Guadalupe Regional MEDICAL CENTER

Approved Date:	04/01/2013		
Last Reviewed Date:	04/01/2013		
Originating Date:	04/01/2005		
Subject:	**NETWORK & HCIS USAGE – PHYSICIAN**	**Originating Position:**	Information Technology
Category:	Federal Regulations, HIPAA	**Rationale:**	45 CFR 164.308

PURPOSE:
The purpose of this policy is to implement certain aspects of Guadalupe Regional Medical Center (GRMC) Privacy and Security Policy as it relates to any entity needing access to GRMC's Computer Network and Healthcare Information System (Meditech).

APPLICATION:
The following entities are principally affected by the policy elements.

- All physicians who currently and potentially will access GRMC's Computer Network for any purpose, ie, Internet Access, Meditech Access.
- All physician's office staff who will access GRMC's Computer Network for any purpose, ie, Meditech Access.

POLICY:
It is GRMC's policy to ensure the integrity and security and appropriate use of its computer network, information 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 (attached) and exercise good judgment while using the Network.

A. Introduction

This Usage Policy covers the use of the Internet (using GRMC resources), Intranet, virtual private network (VPN) access, HCIS (Meditech), and all other uses of GRMC's Network.

1. Violations of this Usage Policy will be investigated and documented and can lead to immediate revocation of Network privileges, in addition to other legal remedies available for damages incurred as a result of any violation of this Usage Policy. GRMC reserves the right to seek injunctive relief 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's 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 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, 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. maintain responsibility for all activities having occurred through the use of User's Meditech User-ID and password and Network User-ID and password;
   d. be responsible for the security of User ID and password;
   e. log out of all computer systems, including VPN access and Meditech when leaving a workstation unattended for an extended period of time;
   f. report security violations immediately to Guadalupe Regional's HIPAA Privacy & Security Officer – Debby Hernandez.
   g. 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, transform, recast, 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. E-mail

There are a variety of free e-mail services available on the internet. These must be used responsibly as e-mails and e-mail attachments are a leading source of viruses getting onto the network. GRMC is not responsible for storage or management of any official business communications or copies thereof made through these email services.

E. Disclaimer of Liability for Internet Use

Although GRMC may use certain technologies to block inappropriate email or websites, GRMC cannot be held responsible for material viewed or downloaded by users from the internet. The internet is a worldwide 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 email containing offensive content, users accessing the internet do so at their own risk.

PROCEDURE:

It is the responsibility of the IT Department and Compliance/HIPAA Officer to ensure practical methods are implemented for carrying out tasks associated with meeting the intent of this Usage Policy. At a minimum medical staff and medical office staff will adhere to the following:

1. Each physician member of the facility medical who wishes to have network privileges is required to sign a Memorandum of Understanding (MOU), which is attached hereto as Exhibit A. The MOU incorporates all of the terms of this Usage Policy. The MOU must be signed before minimally necessary network privileges are granted. The Guadalupe Regional Administration must approve the MOU. Prior to granting network privileges, the IT Department must verify that the MOU has been signed. Proof of verification must be maintained by Guadalupe Regional in auditable format.
2. To have continued Authorized Access, the foregoing users are required to bi-annually re-sign the MOU; this re-signing can be part of the bi-annual-credentialing process or other process that ensures that the MOU is resigned at least once every 24 months.
3. When revisions are made to this Usage Policy, Medical Staff will be provided with a copy of the current version of this Usage Policy.
4. The foregoing MOU signatories (Physicians) may request and sponsor Guadalupe Regional-related, minimally necessary network privileges for their office staff by completing the attached Medical Office Network Access request Form, which is attached hereto as Exhibit B.
    a. Such MOU signatories (Physicians) are required to immediately notify the Guadalupe Regional Information Technology Department or the Compliance/HIPAA Officer (who will then notify Administration) of any terminated, sponsored personnel having network Privileges
    b. The sponsoring physician must approve the request
    c. The original signed copy of Exhibit B must be stored at Guadalupe Regional in auditable format

Exhibit A

Memorandum of Understanding (MOU)
Network Access Request - Physician

The undersigned responsible person (hereinafter referred to as **"you"** or **"your"**) wishes to have access to and use of the undersigned Guadalupe Regional Medical Center's (**"GRMC"**) network, which may include, as applicable, Intranet, Extranet, HCIS (Meditech), or VPN access, desktops and laptops (the **"Network"**). By granting you such access, you may be able to view or copy confidential or privileged patient-related information that is electronically stored and made available to health care professionals

As a condition of receiving access to the Network, you agree as follows:

1. Information that you seek through the Network shall be limited solely to that of patients who are being cared for by both you and GRMC.

