

Northern Arizona Healthcare Electronic Medical Records Remote Access and Confidentiality Agreement and Application

THIS ELECTRONIC MEDICAL RECORDS ACCESS AND CONFIDENTIALITY AGREEMENT ("Agreement") is made and entered into effective date: _____, between Northern Arizona Healthcare ("NAH") and _____ (The Remote Access User). Employer's name if, applicable, for NAH records: _____

- A. NAH creates and maintains demographic and health information relating to its patients (defined as "Confidential Information"). This Confidential Information is located in computer information systems as well as paper charts and files. The Confidential Information is protected from unauthorized or inappropriate access by NAH policy, as well as state and federal law.
- B. To provide the best possible service to NAH and patients, NAH wishes to grant to the Remote Access User appropriate access to Confidential Information contained in NAH Information Systems as needed to provide treatment, facilitate payment and manage healthcare operations. NAH Information Systems is defined to include all NAH computer hardware, software, data or voice communication facilities, excluding the NAH web pages devoted to employment, job resources and general public information.

The parties agree as follows:

AGREEMENT

1. **Access to Confidential Information through NAH Information Systems.** NAH agrees to provide the Remote Access User with access to NAH Confidential Information through the NAH Information Systems, subject to the conditions outlined in this Agreement. This access is provided to allow the Remote Access User to obtain Confidential Information to the extent necessary to provide treatment, facilitate payment and manage healthcare operations.
2. **Scope of Use.** The Remote Access User agrees not to gain access to, use, copy, make notes of, remove, divulge or disclose Confidential Information, except as necessary to provide treatment, facilitate payment and manage healthcare operations.
3. **Protection of Confidentiality and Security of Confidential Information.** The Remote Access User agrees to protect the confidentiality and security of the Confidential Information obtained from NAH. The Remote Access User will comply with NAH HIPAA policies (available upon request), and the HIPAA Privacy and Security Rules.
4. **Patient Permission Before Access.** Unless necessary to provide treatment, facilitate payment and manage healthcare operations, the Remote Access User agrees not to examine patient communicable disease information, genetic testing information, drug and alcohol abuse treatment information, and mental health information without having secured patient permission required by NAH policies or applicable laws or regulations.
5. **Codes and Passwords.** The Remote Access User must complete the Remote Access User

Computer Account Request Form (exhibit C) to receive remote access to NAH Information Systems. The Remote Access User **agrees not to release** their authentication code, password or device to any other person or to allow anyone else to access NAH Information Systems under their authentication code, password or device. The Remote Access User **agrees not to use or release anyone else's** authentication code, password or device. The Remote Access User agrees to notify the NAH Legal Department at 928-773-2569 immediately if they become aware or suspect that another person has access to their authentication code, password or device.

6. **Computer Security.** The Remote Access User agrees to maintain adequate security procedures for the computers on which the Remote Access User accesses the NAH Information Systems. The Remote Access User will abide by the minimum security and NAH hardware and software desktop standards as set forth in Exhibit B. The Remote Access User understands that Exhibit B and the obligations of this Agreement apply to access and use of NAH Information Systems from an office, home or remote location. The Remote Access User will not use or attempt to access NAH Information Systems by any means not specifically authorized by NAH. The Remote Access User will take no action to avoid or disable any protection or security means implemented in the NAH Information Systems or otherwise use any means to access NAH Information Systems without following log-in procedures specified by NAH.
7. **Portable Media Devices.** The Remote Access User agrees that if the Remote Access User saves Confidential Information to portable media devices, The Remote Access User will take reasonable safeguards to protect the devices and Confidential Information from any access or use not authorized by this Agreement. If the Remote Access User is uncertain on how best to protect Confidential Information, the Remote Access User will contact NAH about how to protect Confidential Information on the device while it is being serviced or repaired. The Remote Access User agrees that if any portable media device needs to be reformatted or destroyed, the Remote Access User will follow the guidelines provided by the NAH Information Services Department for proper data cleansing, reformatting or destruction of electronic media. If a portable media device is stolen or lost the Remote Access User agrees to notify NAH immediately.
8. **Printing Confidential Information.** If the Remote Access User prints Confidential Information, the Remote Access User will take reasonable safeguards to protect the printed Confidential Information from any access or use not authorized by this Agreement, and thereafter destroy such copies when they are no longer required for the purposes authorized herein. If printed confidential information is stolen or lost the Remote Access User agrees to notify NAH immediately.
9. **Return of Software or Equipment.** Upon request by NAH, the Remote Access User agrees to immediately return any software or equipment and also agrees to immediately un-install and delete any software programs provided by NAH.
10. **Auditing Compliance.** The Remote Access User agrees that their compliance with this Agreement may be subject to review and/or audit by NAH.
11. **Limitation of Liability of NAH/Exclusions of Warranties.**
The parties agree that the Healthcare Provider is responsible for the ultimate decisions and medical judgment related to the diagnosis and treatment of his/her patients based on

