

ACCESS TO ELECTRONIC HEALTH RECORDS FOR CLINICS/ORGANIZATIONS

THIS AGREEMENT (“Agreement”) is made and entered into this _____ day of _____, 20_____, by and between St. Alexius Medical Center (“Hospital”) and _____ (“Organization”).

RECITALS

- A. The Hospital provides health care to patients in its community located in North Dakota and utilizes information technology for maintenance of electronic health records; and
- B. Organization, located in _____ (city, state), provides health care to patients in the community of Hospital.
- C. Organization and Hospital are Covered Entities as defined by the Health Insurance Portability and Accessibility Act of 1996 (“HIPAA”); and
- D. Organization and Hospital intend to protect the privacy and provide for the security of protected health information pursuant to federal law, including but not limited to HIPAA, the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), the regulations promulgated thereunder, as may be amended from time to time, and any other applicable law (collectively, the “Privacy and Security Regulations”); and
- E. Organization and Hospital desire to provide access to and share electronic health records for treatment, payment and operations purposes, in order to enhance the continuum of health care to mutual patients of Hospital and Organization (the “Purpose”).

AGREEMENT

1. DEFINITIONS

- 1.1 **Breach** means the unauthorized acquisition, access, use, or disclosure of protected health information not permitted by the Privacy and Security Regulations which compromises the security, privacy, or integrity of protected health information.
- 1.2 **Organization** means a physician, practitioner, health care provider, group practice, partnership, or corporation of physicians and/or practitioners, health care providers, and its employees.
- 1.3 **Disclose** and **Disclosure** mean, with respect to protected health information, the release, transfer, provision of, access to, or divulging in any other manner of protected health information outside of the entity that maintains the information.

1.4 **Electronic Health Record** (“EHR”) means a repository of consumer health status information in computer processable form used for Organizational diagnosis and treatment for a broad array of Organizational conditions. EHRs contain protected health information.

1.5 **Electronic Protected Health Information** or **Electronic PHI** means protected health information that is transmitted by electronic media (as defined by the Privacy and Security Regulations) or is maintained in electronic media. Electronic PHI may be transmitted and maintained on devices such as cell phones, PDAs, text pagers, and USB static discs.

1.6 **Information Technology** (“IT”) for purposes of obtaining access to Hospital EHR includes by way of example: rights, licenses, and intellectual property related to the EHR software; connectivity services, including broadband and wireless internet services; portals; secure messaging capabilities and related services that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, or transmission or reception of data or information in any electronic medium to any source. IT for purposes of EHR does not include hardware, including routers or modems necessary to access or enhance connectivity, and operating software that makes the hardware function; storage devices; software with core functionality other than EHR (such as human resources or payroll software or software packages for practice management or billing); or items used to conduct personal business or business unrelated to Organization practice.

1.7 **Protected Health Information** (“PHI”) means information, including demographic information, that (i) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; (ii) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual); and (iii) is received by Organization from or on behalf of Hospital, or is created by Organization, or is made accessible to Organization by Hospital. PHI may be contained in other mediums including without limitation, Electronic PHI, EHR, paper records, audio, and video recording.

1.8 **Unsecured PHI** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified in guidance by the Secretary of the U. S. Department of Health and Human Services, or his designee.

1.9 **Use** or **Uses** means, with respect to PHI, the sharing, employment, application, utilization, examination or analysis of such PHI within the entity that maintains the information.

1.10 Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy and Security Regulations.

2. HOSPITAL OBLIGATIONS

2.1 **Access.** Hospital will provide Organization with access to Hospital EHR subject to licensing agreement with IT vendors, and Organization’s compliance with this Agreement.

2.2 **Electronic Communication.** Hospital may elect to assist Organization by providing necessary link to enable Organization to access PHI in the Hospital system. Nonetheless, Organization is responsible for its installation, operation, and ongoing maintenance of IT hardware associated with communications between Organization's IT system and Hospital's IT system.

2.3 **Training and Support.** At times and manner convenient to Hospital, Hospital will provide Organization training for remote access to Hospital EHR. Hospital will not provide any support for hardware owned or used by Organization.

