

## GRANDE RONDE HOSPITAL

<b>Department: INFORMATION TECHNOLOGY</b>	<b>No. 6.10.46</b>
<b>Procedure for: REMOTE ACCESS POLICY</b>	

### **HIPAA SCOPE**

§164.312.a.1, §164.312.d, §164.308.a.6, §164.312.a.1.ii.A

### **PURPOSE**

To establish policies and procedures to manage remote access to Grande Ronde Hospital's (GRH's) various information systems and ensure GRH's electronic assets, including patient and financial information, are appropriately protected. Remote access via Virtual Private Network (VPN) will be granted based on need, assessed on a case-by-case basis.

### **POLICY**

GRH wishes to promote offsite and telecommuting access for those jobs and employees suitable for this type of work option. GRH also supports remote access for its Medical Staff, Information Technology (IT) vendors, Contractors, and other authorized users, as necessary, to support the IT systems and provide an integrated delivery network for our patients and their families. This policy describes the terms and conditions under which remote service may be used. All use of remote access must comply with local, state, and federal laws. Remote access is a privilege, not a right.

Telework arrangements requiring remote access to IT resources are powerful tools if implemented correctly. While offering potential benefits, remote access to IT resources introduces new risks to the security of GRH information and systems as well as to the privacy of the patients GRH serves. For example, without appropriate safeguards to protect the integrity of the electronic functions and remote processes, the following security issues could occur:

- Confidential information could be unintentionally disclosed
- Sensitive data could be altered or deleted
- Malicious software could be introduced to the user and/or GRH equipment
- Systems sign-on identifications and passwords could be intercepted and reused to access systems and data files without authorizations

Thus, taking the time to identify, implement and use appropriate safeguards is required if GRH is to protect the confidentiality, integrity and availability of the electronic processes during remote access. IT security practices are essential prerequisites to facilitating telework and other remote access work arrangements. It is the responsibility of GRH employees, physicians, vendors, contractors, and other authorized agents with remote access privileges, to ensure that their remote connection is given the same consideration as the user's on-site connection to GRH's IT systems.

### **REMOTE ACCESS SUPPORT**

Grande Ronde Hospital IT Department does not provide in-house hardware or software support for non-GRH owned equipment at remote sites, except as required by contracts.

- For GRH provided hardware, hardware repairs can be accomplished by returning the unit back to GRH for repair via appropriate contract vendor
- Employee owned hardware/software will not be serviced or repaired by GRH. GRH shall be held harmless for any hardware damage, software corruption or data loss on employee owned computers. Problems related to Internet Service Provider (ISP)

connection or ISP hardware should, in all cases, be directed to the ISP provider. Typically, ISP will charge for repair services.

- Problems with GRH provided software shall be directed to the GRH IT Department Helpdesk at extension 1410. [ NOTE: *Business hours are 7:00 AM to 5:00 PM, Monday through Sunday. GRH IT Department does not provide after hours support for remote access users, except as required by contract.*]
- Remote Access using dial-up modem (standard telephone lines) access over the Internet to the GRH network is not supported.

## **REMOTE ACCESS APPLICATIONS**

The GRH IT department provides the following levels of access to various users:

- Line staff can be limited to Outlook Web Access (OWA) for e-mail, calendar, contacts and tasks.
- Managers will be limited to OWA and access to standard software applications (such as Office, Time & Attendance, Intranet and IT prerequisite software, etc.) and network drives for file access via a Windows Terminal Server (WTS).
- Executives will be limited to OWA, WTS and direct Remote Desktop access to their own desktop computers and all applications running on them.
- Members of the Medical Staff and designated office staff of independent physician offices will be given access to the Health Information System (HIS), the Picture Archiving and Communication System (PACS), and other clinical systems as deemed appropriate.

GRH does not provide remote access to any non-standard or departmental or third party applications.

## **PROCEDURES**

### **A. GRH Workforce:**

- a. Executives, managers, and supervisors need to contact IT to have their account activated for remote access. There is no form to fill out. However, every user of the GRH remote access service is urged to read all related policies, which are listed in the “References” section of this policy.
- b. Access for non-exempt employees or other GRH workforce members will require justification based on the employee’s need for remote access. [NOTE: *Non-exempt employees requesting remote access, must have their supervisor fill out the “Information Access Request” form and check “OWA Via AAA” and turn it into IT. If authorized for remote access, non-exempt employees must follow all state and federal employment regulations as well as the GRH Personnel Policy.*]
- c. Failure to comply with the Remote Access Policy may result in withdrawal of permission to have the Offsite Access/Telecommuting privileges. [NOTE: *Please also refer to the Personnel Policy Manual section pertaining to Remote Internet Access.*]
- d. Confidentiality of information: Employees who have Offsite/Telecommuter Access are held to the same standard for protecting confidentiality of information as are employees working from traditional offices. It is the telecommuter’s responsibility to ensure appropriate measures are taken (e.g. shredding of printer documents or documents placed on portable devices such as CD or Diskettes) to ensure confidentiality.