Confidential Information accessed on NAH Information Systems. The Healthcare Provider understands and agrees that remote access to electronic records involves technological risks, including possible introduction of errors, data corruption, and artifacts that may not be present on original versions of radiological results. The Healthcare Provider understands that images accessed remotely may not have the same degree of clarity as images viewed on-site.

The Healthcare Provider agrees that NAH will not be liable for any direct, indirect, incidental, special or other damages incurred by The Healthcare Provider arising out of the remote use of or inability to use the NAH Information System. NAH does not guarantee or warrant the availability of remote access of NAH Information System.

The parties recognize that remote access introduces unique risks associated with unrelated software that may exist on the remote access device that compromises the integrity and security of data and remote access, including but not limited to spyware, hacker access, viruses, worms, and other harmful software (collectively referred to as "Remote Access Risks"). Accordingly, NAH will not be responsible for any losses or damages related to Remote Access Risks.

- 12. Response to Confidentiality Concerns.** Whenever NAH in its sole judgment and discretion believes that the Remote Access User has obtained unauthorized access to Confidential Information, has disclosed Confidential Information inappropriately or in violation of federal or state laws or regulations, has violated any NAH policies or procedures regarding confidentiality or the use of Confidential Information, or has violated any provisions of this Agreement, NAH is also entitled to take any or all of the following actions immediately, as it determines to be appropriate.
- a. Follow the Sanctions policy.
 - b. Suspend or terminate the access to NAH information systems until NAH concerns are addressed.
 - c. Terminate this Agreement.
 - d. Bring legal action to enforce this Agreement.
- 13. Term and Termination:**
- a. **NAH employee Remote Access Users:**
This Agreement shall be effective as of the date above, and shall continue in full force and effect until terminated under Section 12 of this Agreement or an employee leaves NAH employment.
 - b. **Non-NAH employee Remote Access User – Physician, AHP, Vendor, Utilization Review, Payer and billing company and etc:** This Agreement shall be effective as of the date above, and shall continue in full force and effect until terminated under Section 12 of this Agreement or within 30 days' written notice by either party.
- 14. Additional Safeguards.** The Remote Access User understands and agrees that the HIPAA Security Regulations took effect in April 2005 and require NAH and the Remote Access User to implement security and privacy processes, practices and technical requirements in connection with the access and use of electronic Confidential Information. NAH reserves the right to impose additional information security safeguards, including (without limitation) software and hardware requirements, to comply with the Security Standards. If The Remote Access User elects to not adhere to these new requirements, The Remote Access User and/or NAH may terminate this agreement pursuant to Sections 12 & 13 above.

15. The Remote Access User's Employee:

- a. The Remote Access User may permit their employees to access Confidential Information to assist the Remote Access User only if the employees sign a separate Remote Access User Agreement with NAH and obtain separate passwords.
- b. The Remote Access User Employer will not give an employee the Remote Access User's password and will not permit an employee to share Employee's passwords with other Employees.
- c. The Remote Access User Employer agrees to train their employees on the requirements of this Agreement and on confidentiality policies.
- d. The Remote Access User Employer is responsible for their employee's compliance with all provisions of this Agreement.
- e. The Remote Access User Employer must notify NAH contact person within 24 hours of an employee termination.
- f. The employee must notify NAH of termination of employment within 24 hours. The Remote Access User Agreement does not carry over from one employer to another.
(Perot to identify a contact person and telephone number)
 Example: When a Medical Assistant moves to a different practice the MA must notify NAH within 24 hours.
- g. NAH will terminate Remote Access immediately on notification.

