


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-48	1 of 2
TITLE: AUDIT CONTROL POLICY				

PURPOSE:

The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI). This is a standard required under the Technical Safeguards of the HIPAA Security Rule.

Audits may be conducted to:

- Ensure confidentiality, integrity, and availability of ePHI
- Investigate possible security incidents and ensure conformance to Guam Memorial Hospital Authority security policies
- Monitor user or system activity where/when appropriate

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, as well as all facilities, which process, store or transmit ePHI.

POLICY:

Guam Memorial Hospital Authority will identify critical systems that require event auditing capabilities. Guam Memorial Hospital Authority will define the events to be audited on all such systems. At a minimal, event auditing capabilities will be enabled on all systems that process, transmit, and/or store ePHI. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions, and modifications.

Guam Memorial Hospital Authority will ensure the protection of all audit reports and log files.

The Guam Memorial Hospital Authority will review the usage of software and application tools to review audit files.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of Guam Memorial Hospital Authority's security team.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, or stored on Guam Memorial Hospital Authority's equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, and so on)
- Access to interactively monitor and log traffic on Guam Memorial Hospital Authority's networks

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for ensuring the implementation of the Audit Controls standard.

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.

Audit Controls is a standard (164.312 (b)) defined in the Technical 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)).