Guadalupe Regional MEDICAL CENTER	**Approved Date:**	08/08/20129/06/2013	Page **1** of **5**
	Last Reviewed Date:	09/06/2013	
	Originating Date:	09/01/2004	
Subject: **Network and HCIS Usage - GRMC Employees**	**Originating Position:**	Compliance	
Category: Policies, Procedures	**Rationale:**	45 CFR 164.308	

PURPOSE:

The purpose of this policy is to implement certain aspects of Guadalupe Regional Medical Center's (GRMC) Privacy and Security Policy as it relates to Employee access to GRMC's Computer Network and Healthcare Information System (Meditech), Centricity, Allscripts, etc.

APPLICATION:

All employees who currently and potentially will access GRMC's Computer Network for any purpose, i.e. Internet Access, Meditech, etc., are affected by this policy.

POLICY:

It is GRMC's policy to ensure the integrity, security, and appropriate use of its computer network, information systems, e-mail systems, and data. Users are expected to be familiar with and to comply with this Network Usage Policy and any updates or revisions thereof. Users are also expected to comply with the hospital's Confidentiality/HIPAA Guidelines and exercise good judgment while using the Network.

A. Introduction:

This Usage Policy covers the usage of the Internet using GRMC resources, GRMC Intranet, Virtual Private Network (VPN) access, HCIS(Meditech), other patient care software, and all other uses of GRMC's network (collectively, the "Network").

1. Violations of this Usage Policy will be investigated and documented and can lead to immediate revocation of Network privileges and/or disciplinary action up to and including termination of employment or contractual relationship with GRMC, as applicable, in addition to other legal means that may be available for damages incurred as a result of any violation of this Usage Policy. GRMC reserves the right to seek action in a court of law to immediately bar a User from the use or benefit of GRMC's facilities or resources. GRMC may also be required by law to report certain illegal activities to the proper enforcement agencies.

2. Any exceptions or variances to the provisions of this policy must be approved by GRMC Administration.

B. GRMC's Monitoring of User Content:

The Network is a critical component of GRMC's communication and information gathering process. Network access is granted to Users only to facilitate the performance of GRMC related business and patient care. The contents and history of a user's network session, including VPN access and activity are, therefore, the sole and exclusive property of GRMC. While GRMC does not assume any obligation to regularly monitor and log a user's network activity, it may access, monitor, log, review and disclose, as it deems necessary, in its sole discretion, all content created or received by a user including but not limited to, a user's Meditech access, web browsing, instant messaging, E-mail, and application activity for any purpose to any party. GRMC may also disclose the content of a user's network activity to law enforcement officials and appropriate GRMC Management /Administration without prior notice to or consent of a user. As a result, a user should not expect any content a user creates or receives to be private and, by signing the attached acknowledgement form, a user thereby waives any privacy or confidentiality or similar rights to anything a user creates or receives on or via the network.

C. Responsible use of GRMC's Network:

1. A User is required to:
   a) when using GRMC computer systems, including Network access or VPN access, do so only for the benefit of GRMC, its affiliates, and patient care;
   b) maintain the privacy and confidentiality of all confidential and institutional data, including but not limited to patient related data;
   c) understand that when documenting in Meditech, every medical record entry is dated and the author identified by the user ID. The user's Meditech user ID is his/her electronic signature and by signing the Acknowledgement Form for the GRMC Network Usage Policy he/she is assuring that they alone will use their user ID and password.
   d) maintain responsibility for all activities having occurred through the use of User's Meditech User-ID and password, Network User-ID and password or other assigned User-ID and password;
   e) be responsible for the security of any hospital system User ID and password;
   f) log out of all computer systems, including VPN access and Meditech when leaving a workstation unattended for an extended period of time;
   g) report security violations immediately to the GRMC HIPAA Privacy & Security Officer – Debby Hernandez.
   h) comply with all third-party software license requirements.

2. Without the prior authorization of the GRMC IT Department, a User may not do any of the following:
   a) copy GRMC software for use on a User's home computer;
   b) provide copies of GRMC software to any independent contractors or consultants of GRMC or to any third person without the approval of GRMC legal counsel;
   c) download or install software (including screen savers and games) on the Network, other than updates to standard desktop software;
   d) modify, revise, reprogram, or adapt any software unless it is within the scope of the both the software license and the User's job;
   e) reverse engineer, disassemble, or de-compile any software on or from the Network; nor
   f) alter copyrighted works in such a way as to change, obscure, or remove information relating to the copyright owner, copyright notice information, the author of the work, the terms and conditions of use of the work, or identifying numbers or symbols referring to the foregoing information or links to such information.

D. Chat Groups, Listserves, and Newsgroups:

Internet Chat Groups, Listserves, and Newsgroups are public forums where it is inappropriate to discuss or reveal confidential information, patient-related data, trade secrets, and any other material proprietary to GRMC and its affiliates or received in confidence by or on behalf of GRMC. Only those Users who have been duly authorized by GRMC may speak/write in the name of the Hospital when making postings to listserves or newsgroups. Users shall identify themselves honestly, accurately, and completely when participating in listserves, news groups, and when setting up accounts on outside computer systems. Other Users may participate in listserves and newsgroups, provided (1) participation will assist them in the performance of their jobs, and (2) the following footer is included on all postings or comments: ***"This posting reflects the individual views and opinions of the author and does not necessarily represent the views and opinions of GRMC."*** Users should understand that each of their postings will leave an "audit trail" indicating at least the identity of GRMC' s Internet servers, and most likely, a direct trail to the User. Inappropriate postings may damage GRMC's reputation and could result in business or individual liabilities. Accordingly, Users must make every effort to be professional in making comments online.