16. Continuing Education:

- a. The Remote Access User agrees to stay current in their knowledge of all applicable NAH policies, HIPAA Privacy rules, and HIPAA Security rules.
- b. The Remote Access User Employer agrees to provide and require at least annual employee education regarding applicable Confidentiality policies, HIPAA Privacy rules, and HIPAA Security rules.

17. Breach Notification: Reports of Impermissible Use of Disclosure.

- a. The Remote Access User will adhere to the "Breach Notification" requirements of "unsecured PHI" under the Health Information Technology for Economic and Clinical Health (HITECH) Act, The Remote Access User will **immediately** report to the NAH Legal Department any use or disclosure of PHI received from NAH for purposes other than those permitted by this Agreement and any security incident of which it becomes aware that affects PHI created on behalf of or received from NAH. The NAH Legal Department telephone number is 928-773-2569.
- b. For purposes of this section, the following definitions under the HITECH Act will apply:

 "Breach" means "the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."

 "Unsecured PHI" means "PHI that is not secured through the use of a technology or methodology specified by Health and Human Services (HHS) guidance."
- c. The Remote Access User will be financially responsible for all costs (including, but not limited to, the required notification and the maintenance of customer relation phone lines), civil penalties, and damages, that NAH incurs as the result of a "Breach" caused by the Remote Access User, their employees or agents.

- 18. **Minimum Necessary Access:** All Remote Access Users will complete the Remote Office Computer Account Request Form in Exhibit C.
- 19. The Remote Access User agrees not to email any Confidential Information to a non-hospital email account. Remote Access User will email Confidential Information to their NAH email account only as allowed by NAH policies and procedures.
- 20. The Remote Access User agrees not to allow any unauthorized person to use or access NAH Information Systems either on-site or remotely. The Remote Access User agrees not to allow family, friends or other persons to see the confidential Information on the computer screen while accessing NAH Information systems. The Remote Access User agrees to fully log out of all NAH systems before leaving any workstation.
- 21. The Remote Access User will never access Confidential Information for "curiosity viewing." The Remote Access User understands that this includes viewing the Confidential Information of children, other family members, friends, or coworkers, unless access is necessary to provide services to patients with whom there is a direct treatment relationship.
- 22. The Remote Access User agrees that if the Remote Access User sells transfers or donates their computer, The Remote Access User will contact the NAH Information Systems Department, and permit them to review the hard drive for any Confidential Patient Information.
- 23. **Continuing Obligations.** Physician and AHP Remote Access Users agree that the obligations under this Agreement continue in the event his or her medical staff privileges with NAH are terminated or expire, or in the event NAH terminates this Agreement.
- 24. **Non-Assignment.** Neither party may assign this Agreement or their rights hereunder without the prior written permission of the other party.
- 25. **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of Arizona. Jurisdiction and venue shall be in Coconino County, Arizona.

IN WITNESS WHEREOF, this Agreement has been executed on the day and year first above written.

Remote Access User

NAH:

By: _____
Title: _____
Date: _____

By: _____
Title: _____
Date: _____

Exhibit B: Technical Requirements for Off-Site Computer Access

Minimum Workstation Requirements

- Operating system: Windows 2000 or Windows XP. Vista is not supported.
- Memory: 256 MB RAM or greater

Workstation Requirements

- 1 GB RAM
- Hard Disk: 20 GB or greater available space
- Pointing Device: Windows compatible mouse
- Video Adapter: SVGA video adapter with color monitor (1024 x 768 or higher)
- PC architecture: Pentium III processor or greater as required by the operating system.

Minimum Software Requirements

- Internet Explorer version 6.0 or greater.
- Citrix ICA web client version 8.0 or current version

Software Requirements

- Macromedia Flash Player 6 plug-in or current version for using online PowerChart training

Connectivity Requirements

- High speed DSL, cable modem or wireless network connection.

