online with the resources available.

Damage Assessment and Restoration Team

The Damage Assessment and Restoration Team will be activated only in the event a disaster has occurred, resulting in a decision by the Hospital Administrator/CEO and his Management staff to initiate the Disaster Recovery Plan. The responsibility of the Damage Assessment and Restoration Team is to assess the damage and manage the restoration of the affected site in a timely manner, following a Hospital Computer Systems disaster that results in a disruption of service. This team will also be responsible for reestablishing designated network servers within 24-48 hours at an alternate processing facility, such as the Skilled Nursing Facility or other designated area.

The Damage Assessment and Restoration Team will perform recovery tasks that either return processing capabilities to the affected site after repairs have been completed, a temporary processing facility while repairs are being made, or to a new production processing facility. The Damage Assessment & Restoration Team Leader will work with the Command Center and Facilities Maintenance during recovery operations, and damage assessment and restoration activities, as directed.

RETURN TO NORMAL OPERATIONS:

Upon completion of restoration of facilities and systems and full recovery of all data affected by the Disaster, to include the secured computer center, mainframe systems, the Return to Normal Operations will include all users having access to their authorized applications and systems and all of the business functions systems running at full production level, they are:

- AS/400 Primary and Backup Systems
- Network Infrastructure
- Keane Patient Accounting, Clinical, Financial and Operations Applications
- Cerner-DHT Laboratory Information System
- Hospital Enterprise Exchange Servers
- Connect Imaging Radiology PACS Imaging System
- 3M Coding and Reimbursement System
- Computermart EMC and EMR Electronic Billing System
- Internet and Email access system

DISASTER RECOVERY TESTING:

An important element of the disaster recovery program is to confirm the ability of the Hospital's Information technology staff and external support areas to recover these primary systems at remote locations within the projected timeframes established by the plan. Without a proactive program in place, you will never know your realistic recovery capabilities. Although it is possible to have a locally trained technical staff with the capabilities of setting up the recovery systems should a disaster occur, when a disaster occurs, it is not known which staff members would be available to support the recovery operations. The most effective use of financial resources is to only pay for this capability when it is actually required.

Hot-site testing is typically performed once or twice a year. In addition to this testing, it is typical to conduct a readiness review of the Information Technology staff. The results of the testing and readiness reviews are used to confirm the ability of Information Technology department to respond to an emergency as well as providing information for updating the disaster recovery plan and the disaster recovery program itself.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for implementing the requirements of the Disaster Recovery Plan.

The Teams identified in this Disaster Recovery Plan Policy, under the delegated authority of the Hospital Administrator, will be responsible for initiating this plan upon the call of a business systems disaster.

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.

Disaster Recovery 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.

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)).