

**ELECTRONIC MEDICAL RECORDS
ACCESS AND CONFIDENTIALITY AGREEMENT**

THIS ELECTRONIC MEDICAL RECORDS ACCESS AND CONFIDENTIALITY AGREEMENT ("Agreement") is made and entered into effective _____, between Northern Arizona Healthcare ("NAH") and _____ ("Physician").

RECITALS

- 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. Physician regularly provides health care services to NAH patients in NAH facilities. These services can be provided more safely, effectively, and timely if Physician has appropriate access to relevant Confidential Information maintained by NAH.
- C. In order to provide the best possible service to NAH patients, NAH wishes to grant to Physician appropriate access to NAH Confidential Information contained in NAH Information Systems as needed to provide health care for those patients. 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 Physician 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 Physician to obtain Confidential Information to the extent necessary to provide health care to NAH patients under the care of Physician and to permit effective and timely completion of medical records and orders.
- 2. **Scope of Use.** Physician agrees not to gain access to, use, copy, make notes of, remove, divulge or disclose Confidential Information, except as necessary to provide health care to NAH patients under the care of Physician and to permit effective and timely completion of medical records and orders. Physician agrees to control the access and use of NAH Confidential Information or NAH Information Systems by the Physician's staff in a manner to comply with this Agreement.
- 3. **Protection of Confidentiality and Security of Confidential Information.** Physician agrees to protect the confidentiality and security of the Confidential Information obtained from NAH. Physician agrees to comply with applicable Federal and State laws and with all existing and future NAH policies and procedures concerning the confidentiality, privacy, security, use and disclosure of Confidential Information, which are available upon request.
- 4. **Patient Permission Before Access.** Unless necessary for treatment, Physician 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.** Physician must complete the Physician Computer Account Request Form in Exhibit A to receive access to NAH Information Systems. Physician agrees not to release Physician's authentication code or device or password to any other person or to allow anyone else to access NAH information systems under Physician's authentication code or device or password. Physician agrees not to use or release anyone else's authentication code or device or password. Physician agrees to notify the NAH Information Services Department immediately if Physician becomes aware or suspects that another person has access to Physician's authentication code or device or password.
6. **Computer Security.** Physician agrees to maintain adequate security procedures for the computers on which Physician accesses the NAH information systems. Physician will abide by the minimum security and NAH hardware and software desktop standards as set forth in Exhibit B. Physician 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. Physician will not use or attempt to access NAH Information Systems by any means not specifically authorized by NAH, including but not limited to the use of any Internet or other non-secure means of connection. Physician 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.** Physician agrees that if Physician saves Confidential Information to portable media devices (Floppies, ZIP disks, CDs, PDAs, and other devices), Physician will take reasonable safeguards to protect the devices and Confidential Information from any access or use not authorized by this Agreement. If Physician is uncertain on how best to protect Confidential Information, Physician will contact NAH on how to protect Confidential Information on the device while it is being serviced or repaired. Physicians agrees that if any portable media device needs to be reformatted or destroyed, Physician will follow guidelines of the NAH Information Services Department for proper data cleansing or follow any policies or guidelines provided by the NAH for reformatting or destruction of electronic media.
8. **Printing Confidential Information.** If Physician prints Confidential Information, Physician 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.
9. **Return of Software or Equipment.** Upon request by the NAH, Physician agrees immediately to return any software or equipment provided to Physician by NAH. Physician also agrees immediately to delete any software programs provided to Physician by NAH.
10. **Physician Employee Access.** Physician may permit an Employee to access Confidential Information to assist Physician, only if Physician obtains from NAH a separate password for that Employee. Physician will complete the Remote Office Computer Account Request Form in Exhibit C. Physician will not give Employee the Physician's password and will not permit Employee to share Employee's passwords with other Employees. Physician agrees to train Employee on the requirements of this Agreement and on NAH confidentiality policies. Physician is responsible for Employee's compliance with all provisions of this Agreement.
11. **Auditing Compliance.** Physician agrees that Physician's compliance with this Agreement may be subject to review and/or audit by NAH.
12. **Limitation of Liability of NAH/Exclusions of Warranties.** The parties agree that Physician 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. Physician 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. Physician understands that images accessed remotely may not have the same degree of clarity as images viewed on-site.

Physician agrees that NAH will not be liable for any direct, indirect, incidental, special or other damages incurred by Physician 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.

Physician assumes all liability and risks associated with Employee access and use of remote access to NAH Information Systems.

- 13. Response to Confidentiality Concerns.** Whenever NAH in its sole judgment and discretion believes that Physician or Employee 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. Notify Physician of Employee's conduct and require Physician to educate and/or discipline Employee.
 - b. Suspend or terminate Physician's or Employee's remote access to NAH information systems until NAH concerns are addressed.
 - c. Refer Physician to NAH peer review process and report Physician to a professional board, as appropriate.
 - d. Terminate this Agreement.
 - e. Bring legal action to enforce this Agreement.
- 14. Continuing Obligations.** Physician agrees 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.
- 15. Term and Termination.** This Agreement shall be effective as of the date above, and shall continue in full force and effect until terminated under Section 13 of this Agreement or with 30 days' written notice by either party.
- 16. Non-Assignment.** Neither party may assign this Agreement or their rights hereunder without the prior written permission of the other party.
- 17. Notice.** All notices required by this Agreement shall be in writing, and shall be deemed effective when personally delivered, five business days after being mailed by certified or registered mail, return receipt requested; or five business days after being deposited with a comparably reliable postage delivery service, such as Federal Express; addressed to the other party as follows:

IF TO NAH: Legal Department
Northern Arizona Healthcare

1200 N. Beaver Street
Flagstaff, AZ 86001

IF TO Physician: _____

- 18. Waiver.** Any waiver of any of the terms or conditions of this Agreement by any party shall not be construed as a general waiver of the same condition for any subsequent breach.
- 19. Additional Safeguards.** Physician understands and agrees that the HIPAA Security Regulations will become effective in April 2005 and require NAH and Physician 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 IS security safeguards, including without limitation software and hardware requirements, to comply with the Security Standards. If Physician elects to not adhere to these new requirements, Physician and/or NAH may terminate this agreement pursuant to Section 13 above.
- 20. 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.

