


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-14	1 of 2
TITLE: TERMINATION PROCEDURE POLICY				

PURPOSE:

The purpose is to implement procedures for terminating access to electronic protected health information (ePHI) when the employment of a workforce member ends. 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.

POLICY:

People are the greatest threat to the security of any organization. It is thus important that any termination of a workforce member immediately results in both the Human Resources (HR) and the Information Technology (IT) departments coordinating their activities to ensure:

- Password access is immediately revoked
- Access to all systems and applications is revoked
- The workforce member is removed from any systems or applications that processed ePHI
- All digital certificates are revoked
- Any tokens or smart cards issued to the workforce member are returned
- Any keys and IDs provided to the workforce member during their employment are returned
- The workforce member is not provided any access to their desk or office – any such access, if provided, must be limited and carefully supervised

HR must conduct an exit interview and document any issues or concerns related to the workforce member and HR must ensure that terminating employee(s) are routed through to the IT department for clear out notification.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for ensuring that all activities identified in this Termination Procedure document are followed through and implemented.

Termination Procedure is an addressable implementation specification defined within the Workforce Security standard (164.308 (a)(3)) in the Administrative Safeguards category of the HIPAA Security Rule.

Reviewed: 01/2006

Revised: 02/2006

Approved:

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.

PROCEDURES:

HR will have employee processed out using clear-out form. Upon sign-off by IT, the IT designate will remove all systems and data access for terminated employee upon completion of the last day of employment.

Procedures related to the Termination Procedure include:

- Workforce Security Procedure
- Workforce Clearance Procedure
- Password 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)).