3. ORGANIZATION OBLIGATION.

3.1 **Permitted Use.** Organization may use Hospital IT system to access patient information that is necessary and used solely for the Purpose. Organization shall not use Hospital IT system for any other purpose.

3.2 Application for Use.

3.2.1 Organization will complete the application to access EHR (EXHIBIT A) and provide a list of Organization's staff requesting access to Hospital's EHR. To the extent applicable, Organization will identify the Site Administrator responsible for managing a list of users with such access. (EXHIBIT C)

3.2.2 Organization will obtain a signed Access User and Confidentiality Agreement (EXHIBIT B) from each individual requesting access and provide the agreements to Hospital. Organization will provide Hospital with list of users and signed copies of Access User and Confidentiality Agreements when required by Hospital. Organization agrees that any access to Hospital's internal network or other Information Technology assets is subject to CommonSpirit's Data Asset Usage Policy (IT A-002) governing acceptable use of its IT resources, available upon request.

3.3 **Compliance.** Organization is responsible for ensuring compliance with the terms and conditions of this Agreement. Organization acknowledges that its acts or omissions concerning EHR or use of Hospital IT system in any way that is not permitted by this Agreement is considered a breach of this Agreement.

3.4 **Notice of Discontinuance of Access.** Organization will notify Hospital within three business days of the departure of Organization's staff who has access to Hospital's EHR, so that Hospital may discontinue such access.

3.5 **Audits.** Hospital routinely conducts random and targeted audits of access to Hospital's IT system and EHR. Organization agrees to cooperate with Hospital audits and any resulting investigation that may involve Organization's access.

3.6 **Maintenance of Information Technology.** Organization warrants that it shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI in any manner other than as permitted by this Agreement. Organization warrants that it shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the

confidentiality, integrity, and availability of Hospital IT system, EHR, and PHI that it receives, maintains, or transmits from Hospital as required by law. Organization shall protect Hospital IT system from viruses and similar program threats and manage logging and other data collection mechanisms.

3.7 Training. Organization is responsible for HIPAA training and education, including appropriate access to EHR and terms in the Access User Agreement. Organization will provide evidence of training and education of its staff upon Hospital request.

3.8 Reporting Breaches. Organization shall report to Hospital each breach that is made by Organization that is not specifically permitted by this Agreement. Organization shall report to Hospital any security incident of which it becomes aware. For purposes of this Agreement, "Security Incident" means the attempted or successful unauthorized access, use or disclosure, modification, or destruction of information, or interference with the system operations in Hospital IT system.

Organization shall notify Hospital's Privacy Official by telephone call on or before the day immediately following the first day on which Organization knows of such breach.

Organization shall provide a full written report to Hospital's Privacy Official within five (5) days of verbal notice. Organization shall include the following in the written report: Detailed information about the breach, immediate remedial action to stop the breach, and names and contact information of individuals whose PHI has been or is reasonably believed to have been subject to the breach.

For reference purposes, as of the date of this Agreement, Hospital's Privacy Officer is **Tracey Craig**, telephone number **602-407-3929**.

3.9 Confidentiality. Organization shall only access Hospital IT system and EHR as provided in this Agreement. Organization's use of and access to EHR is limited to Organization's treatment of mutual patients of Hospital and Organization. Organization agrees that no other person or entity shall have access to, publish, or pass on Organization's password to access Hospital IT system and EHR, whether in electronic, print, or other form. Unauthorized distribution of Organization or its personnel's password, or information accessed from Hospital IT system, shall result in immediate termination of this Agreement and may subject Organization or associated end users or practitioners to loss of privileges with Hospital and any other action and remedies available to Hospital under law or equity.

3.10 Remedies in Event of Breach. Organization recognizes that irreparable harm will result to Hospital in the event of breach by Organization of any of the covenants and assurances contained in this Agreement. As such, in the event of a breach, Hospital shall be entitled to enjoin and restrain Organization from any continued violation of this Agreement. Furthermore, Organization will reimburse and indemnify Hospital expenses and costs that are reasonably incurred associated with notification of individuals, media, and credit monitoring, as a result of Organization's breach. The remedies contained in this section shall be in addition to any action for damages and/or any other remedy Hospital may have for breach of any part of this Agreement.