Physician:

NAH:

By: _____

By: _____

Its: _____

Its: _____

Date: _____

Date: _____

Exhibit B: Technical Requirements for Off-Site Computer Access

Minimum Workstation Requirements

- Operating system: Windows 9x, Windows 2000, Windows Me or Windows XP..
- Memory: 256 MB RAM or greater

Recommended Workstation Requirements

- Recommend Windows 2000 or Windows XP for optimum performance
- Hard Disk: 20 MD 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 5.5, Service Pack 2 or greater with 128-bit security
- Citrix ICA web client version 8.0 or current version

Recommended Software Requirements

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

Recommended Connectivity Requirements

- High speed DSL, cable modem or wireless network connection required.
- Contact the following vendors in your area to determine which services(s) are provided:
 - DSL – Qwest Communications
 - Cable Modem – Cable Vision, Cable One
 - Wireless – Commspeed, InfoMagic

Security Requirements/Recommendations

- Firewall protection should be installed on the PC and operating 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 OFFICE STAFF ACCOUNT REQUEST FORM

Office Use Only	
<input type="checkbox"/> Office Staff	
<input type="checkbox"/> New	Department/Office Practice:
Start Date	Office Manager:
	Office Phone/Ext:
	Office email Account:

*Section 1 -- Individual Information <small>(To be filled out by the Applicant/Office Staff personnel)</small>		
For Password Security resets please provide your Security verification question (<i>Example: What is favorite pet's name?</i>) and Security Answer (<i>Example: Joey</i>)		
		LAWSON ID:
Last Name / First Name	Q & A	LAWSON ID:
Last Name / First Name	Q & A	LAWSON ID:
Last Name / First Name	Q & A	LAWSON ID:
Last Name / First Name	Q & A	LAWSON ID:

Section 2 – Requested Network and Application Access <small>(To be filled out by the Department Director/Office Manager)</small>		
<input type="checkbox"/> Network (Novell)	<input type="checkbox"/> Cerner	
<input type="checkbox"/> Metaframe (Citrix)	<input type="checkbox"/> Define Position - Office Staff Define Discipline Title (Off Staff)	

Section 3 – Authorized Signature <small>(To be signed and dated by the Physician/Administrator)</small>		
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.		
Authorized by		
_____ Physician Signature /Administrator	_____ Printed Name	_____ Date

Section 4: Return completed form to <small>(Note: Incomplete forms will not be processed but will be returned Requestor/Director for completion)</small>
Email: perotsecurity@nahealth.com
INTERNAL FAX: Perot Systems IS Security Department at 13391 or EXTERNAL FAX: 928-773-2162
MAIL: NAH/ Perot Systems IS Department, Attn Security, 1200 N. Beaver Street, Flagstaff, AZ 86001

Information Systems - Hospital Network and Applications Access PHYSICIAN ACCOUNT REQUEST FORM

Office Use Only		LAWSON ID :
<input type="checkbox"/> Physician	FMC Medical Staff approved	VVMC Medical Staff approved
<input type="checkbox"/> New Start Date	Date: Time: Initials:	Date: Time: Initials:

*Section 1 -- Individual Information <i>(To be filled out by the Applicant/ Medical Staff personnel)</i>		
Last Name	First Name	Middle Initial
Department/Practice	Office Manager	Office Phone/Ext
For Password Security resets please provide your Security verification question <i>(Example: What is my favorite pet's name?)</i>		↑
		Security Answer <i>(Example: Joey)</i>
		↑

Section 2 – Requested Network and Application Access <i>(To be filled out by Authorized personnel)</i>		
<input type="checkbox"/> Network (Novell)	<input type="checkbox"/> Cerner Define Position	Remote Access**
<input type="checkbox"/> E-mail (Groupwise)		<input type="checkbox"/> Remote Access (off campus) Has Legal agreement been signed?
<input type="checkbox"/> Metaframe (Citrix)	Define Discipline Title (if known)	
<input type="checkbox"/> Q.S (Women's and Infant's Center)		

Section 3 – Authorized Signature <i>(To be signed and dated by the Applicant/ authorized personnel)</i>		
By logging into this system, I acknowledge being informed of this statement of confidentiality and Northern Arizona Healthcare's commitment to HIPAA standards and regulations and the treatment and handling of PHI and agree to abide by the requirements of this statement. The requestor agrees to abide by the NAH Information Security computer policies.		
Requester		
_____ Signature	_____ Printed Name	_____ Date
Authorized by		
_____ Signature	_____ Printed Name	_____ Date

Section 4: Return completed form to *(Note: Incomplete forms will not be processed but will be returned Requestor/Director for completion)*

Flagstaff Medical Center
Medical Staff Services
1200 N. Beaver Street
Flagstaff, AZ 86001

Verde Valley Medical Center
Medical Staff Services
269 S. Candy Lane
Cottonwood, AZ 86326