E. E-mail:

The Network's e-mail system is not intended to replace or supplement the existing procedures relating to storage or management of official business communications or copies thereof. A User who is granted e-mail privileges on the Network is expected to regularly delete or archive e-mail and attachments from the User's mailbox after they are finished with them. If a User receives or creates a document using the Network's e-mail system and that document is important to GRMC, then the User shall store the document to a folder or file located on a server on the Network, but should not store it in the User's inbox or other e-mail folders unless these folders reside on a server that is backed up on a regular basis.

1. A User shall not:
   a) forward an e-mail or e-mail attachment generated within GRMC to an address outside the Network without the consent of the author or originator, unless the content of such email is clearly public in nature, or it is reasonable to believe that the author would not object and is included in the "cc" field of such transmittal; nor
   b) Send messages outside of GRMC which contain any Individually Identifiable Health Information, either in the body of the message or as an attachment to the message, unless
      i. approved by the Facility Privacy Official and
      ii. approved encryption methods have been used to secure the message contents.

2. There are a variety of free e-mail services available on the internet. As e-mails and e-mail attachments are a leading source of viruses getting onto the network, it is GRMC's policy that access to these free e-mail services from GRMC's network will be blocked whenever possible. GRMC is not responsible for storage or management of any official business communications or copies thereof made through these e-mail services.

F. Disclaimer of Liability for Internet Use:

1. While GRMC may use certain technologies to block inappropriate email or websites, nevertheless, GRMC cannot be held responsible for material viewed or downloaded by users from the internet. The internet is a world-wide network of computers that contains millions of pages of information often posted by unknown individuals. Users are cautioned that many of the pages may include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some incidental contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the internet may lead to the receipt of unsolicited e-mail containing offensive content. Users accessing the internet do so at their own risk.

2. This Policy is not intended to, and does not grant, the User any contractual rights.

3. If a User is unsure of any of the above requirements, or is otherwise unable to comply with any of the requirement of this Usage Policy, a User should contact the IT Management for assistance with any questions.

PROCEDURE:
It is the responsibilities of the Compliance/HIPAA Officer and the Information Technology Department for ensuring practical methods are implemented for carrying out tasks associated with meeting the intent of this Usage Policy. At a minimum each department will adhere to the following:

A. Policy Distribution:

1. Users who are GRMC employees or volunteers and whose job description requires access and/or use the Network will be given a copy of this policy by the Human Resources Department.
    a) Each user must sign the Acknowledgement Form prior to being granted Network privileges.
    b) The originally signed Acknowledgment Form must be stored in the GRMC Human Resources Department.
    c) Prior to granting Network privileges, the HIPAA Privacy Officer must verify that the User has signed the Acknowledgment Form.

B. Facility Employees and Volunteers:

1. To maintain and continue their Authorized Access, facility employee Users and volunteer Users are required to comply with this Network Usage Policy, the GRMC Confidentiality/HIPAA Guidelines, and to do each of the following:
    a) Attend GRMC Orientation including HIPAA Privacy and Security Education.
    b) Each user must sign the Acknowledgement Form prior to being granted Network privileges.
    c) Receive periodic security awareness education.

2. The initial and subsequent annual security awareness education can be part of a new-hire orientation program, a review process, safety education, or other process that ensures that all Users participate.

Exhibit A

Acknowledgment Form to Comply With GRMC's Network Usage Policy – Employees

I hereby certify that I have received, read and will comply with Guadalupe Regional Medical Center's Network Usage Policy and the GRMC Confidentiality/HIPAA Privacy Guidelines.

I acknowledge that I am responsible for my possession and use of any GRMC's informational resources and must actively protect these informational resources from unauthorized disclosure, modification, deletion, and usage.

I hereby agree, as a condition of continued access to the Network (defined in Section **"Policy"** of the Network Usage Policy) to abide by the policies and procedures described in GRMC's Network Usage Policy and GRMC's Confidentiality/HIPAA Privacy Guidelines. I understand that access to the Network is a privilege, which may be changed or revoked at any time at the sole discretion of GRMC.

I also agree to promptly report all violations or suspected violations of the Usage Policy to the GRMC Compliance/HIPAA Officer or the Information Technology Department.

I acknowledge that GRMC may need to change or update the Network Usage Policy and its Confidentiality/HIPAA Privacy Guidelines from time to time. I will comply with all revisions to the Network Usage Policy and the Confidentiality/HIPAA Privacy Guidelines.

I understand that when I document in Meditech, every medical record entry is dated and the author identified by my user ID. I further understand that my Meditech user ID is my electronic signature and by signing this Acknowledgement Form for the GRMC Network Usage Policy I am assuring that I alone will use my user ID and password.

I understand that if I am unsure of any of the elements of the Network Usage Policy of the GRMC Confidentiality/HIPAA Privacy Guidelines, or if I subsequently learn that I am otherwise unable to comply with certain requirements, I should contact the GRMC Compliance/HIPAA Officer or the Information Technology Department for assistance with any questions I may have. **I have read and understand the Network Usage Policy, the GRMC Confidentiality/HIPAA Privacy Guidelines, and this Acknowledgement Form and hereby agree to fully comply with them.**

Signature of User____ **Date** ________________

(Must be signed by all facility employees and volunteers as required in the Usage Policy)

Print Name of User ____

Title/Job Description ____

Department Name ____