


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-20	1 of 2
TITLE: LOG-IN MONITORING POLICY				

PURPOSE:

The purpose is to implement procedures for monitoring log-in attempts and reporting discrepancies. 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. Further, the policy applies to all systems, network, and applications that process, store or transmit electronic protected health information (ePHI).

POLICY:

Guam Memorial Hospital Authority will configure all critical components that process, store or transmit ePHI to record log-in attempts – both successful and unsuccessful – as well as automatic lock out and reporting after 3 failed attempts.

The security awareness training must include information about the importance of monitoring log-in success or failure. Further, the information must address the steps for checking last log-in information.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for ensuring the implementation of the Log-in Monitoring Policy. The HIPAA Security Officer must identify all critical systems that will record log-in attempts – both successes and failures. The HIPAA Security Officer will ensure the monitoring of logs that record such information by authorized individuals on a regular basis.

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.

Log-in Monitoring is an addressable implementation specification defined within the Security Awareness and Training standard (164.308 (a)(5)) in the Administrative Safeguards category of the HIPAA Security Rule.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

PROCEDURES:

Procedures related to the Log-In Monitoring Procedure includes:

- Information System Activity Review Procedure
- Information Access Management Procedure

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)).