ACCESS TO ELECTRONIC HEALTH RECORDS AGREEMENT

THIS AGREEMENT ("Agreement") is made and entered into this _____ day of _____**,** 20___, by and between Franciscan Health System ("Hospital"), and _____ ("Community Partner").

RECITALS

A. Hospital provides health care to patients in its community located in Tacoma, Washington and utilizes information technology for maintenance of electronic health records; and

B. Community Partner, located in the South Puget Sound, provides health care services to patients in the community of Hospital. This refers to such entities as skilled nursing facilities, home health agencies, home infusion agencies, hospice agencies, home medical equipment agencies, and Washington State and county governing and regulatory bodies.

C. Community Partner and Hospital are Covered Entities as defined by the Health Insurance Portability and Accessibility Act of 1996 ("HIPAA"); and

D. Community Partner and Hospital intend to protect the privacy and provide for the security of protected health information pursuant to HIPAA, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), and the regulations promulgated there under, and as may be amended from time to time (collectively, the "Privacy and Security Regulations").

E. Community Partner and Hospital desire to provide access to and share electronic health records necessary and used solely to enhance the continuum of health care to mutual patients of Hospital and Community Partner.

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 **Community Partner** 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 Hospital internal operations.

1.4 **Electronic Health Record** ("EHR") means a repository of consumer health status information in computer processible form used for clinical diagnosis and treatment for a broad array of clinical 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 Community Partner 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 Community Partner from or on behalf of Hospital, or is created by Community Partner, or is made accessible to Community Partner 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 Hospital's internal operations.

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

Access. Hospital will provide Community Partner with access to Hospital EHR subject to licensing agreement with IT vendors, and Community Partner's compliance with this Agreement.

2.2 **Electronic Communication.** Hospital will assist Community Partner with obtaining IT necessary and used solely to create, maintain, transmit, or receive EHR. Community Partner is responsible for its installation, operation, and ongoing maintenance of IT hardware associated with communications between Community Partner's IT system and Hospital's IT system.

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

3. CLINIC OBLIGATION.

3.1 **Permitted Use.** Community Partner may use Hospital IT system to access EHR that is necessary and used solely for the ongoing treatment of Community Partner's patients. Community Partner shall not use Hospital IT system for any other purpose.

3.2 **Application for Use.**

3.2.1 Community Partner will complete the application to access EHR (EXHIBIT A) and provide a list of Community Partner's staff requesting access to Hospital's EHR.

3.2.2 Community Partner will obtain a signed Access User and Confidentiality Agreement (EXHIBIT B) from each individual requesting access and provide the agreements to Hospital. Community Partner will provide Hospital with an alphabetized list of users and signed Access User and Confidentiality Agreements on an annual basis and at other times as may be requested by Hospital.

3.3 **Compliance.** Community Partner is responsible for ensuring compliance with the terms and conditions of this Agreement. Community Partner 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.** Community Partner will notify Hospital within three business days of the departure of Community Partner staff that 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. Community Partner agrees to cooperate with Hospital audits and any resulting investigation that may involve Community Partner's access.

3.6 **Maintenance of Information Technology.** Community Partner 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. Community Partner 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. Community Partner shall protect Hospital IT system from viruses and similar program threats and manage logging and other data collection mechanisms.

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

3.8 **Reporting Breaches.** Community Partner shall report to Hospital each Breach that is made by Community Partner that is not specifically permitted by this Agreement. Community Partner 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.

Community Partner shall notify Hospital's Privacy Official by telephone call immediately following the first day on which Community Partner knows of such Breach.

Community Partner shall provide a full written report to Hospital's Privacy Official within five (5) days of verbal notice. Community Partner 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 who's 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 Betty Doyle, telephone number, 253-428-8402.

3.9 **Confidentiality.** Community Partner shall only access Hospital IT system and EHR as provided in this Agreement. Community Partner's use of and access to EHR is limited to Community Partner's treatment of mutual patients of Hospital and Community Partner. Community Partner agrees that no other person or entity shall have access to, publish, or pass on Community Partner's password to access Hospital IT system and EHR, whether in electronic, print, or other form. Community Partner's unauthorized distribution of Community Partner's password, or information accessed from Hospital IT system shall result in immediate termination of this Agreement, and may subject Community Partner's employee, physician, or practitioner 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**. Community Partner recognizes that irreparable harm will result to Hospital in the event of Breach by Community Partner 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 Community Partner from any continued violation of this Agreement. Furthermore, Community Partner 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 Community Partner'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.** Community Partner 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 Community Partner.

4. MUTUAL OBLIGATIONS

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

4.2 **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 Hospital may, in its sole discretion, immediately terminate this Agreement upon Community Partner's Breach or imminent Breach.

