


**GUAM MEMORIAL HOSPITAL AUTHORITY
ADMINISTRATIVE MANUAL**

APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-59	1 of 2
TITLE: WIRELESS SECURITY POLICY				

PURPOSE:

The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the Guam Memorial Hospital Authority's wireless 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 wireless infrastructure must follow these guidelines:

Design

- Configure a firewall between the wireless network and the wired infrastructure.
- Ensure that 128-bit or higher encryption is used for all wireless communication.
- Fully test and deploy software patches and updates on a regular basis.
- Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

Access Points (AP)

- Maintain and update an inventory of all Access Points (AP) and wireless devices.
- AP should be installed within the Hospital as appropriate.
- Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- The default settings on APs, such as those for SSIDs, must be changed.
- APs must be restored to the latest security settings when the reset functions are used.
- Ensure that all APs have strong administrative passwords.
- Enable user authentication mechanisms for the management interfaces of the AP.
- Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
- Turn on audit capabilities on AP; review log files on a regular basis.

Mobile Systems

- Install anti-virus software on all wireless clients.
- Install personal firewall software on all wireless clients.
- Disable file sharing between wireless clients.

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 wireless end systems such as laptops and PDAs, as well as all APs are deployed based on policy requirements. The HIPAA Security Officer must review log files from APs and other systems on a regular basis. The HIPAA Security Officer must send reminders to all employees about wireless network 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)).