GUADALUPE REGIONAL MEDICAL CENTER
NETWORK ACCESS AGREEMENT

Guadalupe Regional Medical Center (GRMC) and its affiliates, including Guadalupe Regional Medical Group (GRMG) may offer access to their respective Computer Information System/ Electronic Health Record ("Network") to employees, business associates, physicians, and other individuals, collectively referred to as "User".

Information sought through the Network shall be limited to:

- Patients who are served by either GRMC/GRMG and the User; and/or
- Information as it relates to the service the User provides to GRMC or its affiliates

Users granted access to the Network are responsible for complying with the following standards:

1. **Agreement Responsibility.** User agrees to read and adhere to GRMC's Confidentiality/HIPAA Privacy Guidelines and Network Access Agreement while utilizing the Network.

2. **Acceptable Use Standard.** User agrees to access and use the Network only as necessary to perform User's job related duties and responsibilities; and in a manner consistent with the services the User is contracted to perform. User will not access their personal health information on the Network. User will not access health information regarding their co-workers or family members unless required for their job related functions.

3. **Protection of Confidential Information.** User agrees to protect the confidentiality and integrity of electronic patient health information, sensitive information, and/or confidential information obtained while using the Network. User will not share patient information with unauthorized individuals.

4. **Passwords.** User agrees to follow guidelines for the creation and safeguarding of passwords. User will **NOT** share passwords, codes, credentials, or user accounts with others. User will **NOT** use another User's credentials to access the Network.

5. **Appropriate Safeguards.** User agrees to take proper steps to ensure the security and integrity of the Network while connected.
    - User agrees not to copy information accessed from the Network to local devices or portable devices (i.e. thumb drives).
    - Printing information is not permitted unless necessary for your responsibility and/or as indicated by Contract or Service Agreement.
    - User will log off Network when leaving his/her workstation.
    - User will comply with any third party software license requirements.
    - User will not download or install software on the Network, other than updates to standard desktop software.
    - User will make sure paper records are not left unattended in unsecure areas where unauthorized people may view them.
    - User will appropriately dispose of Confidential Information in a manner that will prevent a breach of confidentiality. Confidential Information shall never be discarded in the trash unless documents have been shredded.
    - Users will ensure security of workstations and portable electronic devices containing Confidential Information including laptops, smartphones, thumb drives, etc.
    - User will comply will all security safeguards, including but not limited to, any multi factor authentication requirement when accessing the Network.

    .
6. **Auditing, logging, and monitoring.** User agrees that his/her access is subject to review and/or audit by GRMC and its affiliates. The contents and history of the User's Network session are the

sole property of GRMC and its affiliates. GRMC and its affiliates may access, monitor, log, review, and disclose, as it deems necessary a User's Network activity, including but not limited to the User's EMR access, web browsing, instant messaging, E-mail, or application activity for any purpose. User understands GRMC and its affiliates may disclose, as it deems necessary, User's activity and any User content on the Network to management without prior notice or consent of the User. GRMC and its affiliates, per subpoena or court order, may disclose a User's Network activity to law enforcement officials without prior notice or consent of the User.

7. **Response to Confidentiality Concerns.** User acknowledges if GRMC or its affiliate determines access has been compromised by unauthorized parties, or access has been misused, any or all of the following actions may be taken:
    - User and/or User's supervisor may be notified of concerns related to user's access;
    - HIPAA Officer, Information Technology, and Senior Management will be notified;
    - User access may be terminated; and/or
    - Inappropriate access may be disclosed as may be necessary to appropriate authorities including State or Federal Agencies

8. **Notification of Breach.** User shall notify GRMC immediately of any suspected or actual breach of security, intrusion or unauthorized use of Network at the time User becomes aware. Notification will be made in the way of contacting GRMC's PBX Operator and asking to speak to GRMC's HIPAA Officer.

9. **User Account Status.** Access is granted to Users who require daily and/or routine access to the Network for business purposes. GRMC has several security measures in place to monitor user activity. If the User's account shows no activity, the User's account will automatically be disabled in accordance with Security policies. Once a User's account has been disabled for this purpose, the User's account will not be reactivated.

10. **User Employment Status.** Access is granted to Users who require daily and/or routine access to the Network for business purposes. The type of access granted is based on the User's roles and responsibilities for their specific employer. Access will terminated once a User separates from their current employer, physician, or business associate. Once the User has "termed", User will not access, use, or disclose Confidential Information from the Network. Should access to the Network be required with the User's new employer, User will complete a new Network Access Agreement.

11. **Health Insurance Portability & Accountability Act (HIPAA) and State/Federal Laws.** User will comply with HIPAA regulations as per 45 CFR Parts 160 and 164, and Federal and State laws governing confidentiality, privacy, and security of health information.