2. You shall limit your use of the information obtained from the Network (the **"Information"**) solely to providing health care services to the patient to whom it relates or the services you are contracted for. Where specifically permitted by GRMC, you and your business associate, as defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), may also use the Information for obtaining payment for your services and for certain health care operations as permitted under HIPAA. You shall not use the Information for any other purpose nor disclose Information relating to a particular patient to any third party without the written authorization of said patient.

3. You agree to undertake a reasonable degree of care to protect the Information considering its confidential and privileged nature, which care shall not, in any event, be less than that required by law and by GRMC's Network Usage Policy, a copy of which is attached.

4. You have read and understand GRMC's Network Usage Policy, and agree that, in addition to the requirements herein, the Network Usage Policy also governs your access to and use of the Network. Any revisions to the Network Usage Policy, which may be necessary from time to time, will be readily available to you.

5. Your Network user ID and password is unique to you and at no time shall you share with or otherwise disclose either of them to any other individual in your office or elsewhere. You agree to immediately report to GRMC the disclosure or loss of your user ID or password.

6. You have read and understand GRMC’s Confidentiality / HIPAA Privacy Guidelines and agree to follow said guidelines in the hospital’s commitment toward ensuring the privacy and security of confidential data, including but not limited to, protected health information (PHI).

7. You acknowledge that any violation of this Memorandum of Understanding could result in irreparable harm, the damages for which are incalculable. You agree that in the case of such breach of the foregoing agreement and trust, the patient, and GRMC shall have every remedy available at law, including immediate injunctive relief.

8. For the purpose of GRMC's compliance with HIPAA, and security and integrity of the Network and the information therein, GRMC will electronically monitor, record and audit your Network activity. Nevertheless, you should not and cannot rely on such monitoring, recording, or auditing to electronically prohibit inappropriate use of your user ID or password by either you or another individual.

ACCEPTED AND AGREED TO:

I acknowledge I have read and understand this Memorandum of Understanding (Exhibit A), GRMC's Network Usage Policy and GRMC's Confidentiality/HIPAA Guidelines and agree to be bound by their requirements.

Print Physician's Name:

_____

Signature: _____

Date: _____

Office Address:

Street: _____

City: _____

Telephone: _____

GRMC HIPAA Officer Signature

Signature: _____

Date: _____

Exhibit B

Memorandum of Understanding
Network Access Request – Allied Health Professional (AHP)/Office Personnel Under Physician Supervision

The undersigned responsible person has previously signed a Memorandum of Understanding for Network access and now wishes to request and sponsor access to and use of the undersigned Guadalupe Regional Medical Center's (**"GRMC"**) network for his or her office staff (including business associates) identified below, which persons hereinafter are referred to as **"you"** or **"your"**). Such access or use will be limited to VPN Access to GRMC's Network for the purpose of accessing GRMC's HCIS (Meditech) (the **"Network"**). By granting you such access, you may be able to view or copy confidential or privileged patient-related information that is electronically stored and made available to health care professionals.

As a condition of receiving access to the Network, you agree as follows:

1. Information that you seek through the Network shall be limited solely to patients who are being cared for by your supervising physician.

2. You shall limit your use of the information obtained from the Network (the **"Information"**) solely to providing health care services to the patient to whom it relates or the services contracted for. Where specifically permitted by GRMC and as directed and approved by your supervising physician you may also use the Information for obtaining payment for your services and for certain health care operations as permitted in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). You shall not use the Information for any other purpose nor disclose Information relating to a particular patient to any third party without the written authorization of said patient.