- e. Security Incidents: It is the responsibility of the employee to notify the IT Department if they feel that their user security or system has been compromised or if patient information has been released inappropriately.
- f. Recreational use of any GRH remote access is strictly prohibited.
- B. Non-GRH Workforce, including Vendors:
  - a. Obtain a signed “Confidentiality of Information” form from each individual requesting access to the GRH IT Network. [*NOTE: Existing vendors, such as McKesson, will be grandfathered and not required to sign individual Confidentiality of Information Forms.*]
  - b. If the requestor is not a Medical Staff Physician or member of their practice staff, verify with the Compliance Office that a current Business Associate and/or Network Use Agreement have been signed. If not, the Business Associate Agreement with IT Access must be signed prior to consideration of remote access. Independent physicians and their office staff must fill out the “Remote Access User Request” form attached to this policy and turn it into the GRH IT Department.
  - c. Vendor access to GRH information systems is limited to systems within their application databases only, via VPN.
  - d. Attempts to access systems outside the external user’s knowledge will be considered and handled as a breach of security.
  - e. External users shall not engage in any network monitoring or management activities without prior knowledge and written permission of the Information Security Officer.
  - f. External users shall promptly terminate unneeded remote access accounts/services, by notifying the GRH IT Department.
  - g. External Users must agree to adhere to all GRH policies for appropriate and secure use of GRH resources.

**REFERENCES**

- GRH Personnel Policy Manual
- Information Security Handbook

<b>EFFECTIVE DATE: 03/20/08</b>	<b>REVIEW DATE:</b>
<b>SIGNED:</b>  President/CEO	<b>REVISED DATE:</b>  <b>01/30/09</b>
<b>SIGNED:</b>  Senior Director of Technology Services	

## REMOTE ACCESS USER REQUEST

I am requesting that the following individual/organization be given access to the system specified below for the expressed purposes listed

**Vendor:** (Y/N) \_\_\_\_\_

Name/Organization: \_\_\_\_\_

Contact Phone: \_\_\_\_\_ E-mail Address: \_\_\_\_\_

**Requested Access:**

Please specify: \_\_\_\_\_

**Purpose for Access:**

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Requested Effective Date:** \_\_\_\_\_

**GRH Sponsor Signature:** \_\_\_\_\_

**APPROVAL**

IT Director: \_\_\_\_\_

Forward to GRH IT Helpdesk (Fax: 541-962-2508)

## GRH Independent Physician User Agreement for Access to Electronic Protected Health Information

\* Required fields

Physician's Name: (Last, First, Middle Initial)*		
Practice Name:*	Practice Address:*	Office Contact Person:*
Office Phone Number:*	Office Fax number:*	Email address:*

**Security Agreement:** I have carefully read the policies attached, and acknowledge that my signature affixed to this security agreement constitutes acceptance of the terms listed therein and an agreement to abide by them. I have carefully read the GRH Electronic Protected Health Information (EPHI) Guidelines. I further understand that any violation of the terms of this agreement may result in civil or criminal penalties.

<i><b>Physician:</b> Please check the application(s) needed and sign below.</i>		
<input type="checkbox"/> Paragon WebStation for Physicians	<input type="checkbox"/> PACS	<input type="checkbox"/> Other _____
<b>I agree to the GRH's EPHI Guidelines.</b>		
Physician Signature	Date	

### GRH Electronic Protected Health Information Guidelines

All data resident within the many GRH's computer systems, including personal computers, intelligent workstations, networks, servers, and any storage media, are the sole property of GRH's and/or specifically designated partners and affiliates of GRH. Data pertaining to the daily operation of GRH entities or to its patients, but resident on privately owned personal systems, shall be considered to be data owned by GRH and, as such, is subject to the policies set forth in this and other relevant documents. The Information Technology Department is responsible for the implementation of data security. Audits will be performed at the department level to assure data integrity.

Permission to access GRH's Electronic Protected Health Information (EPHI) is given to users under the following conditions:

**Guidelines:**

- Permission to access GRH's network and data is granted for the purpose of gathering information and updating records only. Upon termination of the business relationship, the user agrees to relinquish any access privileges to the computer systems on GRH's network.
- Confidential EPHI includes, but is not limited to, medical records, appointment scheduling, clinical data, billing information, demographics and financial records.
- The user agrees that he/she will not disclose sensitive, confidential information or data, either specific or aggregate, which is owned, controlled or protected by GRH's without the express permission of the owner, steward or guardian of that information. Methods of disclosure may include, but are not limited to, data transfer or transmission, verbal or written disclosure, news release, and documents left in full or partial view including unattended, connected computer workstations.
- GRH's will actively monitor system usage and will terminate accounts that reflect abuse.
- Usernames and passwords are strictly confidential and may not be disclosed or shared by anyone.

- Failure to logoff from a workstation when your work is completed allows unauthorized system access by others. This is a direct violation of the GRH's security policies.
- Upon receipt of EPHI access, the undersigned acknowledges that the Username and password are **NON-TRANSFERABLE**. The user also agrees to abide by the policies and guidelines of this document.