4.3 **Assignability.** Except as otherwise expressly provided in this Agreement, Community Partner 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 Washington 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 Clinic

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:	**COMMUNITY PARTNER:**
Franciscan Health System	
By:_____	By:_____
FHS Privacy Officer or System Access Steward	Title: _____
Date: _____	Date:_____

NOTE: The completed and signed agreement must be routed to the Access Coordinator
FHScommunityaccesstacoma@chifranciscan.org

EXHIBIT A

APPLICATION TO ACCESS ELECTRONIC HEALTH RECORDS FROM FRANCISCAN HEALTH SYSTEM

Date:_____
Community Partner Name:_____
Community Partner Manager Name:_____
Business Address:_____
City:_____ State: ____ ZIP Code:_____
Community Partner Hours:_____
Email Address:_____
Community Partner Telephone Number:_____
Cell Phone Number:_____ FAX Number:_____

Complete the following information for each Community Partner staff requesting access: Name, position/title, home address, telephone number (home/cell), email address, and date of hire.

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

List all IT equipment that will be used to access electronic health records (if stationary equipment, state the location; if mobile, name the individual responsible for possession of the equipment).

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

EXHIBIT B

ELECTRONIC HEALTH RECORD
ACCESS USER AND CONFIDENTIALITY AGREEMENT
WITH FRANCISCAN HEALTH SYSTEM

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

Name of individual requesting access (please print):_____

_____

Community Partner Name and Address:_____

_____

I am requesting access to Franciscan Health System in Tacoma, Washington IT System to obtain Electronic Health Records, and agree to the following terms and conditions:

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.

Community Partner provides health care services to patients in the community of Hospital. This refers to such entities as skilled nursing facilities, home health agencies, home infusion agencies, hospice agencies, home medical equipment agencies, and Washington State and county governing and regulatory bodies. Community partners may consist of a physician, practitioner, health care provider, group practice, partnership, or corporation of physicians and/or practitioners, health care providers, and its employees.

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 Hospital internal operations.

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

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.

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 Community Partner practice.

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 Hospital from or on behalf of Community Partner, or is created by Hospital, or is made accessible to Hospital by Community Partner. PHI may be contained in other mediums including without limitation, electronic PHI, EHR, paper records, audio, and video recording.

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.

Use or **Uses** means, with respect to PHI, the sharing, employment, application, utilization, examination or analysis of such PHI within Hospital's internal operations.

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

I acknowledge that Hospital IT system is the property of Franciscan Health System. I agree to use Hospital IT system solely for job-related purposes.

I understand that all EHR available through Hospital IT system is confidential and is to be treated as such.

I promise to access Hospital IT system only in the minimal amount necessary to obtain EHR for the provision of health care services to the Community Partner patient(s).

I understand that passwords and user identification ("ID") are utilized to access Hospital IT system. I acknowledge that I may not divulge my password or ID to any other individual or entity. I understand that I am responsible for any damages, including monetary damages, for the inappropriate use and/or disclosure of EHR, even if such inappropriate use and/or disclosure was made by another individual using my password or ID. I agree that if I suspect that my password or ID has been obtained by another individual, I will immediately inform Franciscan Health System Privacy Officer so that appropriate action may be taken.

I understand that I am not permitted to access the Hospital IT systems for anything other than my intended job-related purpose. Accordingly, I understand that I am not permitted access to my health information, my family, or relative's health information, or another person's health information because of personal curiosity or personal reasons. I acknowledge that unauthorized access of EHR, confidential files, or Hospital IT system without the proper security clearance and/or access authorization, is, for whatever reason, considered a violation of Community Partner Agreement.

I understand that the Hospital IT systems are monitored by Franciscan Health System Information Technology Department. I understand that IT security features, such as passwords and message deletion functions, do not remove the ability to archive messages, at any time, for future auditing. I understand that the Hospital IT system is subject to search, and that Franciscan Health System is able to track and monitor my access into Hospital IT system. I understand that I do not have any personal privacy rights by utilizing Hospital IT system.

I agree that I will use Franciscan Health System IT system only to access EHR for patient care purposes. I promise that I will not use Hospital IT system for any other purpose including personal use, solicitation for outside business ventures, campaigns, and political or religious causes. I understand that I am prohibited from storing, displaying, or disseminating obscene, offensive, harassing, or discriminatory textual or graphical materials on Hospital IT systems.

I understand that should I violate any provision of this Access User and Confidentiality Agreement, Franciscan Health System will discontinue my access to Hospital IT system. Additionally, Franciscan Health System may take legal action against me, including seeking monetary damages for inappropriate use and/or disclosure of PHI. I understand that Franciscan Health System may be obligated to report my unauthorized access and use of PHI to federal authorities, including the federal Office for Civil Rights, and local and federal law enforcement officials.

I agree to 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 unauthorized or prohibited Use or Disclosure of Hospital IT system, PHI, or any other breach of this Agreement.

I acknowledge that I have read, understand, and agree with the conditions above. Further, I agree to immediately notify Franciscan Health System of any conflict with or violation of the above conditions.

User Signature	Date	Witness Signature