3. You agree to undertake a reasonable degree of care to protect the Information considering its confidential and privileged nature, which care shall not, in any event, be less than that required by law and by GRMC's Network Usage Policy, a copy of which is attached.

4. You have read and understand GRMC's Network Usage Policy, and agree that, in addition to the requirements herein, the Network Usage Policy also governs your access to and use of the Network. Any revisions to the Network Usage Policy, which may be necessary from time to time, will be readily available to you.

5. Your Network user ID and password is unique to you and at no time shall you share with or otherwise disclose either of them to any other individual in your office or elsewhere. You agree to immediately report to GRMC the disclosure or loss of your user ID or password.

6. You have read and understand GRMC's Confidentiality / HIPAA Privacy Guidelines and agree to follow said guidelines in the hospital's commitment toward ensuring the privacy and security of confidential data, including but not limited to, protected health information (PHI).

7. You acknowledge that any violation of this Memorandum of Understanding could result in irreparable harm, the damages for which are incalculable. You agree that in the case of such breach of the foregoing agreement and trust, the patient, and GRMC shall have every remedy available at law, including immediate injunctive relief.

8. For the purposes of GRMC's compliance with HIPAA, and security and integrity of the Network and the information therein, GRMC will electronically monitor, record and audit your Network activity. Nevertheless, you should not and cannot rely on such monitoring, recording, or auditing to electronically prohibit inappropriate use of your user ID or password by either you or another individual.

Exhibit B -- Memorandum of Understanding (cont'd)
Network Access Request – Allied Health Professional (AHP)/Office Personnel
Under Physician Supervision

ACCEPTED AND AGREED TO:

I acknowledge I have read and understand this Memorandum of Understanding (Exhibit B), GRMC's Network Usage Policy and GRMC's Confidentiality/HIPAA Guidelines and agree to be bound by their requirements.

Print Name of AHP/Office Personnel:	Signature, AHP/Office Personnel

By signing below, I agree to sponsor necessary access and usage of the Network by the member of my office staff identified below and shall be responsible for their supervision to ensure their compliance with this Memorandum of Understanding, GRMC's Network Usage Policy, and GRMC's Confidentiality/HIPAA Guidelines. I also agree to immediately notify the GRMC's Information Technology Department or Compliance/HIPAA Officer once the above individual is terminated or no longer needs Network access.

Physician Information:

_____
Physician's Name (Printed)

_____
Physician's Signature

_____
Date

Guadalupe Regional Medical Center:

_____
HIPAA Officer's Signature

_____
Date

Guadalupe Regional
MEDICAL CENTER

Confidentiality / HIPAA Privacy Guidelines

Guadalupe Regional Medical Center is committed to ensuring the privacy and security of confidential data, including but not limited to, protected health information (PHI). Protected Health Information is generally defined as any information that can be used to identify a patient – whether living or deceased and which relates to the patient's past, present, or future medical condition.

To support this commitment, individuals accessing the hospital's network and information systems are expected to follow these guidelines:

- ACCESS health information only when necessary to perform your job-related duties and responsibilities.
- MAINTAIN the privacy and confidentiality of all confidential data, including but not limited, to patient related information.
- BE RESPONSIBLE for securing your User ID and password. Do not share this information or authorize anyone to use your User ID and password.
- LOG OFF computer systems with access to patient information when station is left unattended.
- DO NOT access health information about co-workers or family members unless necessary for job-related functions.
- DO NOT access your own health information. This is against hospital policy.
- DO NOT share patient information with those who are not authorized to know.
- DO NOT send PHI in emails without appropriate encryption.
- DO NOT discuss PHI in public areas.
- NOTIFY the hospital of staffing changes impacting network usage. An individual who no longer works for you must have network privileges removed.
- REPORT security violations of hospital network and information systems to Debby Hernandez, Privacy/Security Officer, at (830) 401-7100.

The hospital electronically monitors, records, and audits individual Network usage activity to help prohibit inappropriate use. Violations of GRMC's network usage agreement, guidelines, and policies, result in a breach of the network agreement. This in turn may result in changes in assigned network privileges and subjects the user to any remedy as per law and regulation.