3.11 **Indemnity.** Organization shall indemnify, defend and hold harmless, Hospital and its affiliates, and their respective members, trustees, officers, directors, employees, and agents, from and against any claim, cause of action, liability, damage, fine, penalty, cost, or expense, including, without limitation, reasonable attorneys' fees and costs arising out of or in connection with any breach of PHI or any other breach of this Agreement by Organization.

4. MUTUAL OBLIGATIONS

4.1 **No Referral Obligation.** Nothing herein shall be construed to require Organization to refer patients to Hospital or to require Hospital to refer patients to Organization.

Term and Termination.

4.2.1 This Agreement shall be for a term of one year. Unless otherwise terminated earlier, this Agreement shall automatically renew for successive one-year terms.

4.2.2 Either party may terminate this Agreement by providing thirty days written notice to the other party of its intent to terminate.

4.2.3 This Agreement shall automatically terminate when the relationship no longer exists between the Organization and Hospital.

4.2.4 Hospital may, in its sole discretion, immediately terminate this Agreement upon Organization's breach or imminent breach.

4.3 **Assignability.** Except as otherwise expressly provided in this Agreement, Organization may not assign any of its rights or obligations under this Agreement.

4.4 **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of North Dakota applicable to agreements made and to be performed wholly within that state, irrespective of such state's choice-of-law principles.

4.5 **Insurance.** Each party shall maintain for its respective business, at its sole expense, policies of property, general liability and professional liability insurance, in an amount considered adequate for such businesses. Such policies shall insure against any claim or claims for damages arising directly or indirectly in connection with the acts or omissions of the respective party, its agents or employees pursuant to performance under this Agreement. Each party shall provide, upon request of the other party, applicable and valid certificates of insurance for any of the aforementioned policies.

5. Authority to Sign On Behalf Of Organization

Any entity signing this Agreement on behalf of any other entity hereby represents and warrants in its individual capacity that it has full authority to do so on behalf of the other entity. Any individual signing this Agreement on behalf of an entity hereby represents and warrants in his individual capacity that he has full authority to do so on behalf of such entity.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement, effective the date first above written.

HOSPITAL:

ORGANIZATION:

St. Alexius Medical Center

Organization: _____

By: Steven Leitch, MD

By: _____

Title: Chief Medical Information Officer

Title: _____

Date: _____

Date: _____

EXHIBIT A

APPLICATION TO ACCESS ELECTRONIC HEALTH RECORDS FROM ST. ALEXIUS MEDICAL CENTER

INSTRUCTIONS **COMPLETE THIS**

1. Review the Access to Electronic Health Records for Clinics/Organizations Agreement.
2. Fill in the appropriate information and have the appropriate party sign the agreement.
3. Return the completed access agreement to St. Alexius Medical Center's EpicCare Link Access Team

FORM ONLINE

Incomplete agreements will delay processing.

- If you have any questions, please contact MidwestECLAccess@commonspirit.org
- Once submitted, please start the next step by having your site administrators complete their access requests.

A completed copy of the agreement will be sent back to the contact listed below.

Organizational Information

Organization's Legal Name: _____

Please make sure to type the name correctly as this will be used for site administrator and end user agreements (to be picked from dropdown).

Address _____

Phone _____ **Fax** _____ **Tax ID** _____

Type of Healthcare Organization*(required)

- Ambulance Company
- Ambulatory Surgical Center
- Birth Center
- Chiropractic
- Counseling Center
- Dental
- Dialysis / Renal
- Durable Medical Equipment
- Home Health
- Hospice
- Imaging / Radiology
- Laboratory
- Long-Term Care
- Mental Health / Addiction Treatment
- Nursing Home / Skilled Nursing
- Optical / Optometric
- Orthotist / Prosthetic
- Pharmacy
- Physical / Occupational Therapy
- Podiatry
- Provider Practice / Clinic
- Rehab

