


**GUAM MEMORIAL HOSPITAL AUTHORITY  
ADMINISTRATIVE MANUAL**

<b>APPROVED</b>	<b>RESPONSIBILITY</b>	<b>EFFECTIVE DATE</b>	<b>NUMBER</b>	<b>PAGE</b>
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-63	1 of 4
<b>TITLE: INTERNET AND EMAIL ACCESS</b>				

**PURPOSE:**

This procedure describes the standards and process for granting access to the Internet and Email for authorized users at Guam Memorial Hospital Authority. This is a required standard of the HIPAA Security Rule.

To provide access to Internet and Email resources and to insure that authorized users effectively use these resources, while protecting Guam Memorial Hospital Authority from inappropriate resource use, security risks and legal liability.

**SCOPE:**

Guam Memorial Hospital Authority and all authorized Internet and Email users.

**POLICY:**

Internet and email access will be granted to authorize users for the purpose of conducting appropriate Hospital business. Use of the Internet and email by employees and authorized non-employees with access to Guam Memorial Hospital Authority's information systems is permitted and encouraged in cases where such use is both suitable for business purposes and supports the goals and objectives of the Hospital. In such cases, the Internet and email access is to be used in a manner that is consistent with standards of business conduct and as part of the normal execution of a user's job functions.

Internet and email access is for official business use and not for personal use. Personal Internet and email activities are strictly prohibited.

**PROCEDURE:**

**Requesting for Internet and Email Access:**

Requests for an Internet and Email access must be made using the attached Internet and Email Access Request Form. The request form has to be completed by both the requesting user and the Department Head or Supervisor. Incomplete or unsigned forms will be returned to requestor and request will not be processed by the Information Technology Department. Upon approval of request, the requestor will be notified and provided with their registered Account and Password.

Reviewed: 01/2006

Revised: 02/2006

Approved: EMC 2/15/06

### **Standards of Business Conduct:**

Use of computers and networks is subject to monitoring by HIS and an audit record of user activity will be kept and reviewed for proper Internet and Email usage. This includes the URLs of Web sites visited.

Hospital confidentiality policies and Federal and State laws govern any information from the computer systems. The information from the Hospital's computer systems is to be kept strictly confidential and not to be shared with persons, except for legitimate, job related duties.

### **Appropriate Internet and Email Usage Guideline:**

- Searching for information that supports and promotes Hospital business.
- Participating in professional business related organizations.
- Conducting business related educational or research projects.
- Communicating with business associates and professionals.

### **Inappropriate Internet and Email Usage Guidelines:**

- Revealing or publicizing proprietary or confidential information, including patient information.
- Accessing or downloading pornographic, sexually explicit or offensive material to the corporate network or to their PCs.
- Conducting illegal activities, including online gaming and gambling.
- Soliciting for personal gain or profit.
- Misrepresenting the Hospital with personal opinions.
- Posting to newsgroups or sending email with indecent or inappropriate remarks, which may be embarrassing to the organization.
- Uploading or downloading commercial software in violation of its copyright.
- Downloading any software or electronic files without reasonable virus protection measures in place.
- Intentionally interfering with the normal operation of any Internet gateway.
- Attempting to gain illegal or unauthorized access to any systems on the Internet.
- Unauthorized Telnet access to remote Internet sites.
- Downloading screen savers from the Internet. Only desktop/screensaver(s) available with Windows program(s) installed by the Information Technology department are appropriate to use on Hospital computers.
- Using instant messaging software such as but not limited to AOL, Yahoo and MSN.
- Using unauthorized software to monitor real-time streaming data such as financial (stock) information.
- Downloading or Uploading Streaming Video, Music, Ringtones.

### **Information Security:**

Hospital or patient confidential, classified, or proprietary information **will not** be transmitted over the Internet without prior management approval and reasonable security measures in place.

Any messages sent over the Internet, including personal email messages, are not considered secure unless additional measures are taken to protect such information (e.g., encryption). Users should communicate via email as they would in a public meeting (e.g., if you are not comfortable saying something to a room full of people, it should not be said via Email).

Contacts made over the Internet must never be trusted with information unless a due diligence process has first been performed.

### **Reporting Security Problems:**

Each user has the responsibility to notify Information Technology Department immediately of any evidence of any security violation involving Internet connectivity and assist in filling out incident report.

### **Public Representations:**

Internet users may not indicate their affiliation with Guam Memorial Hospital in newsgroup discussions, chat sessions, or other places on the Internet. Only the Hospital Administrator or his/her designee may speak about or produce a news release announcement. All external representations on behalf of the Hospital must first be cleared with management.

### **RESPONSIBILITIES:**

All individuals identified in the scope of this policy are responsible for:

- Abide by the terms and guidelines set forth by this policy

The Guam Memorial Hospital Authority HIPAA Security Officer, under the delegated authority of the Hospital Administrator, is responsible for:

- Evaluate, on a periodic basis, emerging encryption solutions for email and implementing them when one is found that meets the criteria described in the policy section of this document
- Maintaining procedures and forms in support of this policy
- Monitoring and enforcing workforce compliance with this policy

### **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)).

**GUAM MEMORIAL HOSPITAL AUTHORITY  
INFORMATION TECHNOLOGY DEPARTMENT  
INTERNET AND EMAIL ACCESS REQUEST FORM**

**GENERAL INFORMATION: (Check one)**    Employee    Non-Employee    Physician

Employee Name: \_\_\_\_\_ Employee Social Security #: \_\_\_\_\_

Non-Employee Name: \_\_\_\_\_ Non-Employee Social Security # \_\_\_\_\_

Physician Name: \_\_\_\_\_ Physician #: \_\_\_\_\_

Department Name: \_\_\_\_\_ Telephone Number: \_\_\_\_\_

**Check One:**    Internet Access Only    Email Access Only    Both Internet & Email Access

Justification/Need: \_\_\_\_\_  
\_\_\_\_\_

*By signing this form I agree to abide by the Internet and Email Access Policy 6420-63.*

Employee's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Non Employee's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Physician's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Requesting Department Approval Section:**

Department Head Name: \_\_\_\_\_ Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Please return this form to:**  
GMHA Information Systems Department Help Desk

**SECTION BELOW TO BE COMPLETED BY INFORMATION TECHNOLOGY PERSONNEL:**

Request received by: \_\_\_\_\_ Date request received: \_\_\_\_\_

**Information Technology Department Approval Section:**

Department Head Name: Vince Quichocho Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Email Account/Address: \_\_\_\_\_ **@gmha.org** Email Password: \_\_\_\_\_

Email Account set up by: \_\_\_\_\_ Date: \_\_\_\_\_

Email Profile setup at User's PC by: \_\_\_\_\_ Date: \_\_\_\_\_

User Notified by: \_\_\_\_\_ Date: \_\_\_\_\_