


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-60	1 of 2
TITLE: VPN SECURITY POLICY				

PURPOSE:

The purpose of this policy is to implement security measures sufficient to reduce the risks and vulnerabilities of the Guam Memorial Hospital Authority's Virtual Private Network (VPN) infrastructure to a reasonable and appropriate level. This is a required standard of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all facilities and systems that process sensitive information.

POLICY:

The Guam Memorial Hospital Authority VPN infrastructure must follow these guidelines:

- Members of the workforce with VPN privileges must ensure that unauthorized users are not allowed access to Guam Memorial Hospital Authority's internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a strong password solution.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic must be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set up and managed by Guam Memorial Hospital Authority's network operational groups.
- All computers connected to Guam Memorial Hospital Authority's internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
- VPN users are automatically disconnected from Guam Memorial Hospital Authority's network after fifteen minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Users of computers that are not Guam Memorial Hospital Authority-owned equipment must configure the equipment to comply with Guam Memorial Hospital Authority's VPN and other policies.
- Only approved VPN clients may be used.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Guam Memorial Hospital Authority's network, and as such are subject to the same rules and regulations that apply to Guam Memorial Hospital Authority-owned equipment; in other words, their machines must be configured to comply with the Guam Memorial Hospital Authority's Security Policies.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, has the responsibility to ensure that all VPN end systems such as laptops and desktops, are deployed and used based on policy requirements. The HIPAA Security Officer or his/her team must review log files from VPN devices such as concentrators and other systems on a regular basis. The HIPAA Security Officer must send reminders to all employees about VPN security.

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.

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)).