- Other Covered Entity _____

Additional Locations

Do you have more than one location? Yes ___ No ___

If yes, please complete the next section. **COMPLETE THIS**

Facility Name _____

Address _____ **FORM ONLINE**

Phone _____ Fax _____

Organizational Contact(s)

Primary Contact Name*(required) _____

Title _____

Direct Phone*(required) _____ Email*(required) _____

Additional Contact Name _____

Title _____

Direct Phone _____ Email _____

Completed Access to Electronic Health Record Agreement*(required)

Please review the agreement prior to submission to ensure it is signed.

Incomplete agreements will delay processing.

EXHIBIT B

**ELECTRONIC HEALTH RECORD
ACCESS USER AND CONFIDENTIALITY AGREEMENT
WITH ST. ALEXIUS MEDICAL CENTER (“HOSPITAL”)**

This Agreement must be completed and signed by each individual requesting access to Hospital Electronic Health Records. The Agreement must be completed and returned to the Hospital Information Technology Department before access will be granted.

**COMPLETE THIS
FORM ONLINE**

Organization Name and Address _____

Site Administrator (Please print) _____

Name of individual requesting access (please print): _____

Job Title: _____

Any previous names used: _____

Direct Work Phone*(required): _____

Home or Mobile Phone*(required): _____

Home Address (cannot be organizational address)*(required): _____

(Cannot be clinic address, home address is required to allow access to medical records.)

Are you a Provider? Yes No

Degree: _____

Speciality: _____

NPI: _____

User Attestations

As a user, I attest I:

1. Am an employee or contractor of the healthcare organization named above.
2. Am aware of and agree to comply with state and federal Privacy and Security Rules, including HIPAA.
3. Understand that the use of St. Alexius Medical Center’s EpicCare Link, including associated files or records is strictly limited to activities directly related and appropriate to my job responsibilities.
4. Understand that the use of my identification (ID) and password by anyone other than me is prohibited. If I suspect my account may be compromised, I will report it immediately to St. Alexius Medical Center by calling 866-236-0441.
5. Acknowledge that I will only access patient health information (PHI) of patients who are being treated by the above-named organization for legitimate treatment purposes, payment activities, and/or bona fide healthcare operations.
6. Understand that I have no right or expectation of privacy in my use of St. Alexius Medical Center’s EpicCare Link. I further consent to St. Alexius Medical Center

monitoring my use of St. Alexius Medical Center's EpicCare Link.

- 7. Will notify St. Alexius Medical Center immediately at 866-236-0441 of any actual or potential breach of confidentiality or data loss associated with this access.
- 8. User agrees that any access to Hospital's internal network or other Information Technology assets is subject to CommonSpirit's Data Asset Usage Policy (IT A-002) governing acceptable use of its IT resources, available upon request.

COMPLETE THIS

I understand:

- St. Alexius Medical Center is in no way responsible for my or my organization's compliance with HIPAA or any other applicable state or federal regulations.
- Failure to comply with federal or state regulations, including HIPAA privacy and/or security rules, will result in immediate loss of access for me and potentially for my organization. Additional sanctions may be assessed based on severity of violations with federal or state regulations.

FORM ONLINE

User Signature

I HAVE READ AND UNDERSTAND AND WILL ABIDE BY ALL REPRESENTATIONS.*(required)

Signature _____

Print Name _____

Today's Date _____

REQUIRED TO BE COMPLETED BY SITE ADMINSTRATOR

I attest the above user is an employee of the healthcare organization listed and I attest to their need to access St. Alexius Medical Center's medical record.

Signature _____

Print Name _____

Today's Date _____

EXHIBIT C

SITE ADMINISTRATOR AGREEMENT

**Healthcare Organization - Site Administrator Request
WITH ST. ALEXIUS MEDICAL CENTER (“HOSPITAL”)**

INSTRUCTIONS

The enrollment process is in **TWO PARTS** as follows:

1. Requestor completes their portion of the form and **SUBMITs** the request. This will send an email to the Signatory Authority for processing.
2. Signatory Authority will receive an email with a link to complete the process. If they do not receive the link, please check junk mail. Signatory Authority completes the form and clicks **UPDATE**.