*Return completed form to GRH Information Technology or the Physician Services Office*

## GRH Independent Physician Office Staff User Agreement for Access to Electronic Protected Health Information

\* Required fields

Physician's Name: (Last, First, Middle Initial)*		
GRH Network Username, if applicable:		Office Contact Person:*
Practice Name:*	Practice Address:*	
Office Phone Number:*	Office Fax number:*	Email address:*

**Security Agreement:**

My staff and I have carefully read the policies attached, and acknowledge that my signature affixed to this security agreement constitutes acceptance of the terms listed therein and an agreement to abide by them. My staff and I have carefully read the GRH Electronic Protected Health Information (EPHI) Guidelines. My staff and I further understand that any violation of the terms of this agreement may result in civil or criminal penalties. I assume the responsibility of enforcing the agreement with the hospital included here. I also further assume the responsibility of notifying the Information Technology Department of the Hospital of any discontinuation of employee-employer relationship of any of my staff below for whom I am requesting access.

<b>Physician:</b> Please countersign below to indicate your approval of the addition of your staff to GRH systems.	
I agree to the GRH EPHI Guidelines.	
Physician Signature	Date

<b>Office Staff 1:</b> Please check the application(s) needed and sign below.	
Employee Name:	Employee Title:
<input type="checkbox"/> Paragon WebStation for Physicians <input type="checkbox"/> PACS <input type="checkbox"/> Other: _____	
I agree to the GRH EPHI Guidelines.	
User Signature	Date

## GRH Independent Physician Office Staff User Agreement for Access to Electronic Protected Health Information

**Office Staff 2:** Please check the application(s) needed and sign below.

Employee Name: \_\_\_\_\_ Employee Title: \_\_\_\_\_

Paragon WebStation for Physicians       PACS       Other: \_\_\_\_\_

**I agree to the GRH EPHI Guidelines.**

User Signature \_\_\_\_\_ Date \_\_\_\_\_

**Office Staff 3:** Please check the application(s) needed and sign below.

Employee Name: \_\_\_\_\_ Employee Title: \_\_\_\_\_

Paragon WebStation for Physicians       PACS       Other: \_\_\_\_\_

**I agree to the GRH EPHI Guidelines.**

User Signature \_\_\_\_\_ Date \_\_\_\_\_

**Office Staff 4:** Please check the application(s) needed and sign below.

Employee Name: \_\_\_\_\_ Employee Title: \_\_\_\_\_

Paragon WebStation for Physicians       PACS       Other: \_\_\_\_\_

**I agree to the GRH EPHI Guidelines.**

User Signature \_\_\_\_\_ Date \_\_\_\_\_

## GRH Independent Physician Office Staff User Agreement for Access to Electronic Protected Health Information

<b>Office Staff 5:</b> Please check the application(s) needed and sign below.	
Employee Name:	Employee Title:
<input type="checkbox"/> Paragon WebStation for Physicians <input type="checkbox"/> PACS <input type="checkbox"/> Other: _____	
<b>I agree to the GRH EPHI Guidelines.</b>	
User Signature	Date

<b>Office Staff 6:</b> Please check the application(s) needed and sign below.	
Employee Name:	Employee Title:
<input type="checkbox"/> Paragon WebStation for Physicians <input type="checkbox"/> PACS <input type="checkbox"/> Other: _____	
<b>I agree to the GRH EPHI Guidelines.</b>	
User Signature	Date

# GRH Independent Physician Office Staff User Agreement for Access to Electronic Protected Health Information

## GRH Electronic Protected Health Information Guidelines

All data resident within the many GRH computer systems, including personal computers, intelligent workstations, networks, servers, and any storage media, are the sole property of GRH and/or specifically designated partners and affiliates of GRH. Data pertaining to the daily operation of GRH entities or to its patients, but resident on privately owned personal systems, shall be considered to be data owned by GRH and, as such, is subject to the policies set forth in this and other relevant documents. The Information Technology Department is responsible for the implementation of data security. Audits will be performed at the department level to assure data integrity.

Permission to access GRH Electronic Protected Health Information (EPHI) is given to users under the following conditions:

### Guidelines:

- Permission to access GRH network and data is granted for the purpose of gathering information and updating records only. Upon termination of the business relationship, the user agrees to relinquish any access privileges to the computer systems on GRH network.
- Confidential EPHI includes, but is not limited to, medical records, appointment scheduling, clinical data, billing information, demographics and financial records.
- The user agrees that he/she will not disclose sensitive, confidential information or data, either specific or aggregate, which is owned, controlled or protected by GRH without the express permission of the owner, steward or guardian of that information. Methods of disclosure may include, but are not limited to, data transfer or transmission, verbal or written disclosure, news release, and documents left in full or partial view including unattended, connected computer workstations.
- GRH will actively monitor system usage and will terminate accounts that reflect abuse.
- Usernames and passwords are strictly confidential and will not be disclosed or shared by anyone.
- Failure to logoff from a workstation when your work is completed allows unauthorized system access by others. This is a direct violation of the GRH security policy.
- Upon receipt of EPHI access, the undersigned acknowledges that the Username and password are **NON-TRANSFERABLE**. The user also agrees to abide by the policies and guidelines of this document.

*Return completed form to GRH Information Technology or the Physician Services Office*