CHI Franciscan Health
Our best care. Your best health.℠

Access to Electronic Health Records Policy
Franciscan Health System

PURPOSE: The purpose of the Access to Electronic Health Records Policy ("EHR Policy") is to establish processes and procedures for permitting medical staff members and their office staff access to and sharing of the Hospital's Electronic Health Records in order to enhance the continuum of health care to mutual patients.

DEFINITIONS:

1. **Clinic** means a physician, practitioner, health care provider, group practice, partnership, or corporation of physicians and/or practitioners, health care providers, and its employees.

2. **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.

3. **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.

4. **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 Clinic practice.

5. **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 Clinic, or is created by Hospital, or is made accessible to Hospital by Clinic. PHI may be contained in other mediums including without limitation, electronic PHI, EHR, paper records, audio, and video recording.

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

7. **User** means individual who will be accessing the electronic systems requested through a unique login and password.

8. Terms used, but not otherwise defined, in this Policy shall have the same meaning as those terms in the Privacy and Security Regulations including, but not limited to, 45 C.F.R. Sections 160.103 and 164.501; 42 C.F.R. Chapter IV, Section 411.351, and 411.357, and 42 C.F.R. Section 1001.952

POLICY:
It is the policy of the Hospital to provide access to and share with each physician and/or practitioner from a Clinic who is a member of the Hospital's Medical Staff and participates in the Organized Health Care Arrangement with the Hospital ("OHCA"), the Hospital's EHR subject to the provisions and procedures outlined in this Policy.

1. Access

1.1 Each User shall sign and submit a Franciscan Access Request Form (Exhibit A).
1.2 Each user will sign a User and Confidentiality Access Agreement (Exhibit B).
1.3 Hospital will issue passwords and user identification ("ID") to access Hospital's IT system to each individual user once the completed forms are submitted. Such passwords and IDs may not be shared with any other individual or entity.
1.4 Reauthorization for access to the Hospital's EHR will be reviewed and reauthorized every two years along with the Medical Staff reappointment process.
1.5 Clinic will notify the Hospital within three business days of the departure (employment relationship or otherwise) of Clinic's staff who has access to Hospital's EHR, so that the Hospital may discontinue such access.

2. Permitted and Non-Permitted Uses

2.1 The Hospital's IT system to access EHR shall only be accessed and used solely for the ongoing treatment of Clinic's patients.
2.2 The Hospital's IT system shall not be used for any other purpose. Prohibited uses include but are not limited to: personal use, solicitation for outside business ventures, campaigns, and political or religious causes.
2.3 Clinic is prohibited from storing, displaying, or disseminating obscene, offensive, harassing, or discriminatory textual or graphical materials on the Hospital's IT system.
2.4 Clinic is not permitted to access his/her own or another individual's health information because of a personal request, personal curiosity or personal reasons.
2.5 Clinic will not permit any other person or entity to access, publish, or pass on User's password to access the Hospital's IT system and EHR, whether in electronic, print, or other form.

3. Electronic Health Record IT

3.1 The Hospital will provide Clinic with access to Hospital EHR subject to a licensing agreement with its IT vendors.

3.2 The Hospital will assist a Clinic with obtaining the necessary IT which is to be used solely to create, maintain, transmit, or receive EHR.

3.3 The Hospital will provide Clinic with minimum IT hardware requirement specifications in order for Clinic to ensure Clinic's IT systems can support Hospital's EHR. Clinic is responsible for acquiring IT hardware and ensuring IT hardware meets minimum requirements to access EHR.

3.4 Clinic is responsible for installation, operation, and ongoing maintenance of the IT hardware associated with communications between Clinic's IT system and Hospital's IT system.

3.5 At times and manner convenient to the Hospital, the Hospital will provide Clinic training for remote access of the Hospital' IT system. Hospital will not provide any support for hardware owned or used by a Clinic.

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

4. Confidentiality

4.1 All EHR available through the Hospital's IT system is confidential.

4.2 Clinic shall only access the Hospital IT system and EHR as permitted by this Policy. Clinic's use of and access to EHR is limited to the Clinic's treatment of mutual patients of the Hospital and Clinic.

4.3 Clinic will only access Hospital's IT system in the minimal amount necessary to obtain EHR for the provision of health care services to the Clinic's patients.

4.4 Hospital will routinely conduct random and targeted audits of access to Hospital's IT system. Clinic shall cooperate with the Hospital audits and any resulting investigation that may involve Clinic's access.

4.5 Hospital may track and monitor Clinic's access into the Hospital IT system.

Clinic and Users do not have any personal privacy rights by utilizing Hospital's IT system.

4.6 Clinic shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI in any manner other than as permitted by this Policy. These shall include administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI that it receives, maintains, or transmits from the Hospital and as required by law.

4.7 Clinic shall protect the Hospital IT system from viruses and similar program threats and manage logging and other data collection mechanisms.

5. Reporting Unauthorized Use or Disclosure.

5.1 Clinic shall report to the Hospital each unauthorized Use or Disclosure of PHI that is made by the Clinic that is not specifically permitted by this Policy.

5.2 Clinic shall report to the Hospital any security incident of which it becomes aware. "Security Incident" means the attempted or successful unauthorized access, use or disclosure, modification, or destruction of information, or interference with the system operations in the Hospital IT system.

5.3 The initial report shall be made by telephone call to the Hospital's Information Security Officer in the FHS Compliance Department 253-428-8353, within two business days from the time the Clinic becomes aware of an actual or apparent non-permitted Use or later than ten business days from the date the Clinic becomes aware of the actual or apparent non-permitted Use or Disclosure of PHI.

5.4 Clinic shall provide in such notice the remedial or other actions undertaken to correct the unauthorized Use or Disclosure of PHI.

5.5 Clinic shall mitigate, to the extent practicable, any harmful effect that is known to the Clinic of a Use or Disclosure of PHI by the Clinic in violation of this Policy.

5.6 Clinic shall work cooperatively with the Hospital in mitigating and preventing any further unauthorized Use or Disclosure of PHI.

6. Violations

6.1 Clinic is responsible for ensuring compliance with the terms and conditions of this Policy.

6.2 Clinic's and User's unauthorized distribution of individual password, or information accessed from the Hospital's IT system shall result in immediate termination of the User's and potentially the Clinic's access to the Hospital's IT system, and may subject the Clinic physician or practitioner to loss of privileges with the Hospital and any other action and remedies available to the Hospital under law or equity.

6.3 Clinic will be responsible for any damages, including monetary damages, for the inappropriate use and/or disclosure of EHR, even if the inappropriate use and/or disclosure was made by Clinic's employee or another individual using the Clinic's User's passwords or IDs.

6.4 If a Clinic User suspects that his/her password or ID has been obtained by another individual, they will immediately change the password for the account and inform the Hospital's Information Security Officer so that appropriate action may be taken.