


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-9	1 of 2
TITLE: INFORMATION SYSTEM ACTIVITY REVIEW POLICY				

PURPOSE:

The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. 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 systems that process electronic Protected Health Information (ePHI).

POLICY:

Guam Memorial Hospital Authority will clearly identify all critical systems that process ePHI. Guam Memorial Hospital Authority will implement security procedures to regularly review the records of information system activity on all such critical systems that process ePHI.

The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:

- User IDs
- Dates and times of log-on and log-off
- Terminal identity, IP address and/or location, if possible
- Records of successful and rejected system access attempts

Safeguards must be deployed to protect against unauthorized changes and operational problems including:

- The logging facility being deactivated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself

Reviewed: 01/2006
Revised: 02/2006

Approved: EMC 2/15/06

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will clearly identify:

- The systems that must be reviewed
- The information on these systems that must be reviewed
- The types of access reports that are to be generated
- The security incident tracking reports that are to be generated to analyze security violations
- The individual(s) responsible for reviewing all logs and reports

When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

PROCEDURES:

Procedure(s) related to Information System Activity Review include:

- Security Incident Procedures

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.

Sanction Policy is a required implementation specification defined within the Security Management Process standard (164.308 (a) (1)) 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)).