


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-61	1 of 2
TITLE: REMOTE ACCESS 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 with regard to remote access to the Hospital Network and/or Systems that contain electronic protected health information (ePHI). 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. Remote Access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, Web Portal, and cable modems.

POLICY:

The Guam Memorial Hospital Authority remote access infrastructure must follow these guidelines:

- It is the responsibility of Guam Memorial Hospital Authority employees, contractors, vendors and agents with remote access privileges to Guam Memorial Hospital Authority's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Guam Memorial Hospital Authority.
- General access to the Internet for recreational use by immediate household members through the Guam Memorial Hospital Authority network on personal computers is permitted for employees that have flat-rate services. The Guam Memorial Hospital Authority employee is responsible to ensure the family member does not violate any Guam Memorial Hospital Authority policies, does not perform illegal activities, and does not use the access for outside business interests. The Guam Memorial Hospital Authority employee bears responsibility for the consequences should the access be misused.
- Secure remote access must be strictly controlled. Control will be enforced by using strong passwords.
- At no time should any Guam Memorial Hospital Authority employee provide their login or e-mail password to anyone, not even family members.
- Guam Memorial Hospital Authority employees and contractors with remote access privileges must ensure that their Guam Memorial Hospital Authority-owned or personal computer or workstation, which is remotely connected to Guam Memorial Hospital Authority's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

- Guam Memorial Hospital Authority employees and contractors with remote access privileges to Guam Memorial Hospital Authority's corporate network must not use non-Guam Memorial Hospital Authority e-mail accounts (for example, Hotmail, Yahoo, AOL), or other external resources to conduct Guam Memorial Hospital Authority business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the Guam Memorial Hospital Authority network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Remote Access Services, and the Security Officer must approve security configurations for access to hardware.
- All hosts that are connected to Guam Memorial Hospital Authority internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the Guam Memorial Hospital Authority production network must obtain prior approval from the Security Officer.

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, has the responsibility to ensure that all remote access connections are used based on policy requirements. The Security Officer must review related log files from key systems on a regular basis. The Security Officer must send reminders to all employees about remote access 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)).