**COMPLETE THIS
FORM ONLINE**

Incomplete forms will delay processing.

- Once submitted, please start the next step by having your end users complete their access requests
- If you have any questions, please contact MidwestECLAccess@commonspirit.org

Healthcare Organization Name*(required)_____

User Information

Name*(required)_____

First, Middle, and Last names are required. If no middle name, enter "None".

Job Title*(required)_____

Any previous names used _____

Work Email*(required) _____

Failure to provide a business related email address will result in denial of access. Generalized (Yahoo, Gmail, Hotmail, etc.) email addresses may be subject to denial of access.

Direct Work Phone*(required)_____

Home or Mobile Phone*(required)_____

Date of Birth*(required)_____

Home Address*(required)_____

Cannot be clinic address, home address is required to allow access to (Insert Facility) medical records.

Are you a provider?*(required) No ___ Yes ___

Degree*(required) _____ Specialty *(required) _____ NPI*(required) _____

COMPLETE THIS Site Administrator Attestations FORM ONLINE

As Site Administrator, I attest that I will:

1. Ensure my site's users compliance with federal or state regulations, including HIPAA privacy and/or security rules.
2. Notify St. Alexius Medical Center by calling 866-236-0441 of user termination within the 90-day period and deactivate terminated users within 24 hours of departure.
3. Coordinate end user education within my site.
4. Perform password resets for my users.
5. Validate my users every 90 days through notification received through EpicCare Link/
6. Approve user access requests for my organization.

I understand:

- That my users' access will be terminated if validation does not occur on or before the end of the 90-day period. Unvalidated user accounts will be deactivated for 30 days and then formally terminated. Once user accounts are terminated, a new user request will need to be submitted to resume access.
- I am responsible for immediately notifying St. Alexius Medical Center by calling 866-236-0441 of any breach of confidentiality or data loss.

User Attestations

As a user, I attest I:

1. Am an employee or contractor of the healthcare organization named above.
2. Am aware of and agree to comply with state and federal Privacy and Security Rules, including HIPAA.
3. Understand that the use of St. Alexius Medical Center, including associated files or records is strictly limited to activities directly related and appropriate to my job responsibilities.
4. Understand that the use of my identification (ID) and password by anyone other than me is prohibited. If I suspect my account may be compromised, I will report it immediately to St. Alexius Medical Center by calling 866-236-0441.

COMPLETE THIS FORM ONLINE

5. Acknowledge that I will only access patient health information (PHI) of patients who are being treated by the above-named organization for legitimate treatment purposes, payment activities, and/or bona fide healthcare operations.
6. Understand that I have no right or expectation of privacy in my use of St. Alexius Medical Center's EpicCare Link. I further consent to St. Alexius Medical Center monitoring my use of St. Alexius Medical Center's EpicCare Link.
7. Will notify St. Alexius Medical Center immediately at 866-236-0441 of any actual or potential breach of confidentiality or data loss associated with this access.
8. User agrees that any access to Hospital's internal network or other Information Technology assets is subject to CommonSpirit's Data Asset Usage Policy (IT A-002) governing acceptable use of its IT resources, available upon request.

I understand:

- St. Alexius Medical Center is in no way responsible for my or my organization's compliance with HIPAA or any other applicable state or federal regulations.
- Failure to comply with federal or state regulations, including HIPAA privacy and/or security rules, will result in immediate loss of access for me and potentially for my organization. Additional sanctions may be assessed based on severity of violations with federal or state regulations.

User Signature

I HAVE READ AND UNDERSTAND AND WILL ABIDE BY ALL REPRESENTATIONS.*(required)

Signature _____

Print Name _____

Today's Date _____

REQUIRED TO BE COMPLETED BY PRACTICE SIGNATORY AUTHORITY

I attest the above user is an employee of the practice listed, I am the contact listed above, and I have signatory authority for this practice.

Signature _____

Print Name _____

Today's Date _____