


**GUAM MEMORIAL HOSPITAL AUTHORITY  
ADMINISTRATIVE MANUAL**

<b>APPROVED</b>	<b>RESPONSIBILITY</b>	<b>EFFECTIVE DATE</b>	<b>NUMBER</b>	<b>PAGE</b>
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-46	1 of 2
<b>TITLE: AUTOMATIC LOGOFF POLICY</b>				

**PURPOSE:**

The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity and/or non-usage. This is a standard required under the Technical 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, as well as all facilities, which process, store or transmit electronic protected health information (ePHI).

**POLICY:**

Guam Memorial Hospital Authority will maintain procedures for Automatic Logoff of systems that contain sensitive information, such as ePHI, after a period of inactivity. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located.

Guam Memorial Hospital Authority will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.

**RESPONSIBILITIES:**

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for ensuring the implementation of the Automatic Logoff Policy.

**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.

Automatic Logoff is an addressable implementation specification defined within the Access Control standard (164.312 (a)(1)) in the Technical Safeguards category of the HIPAA Security Rule.

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

**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)).