


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-21	1 of 4
TITLE: SECURITY INCIDENT PROCEDURES POLICY				

PURPOSE:

The purpose is to address security incidents. Guam Memorial Hospital Authority will create processes for the identification, reporting, and ensuring a timely response to real or potential violations of the security or a material breach of any part of Guam Memorial Hospital Authority's security policy. 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. In addition, some third parties such as contractors or vendors, may be required to abide by parts of this policy if required by Guam Memorial Hospital Authority in a Business Associate Contract (BAC).

POLICY:

Guam Memorial Hospital Authority will maintain procedures for identifying security incidents. Incidents will be classified as "serious" or "non-serious." Non-serious incidents generally have the following characteristics:

- It is determined that there was no malicious intent (or the attack was not directed specifically at Guam Memorial Hospital Authority associated with the incident and
 - It is determined that no sensitive information, especially electronic protected health information (ePHI), was used, disclosed, or damaged in an unauthorized manner
- Serious incidents generally have the following characteristics:
- It is determined that there was malicious intent and/or an attack was directed specifically at Guam Memorial Hospital Authority
 - It is determined that sensitive information, especially ePHI, may have been used, disclosed, or damaged in an unauthorized manner

All workforce members of Guam Memorial Hospital Authority will report any security incident to the Security Officer that they become aware of or suspect. A security incident is any breach of security policy, or any activity that could potentially put sensitive information, especially ePHI, at risk of unauthorized use, disclosure, or modification.

Guam Memorial Hospital Authority will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.

Reviewed: 01/2006
Revised: 02/2006
Approved: EMC 2/15/06

Incidents characterized as serious by the HIPAA Security Officer will be responded to immediately and reported to all upper-level management.

Guam Memorial Hospital Authority will attempt to mitigate any harmful effects, when possible, where a security incident affects customer or patient information.

The Guam Memorial Hospital Authority will develop security policies to identify core activities in the area of Response and Reporting implementation specification of the HIPAA Security Rule.

RESPONSIBILITIES:

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents
- Reporting any suspected security incident to the HIPAA Security Officer by using the attached Security Incident Report Form
- Assisting the HIPAA Security Officer in ending the security breach and mitigating its harmful effects, if possible

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for:

- Maintaining all security incident-related policies and procedures
- Characterizing all reported security incidents as “serious” or “non-serious” as per the guidelines outlined above. The HIPAA Security Officer may take into account their professional expertise and experiences when making these characterizations
- Maintaining procedures for responding to security incidents
- Documenting all reported security incidents and their outcome by using the attached Security Incident Report Form

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, and other members of management are jointly responsible for:

- Mitigating, to the extent possible, any harmful effects of security incidents
- Deciding when it is appropriate to contact law enforcement officials about a security incident that has been characterized as serious

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for leading compliance activities that bring the Guam Memorial Hospital Authority into compliance with the HIPAA Security Rule implementation specifications of:

- Response and Reporting

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.

Security Incident Procedures is a standard (164.308 (a)(6)) defined in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures related to the Security Incident Procedures Policy include:

- Security Incident Report Form (attached) Documentation Procedure
- Information System Activity Review Procedure
- Response and Reporting

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)).

GUAM MEMORIAL HOSPITAL AUTHORITY HIPAA SECURITY

Incident Report Form

(Please Mark [X] appropriate box)

[] Patient [] M.D. [] Other Date submitted: _____
[] Visitor [] Staff/Employee

Name: _____ Telephone #: _____
(Person reporting incident)

Department: _____ Other Dept. Involved: _____

Date of incident: _____ Time of incident: _____

Location of Incident: _____

Circle item(s) affected by incident: | AS/400 | PC | Terminal | Laptop | Printer | Monitor |
Keyboard | Mouse | External Drive | Flash Drive | UPS | Internet Access | Email | Server |
Switch | Hub | Router | Firewall | Wireless Access-Point | Scanner | Xerox Work-Centre |
Digital Camera | Multi-Media Projector | File(s) | Record(s) | Password | Video Conferencing
Equipment | Conference Pod | Access Smart Key | Door Security Lock | Other _____ |

Nature/Description of the incident: _____

Below for HIPAA Security Officer - MIS Department Use Only

Assessment/Findings of Incident:

Assessment done by: _____ Date: _____

Corrective Action Taken:

Signature: _____ Date: _____

HIPAA Security Officer