Security Requirements/Recommendations

- Firewall protection should be installed on the PC and operate with detection alert capabilities enabled. Anti-virus protection software must be installed and enabled. Updates must be installed as made available from the software vendor.

Information Systems - Hospital Network and Applications Access ACCOUNT REQUEST FORM

Section 1 <input type="checkbox"/> Employee <input type="checkbox"/> New Start Date:	Mark appropriate boxes only <input type="checkbox"/> Physician <input type="checkbox"/> NAH employee <input type="checkbox"/> NAH Contracted Location: <input type="checkbox"/> FMC <input type="checkbox"/> VVMC <input type="checkbox"/> Non - Staff Provider <input type="checkbox"/> Physician Office Staff <input type="checkbox"/> Other <input type="checkbox"/> Temp <input type="checkbox"/> Traveler RN <input type="checkbox"/> Intern <input type="checkbox"/> volunteer <input type="checkbox"/> Registry <input type="checkbox"/> Perot <input type="checkbox"/> Contractor / Vendor Start Date:	Lawson ID: <input type="checkbox"/> Student <input type="checkbox"/> Nurse <input type="checkbox"/> Pre-Hospital <input type="checkbox"/> Returning Student <input type="checkbox"/> Extern <input type="checkbox"/> PCT/CNA <input type="checkbox"/> Medical <input type="checkbox"/> Other: Start Date: End Date: Instructor Name: Instructor Phone #:
--	--	--

Section 2 Individual Information		
Last Name	First Name	Middle Initial
Department or Office Name	Supervisor / Office Director	Supervisor / Office Director Contact #
Office Address	City	State
Position / Title	Contact #	Email Address
Question & Answer for when you call the Service Desk to have you password reset.		

Section 3 Requested Network and Application Access	
(To be filled out by the HR Representative or Department Director for NAH employees. By the Contact person for non NAH employees)	
<input type="checkbox"/> Network Access	<input type="checkbox"/> Off Site Access (Citrix)
<input type="checkbox"/> Email Account	<input type="checkbox"/> Chart One (ChartVault)webhealth
<input type="checkbox"/> VPN	<input type="checkbox"/> Cerner - Domains besides PROD
<input type="checkbox"/> Lawson	Define Position:
<input type="checkbox"/> NAH Portal	Whom to Copy?
<input type="checkbox"/> QS	
<input type="checkbox"/> Other Applications – please add below	Define Discipline Title: ex: (Off Staff)

Section 4 – Signature *(To be signed and dated by the applicant and if applicable the Physician/Administrator)*

I agree to protect the confidentiality and security of the protected health information ("PHI") obtained from Northern Arizona Healthcare ("NAH"). I agree to comply with applicable laws in respect to the PHI of patients and with all existing and future NAH policies and procedures concerning the confidentiality, privacy, security, use and disclosure of PHI. I will also abide by the NAH Information Systems security policies. I will ensure that the undersigned users comply with the privacy and security regulations and policies.

Name (print)	Title	Date
--------------	-------	------

Signature

If non- NAH employee the requesting physician or employee's administrator will sign below

Printed Name	Title	Date
--------------	-------	------

Physician Signature /Administrator

Section 5 NAH Authorization Signature *(to be signed by HR or those who generate Lawson # for NAH employees. Signed by the NAH Legal Department for Remote access of non NAH employees.)*

Printed Name	Title	Date
--------------	-------	------

Signature

Section 6: Return completed form to *(Note: Incomplete forms will not be processed but will be returned Requestor/Director for completion)*

NAH Employees: Your Director or Supervisor

Non NAH employees: Your NAH Contact Person

All Remote Access Requestors must complete and sign The Remote Access Agreement and return with this application

Third Party Account requestors will fill out Section 7 and return with the application.

Section 7: Contractor/Third Party Information Sheet - to be filled out along with the Security Form:
Human Resources Requests we will fill out this form for all new Third Party accounts

	Name (First, Last, MI)
	Date of Birth
	Home Address
	City, State, Zip
	Home Phone Number
	Job Title
	Department
	Start Date
	Work Phone Number
	Last 4 numbers of Social Security Number