12. **Access, Usage, and Disclosure Requirements.**
    - User will access, display, store, use, and disclose protected health information (PHI) for legitimate purposes of treatment, payment, and healthcare operations as permitted by HIPAA or in accordance to his/her Contractual Obligations with GRMC or its affiliates.
    - User will access, use, or disclose Confidential Information only for legitimate business purposes of GRMC or its affiliates.
    - User will disclose Confidential information only to authorized individuals, i.e. individuals who require information for the performance of their job responsibilities.
    - User will only access, use, or disclose minimum necessary amount of Confidential Information necessary to carry out User's job responsibilities.
    - User will protect Confidential Information from loss, misuse, alteration, or unauthorized disclosure.
    - User will remove/delete Confidential Information (as applicable) when no longer needed.
    - User will ensure any Confidential Information transmitted uses a secure internet connection. PHI/Confidential Information transmitted via email will be encrypted.

- User understands access to GRMC and its affiliates Network is a privilege and not a right.
- User will comply with GRMC/GRMG's respective HIPAA Privacy and Security Policies.*****

13. Prohibited Access, Use and Disclosure.

- User will not access, display, store, use or disclose Confidential Information in electronic, paper or oral forms for personal reasons, or for any purpose not permitted by HIPAA, including information about co-workers, family members, friends, neighbors, celebrities, or User.
- User will not engage in activity that attempts to circumvent or avoid security controls in place by the Network.
- User will not access Confidential Information from the Network for purposes of distributing, selling, marketing or commercializing for personal gain.
- User will not misuse or attempt to alter the Network in any way.
- User will not carelessly use Internet capability that negatively affect the Network's normal performance or unduly jeopardizes the Network's capabilities and resources.
- User understands shared email and/or network accounts are not permitted.
- User will not willfully introduce a computer virus or other destructive program into the Network.
- User will not automatically forward email to an external destination not specifically approved by GRMC policy, procedure, administration, or department management.
- User will not use the Network or email for chain letters or for non-GRMC commercial activities not specifically approved by GRMC or its affiliates.
- User will not send unsolicited mass email messages, including the sending of "junk mail" or other advertising material (e.g., email spam), over the Network.
- User will not access, display, store or distribute any offensive, or discriminatory materials on the Network.
- User will not use the Network unethically, i.e. for misrepresentation or to commit fraud.
- User will not engage in any personal use of GRMC/GRMG's Network that interferes with the productivity of employees or others associated within GRMC and its affiliates business operations, or that is intended for personal gain.*
- User will not use the Network to access Internet sites that contain content that is inconsistent with GRMC/GRMG's mission, values, policies, and procedures. *

14. Equipment Return. User agrees to return any GRMC/GRMG equipment and portable devices for purposes of ensuring compliance with this Agreement and the policies described herein.*

15. Software Use.

- User understands the use of the software on the Network is regulated by the terms of separate license agreements between GRMC/GRMG and the vendors of that software.
- User agree to use software on the Network for its intended use.
- User will not attempt download, copy, or install the software on any computer or other device.
- User will not make any change to the Network without GRMC/GRMG's prior approval.
- User will not may any unauthorized reproduction of information system software.
- User will not violate any copyright or intellectual property rights laws.

16. Network.

- User understands access to the Network is "as is", with no warranties and all warranties are disclaimed by GRMC and its affiliates.
- User understands GRMC and its affiliates may suspend or discontinue access to protect the Network or to accommodate necessary down time.
- User understands in an emergency or unplanned situation, GRMC or its affiliates may suspend or terminate access without advance warning.

17. Accountability, Reporting and Sanctions.

- User understands he/she is accountable for use of the Network including, but not limited to User's content, email, and Internet use.

- User will immediately notify GRMC's HIPAA Officer if user believes there has been improper or unauthorized access to the Network.
- User will report any lost or stolen devices containing GRMC/GRMG Confidential Information to GRMC's Information Technology Department or GRMC's HIPAA Officer. If User is unable to contact the IT Department or HIPAA Officer personally, User will call GRMC's PBX Operator so that the Operator can reach them by cellular phone.
- User understands any violation of the requirements of this agreement, may subject User to disciplinary action; User access may be suspended or terminated and/or User may be liable for breach of contract and subject to substantial civil damages and/or criminal penalties.

18. ***Termination of User's Access to GRMC's Computer System.***

- GRMC and affiliates have the right to terminate this agreement and the User's access at any time, with or without notice, for any reason or no reason without any damages or liability to User.

*Applicable to GRMC Staff

Network Access Request
User Information

By completing and signing this form, you acknowledge you have read, understand, and will adhere to GRMC's Network Access Agreement and Confidentiality/HIPAA Privacy Guidelines.

Access requests are coordinated through one individual (Main Contact). This individual is typically the Senior Company Representative or Physician Office Manager. GRMC only honor requests from the Main Contact.

Complete the sections below and have your supervisor (Senior Company Representative and/or Physician) sign in the applicable section below. Once completed, email form to dhernandez@grmedcenter.com

General Information		
Office Type:	☐ Physician Office	☐ Consultant/Third Party
Company Name / Address:		
Company Phone Number:		
Main Contact Name / Phone / Email Address:		
User Request		
Printed Name	Signature	Email Address / Cellular Phone

By signing below, you acknowledge access authorization for the Users identified above. You shall be responsible for ensuring User's compliance with GRMC's Network Agreement. You will notify GRMC's Information Technology Department of HIPAA Officer if a User is termed from your facility or no longer needs Network access.

Senior Company Representative/Physician Signature

HIPAA Officer Signature

Date

Date