


**GUAM MEMORIAL HOSPITAL AUTHORITY  
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-62	1 of 2
<b>TITLE: DIAL IN ACCESS POLICY</b>				

**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 Dial In or Dial Up Access 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 dial-in access infrastructure must be based on these guidelines:

- Guam Memorial Hospital Authority employees and authorized third parties (customers and vendors) can use dial-in connections to gain access to the enterprise network. Dial-in access should be strictly controlled, using strong password authentication.
- It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to Guam Memorial Hospital Authority is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and Guam Memorial Hospital Authority are extensions of Guam Memorial Hospital Authority's enterprise network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect Guam Memorial Hospital Authority's assets.
- Analog and non-GSM digital cellular phones cannot be used to connect to Guam Memorial Hospital Authority's enterprise network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to Guam Memorial Hospital Authority's network.

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

### **RESPONSIBILITIES:**

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, has the responsibility to ensure that all dial-in connections are used based on policy requirements. Account activity must be monitored, and if a dial-in account is not used for a period of six months the account must expire and no longer function. If dial-in access is subsequently required, the individual must request a new account.

### **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)).