



**System Access Request
Physician/Resident/Allied Health Professional**

<i>Last Name:</i> _____			<i>First Name:</i> _____			<i>MI:</i> _____		
<i>Title:</i> <input type="checkbox"/> MD/DO/DDS <input type="checkbox"/> Resident <input type="checkbox"/> NP <input type="checkbox"/> PA <input type="checkbox"/> Med Student <i>Specialty:</i> _____								
<i>Phone:</i> _____			<i>Pager:</i> _____			<i>Fax:</i> _____		
<i>Email:</i> _____						<i>HCAPS Physician?</i> Yes <input type="checkbox"/> No <input type="checkbox"/>		
						<i>(HCA employed Physicians)</i>		
<i>Social Security #</i> _____ - _____ - _____ <i>(required field)</i>								

Clinical Systems

- Meditech
 PACS Imaging
 Remote Access
 T-Systems (ER providers only)
 Transcription

To request remote access to St. David's Healthcare systems please visit our website
www.sdhpremove.com

GROUP/CALL PARTNER AFFILIATION:

I am aware of policy IS.AA.010 that states: "All physicians, except hospital-based (radiologist, pathologist, anesthesiologist and ER physicians), must be restricted to a specific group for access to only those patients associated with the group. A Group is defined as an entity of practitioners with financial interdependence. The group restriction must always be restricted to the smallest possible coverage. If no financial interdependence exists, both parties must complete an agreement to allow for cross-coverage and access to each others' patient information". I acknowledge that by listing the physicians below the physician(s) listed and their office staff will have access to my patients' records within CPCS and that I have such an agreement as described above with these physician.

_____ *Signature* _____ *Date*

Group Name (if applicable): _____

Group Members: _____

Office Manager/Contact: _____

**Please fax completed paperwork to the Help Desk at 512-341-6933.
 Since some faxes fail to transmit, please call the Service Desk to confirm receipt of your forms.
 Service Desk Phone 901-HELP (4357)**

*** The completed Computer Access Request Form must be submitted to the Division Service Desk at least 3 business days prior to when access is needed.***

INFORMATION SERVICES USE ONLY	
3/4 User ID:	Template Used:
MT Mnemonic:	



Physician Connectivity Agreement

THIS AGREEMENT is made and entered into this ____ day of _____, 20____, by and between HCA d/b/a St David's HealthCare Partnership (herein referred to as "Hospital") and _____ (herein referred to as "Physician").

WITNESSETH:

WHEREAS, the purpose of this agreement is to state the terms and conditions under which Hospital will provide Physician computer terminal access to Hospital medical records pertaining to Physician's patients admitted or treated at Hospital, in order to promote the efficient and economical delivery of medical care to such patients;

NOW, THEREFORE, in consideration of the mutual promises herein contained, Hospital and Physician agree as follows:

Article I.

Section 1.1. The Program. Hospital has developed and maintains an information computer program and database (collectively, the "Program") which permits Physician to review through a computer terminal in Physician's office or at various locations in Hospital the medical records of Physician's patients at Hospital and to obtain results of radiology treatments performed at Hospital, review medication prescriptions, treatment orders, and results of laboratory procedures and tests performed at Hospital. Hospital reserves the right to modify or discontinue the Program at any time.

Section 1.2. Program Purpose and Limitation. The Program has been designed to assist Physician in providing efficient, economical and quality medical treatment to Physician's patients, but the Program only provides access to medical information pertaining to such patients, and does not relieve Physician of the duty to visit Physician's patients at Hospital, or to sign patient charts and orders as required under Hospital's medical staff bylaws.

Section 1.3. Program Computer Terminal Access. Computer terminals to access the Program have been placed at locations within Hospital for Physician's authorized use without charge to Physician. Hospital will also place in Physician's office without charge to Physician a terminal (which shall remain property of Hospital as hereinafter more fully provided) for authorized use, and access for such terminal (with the means and method of such access to be solely determined by Hospital) to the Program. Physician will provide and maintain a compatible working telephone line which can be used to access the Program through the terminal and means of access provided by Hospital. Terminals so provided to Physician shall be used for accessing the Program as hereinafter more fully provided.

Article II.

Section 2.1. Physician Program Access. Physician will be assigned a confidential code number or other method (as may be solely determined by Hospital) by which Physician can access information in the Program pertaining to Physician's patients, and Physician shall take reasonable care to protect the confidentiality of such confidential code number or other method and shall not divulge such confidential code number or other method to other persons except as permitted herein.

Section 2.2. Medical Staff Membership. Since the purpose of providing Physician with computer terminal access through the Program to Hospital medical records is to promote the delivery of quality, efficient and economical medical care to patients at Hospital, Physician shall have access to the Program only if and so long as Physician shall be a member in good standing of the medical staff of Hospital, with clinical privileges according to Hospital's medical staff bylaws. If such membership and/or clinical privileges are suspended or terminated for any reason, Hospital may terminate Physician's access to the program immediately and without notice to Physician.

Section 2.3. Physician Employee Program Access. Upon Hospital's receipt of written request from Physician (which shall be made by Physician on a form or forms supplied by Hospital), Physician's employees designated in such request shall be provided a method by which such designated employees can access the Program, but such access shall be limited to only such information pertaining to Physician's patients as Physician may designate on such request. Physician's designated employees shall only be permitted to access the Program while employed by Physician (and only so long as Physician is permitted access to the Program), and Physician shall promptly notify

Hospital in the event any such designated employee ceases to be employed by Physician. Unless and until Hospital receives such notification, Hospital shall be entitled to assume that all such designated employees remain employed by Physician and continue to be permitted by Physician to access the Program.

Article III.

Section 3.1. Copyright. The Program, any related operating instructions, the patient's medical records, and all other documentation developed for or specifically relating to the records of a patient while at Hospital shall be copyrighted property of Hospital. Physician is granted the right and license under this Agreement to make copies thereof if and to the extent permitted or authorized hereunder.

Section 3.2. Computer Terminal. The computer terminal, modem and other hardware and software (collectively, the "Equipment") furnished by Hospital to Physician in connection with the Program under or pursuant to this Agreement shall remain the property of Hospital. Physician shall use the Equipment only to access the Program and for no other reason. Physician shall take good care of the Equipment while it is in the possession of Physician, and shall not purport to pledge, encumber or convey title to any of the Equipment and shall return the same to Hospital upon termination of Physician's access to the Program for any reason.

Article IV.

Section 4.1. Medical Records Confidential. The parties recognize that the records of the patients maintained in the Program are confidential and both Hospital and Physician are under an obligation to maintain the confidentiality of such records. Physician shall not disclose such records except to (a) other physicians and personnel under the direction of Physician who are participating in the diagnosis, evaluation, or treatment of the respective patients; (b) entities involved in the payment or collection of fees for medical services rendered by Physician provided that the patient in question has consented to such disclosure; (c) medical or law enforcement personnel if Physician determines there is an immediate probability of imminent physical injury to the patient or to others, or if there is a probability of immediate mental or emotional injury to the patient; or (d) to others as provided by law.

Section 4.2. Unauthorized Disclosure. Should Physician or an agent or employee of Physician disclose in an unauthorized manner any information obtained through access to the Program, Physician shall indemnify and save Hospital harmless from and against all claims, demands, suits, judgments, costs and expenses (including reasonable attorney's fees), if any, that may be made or taken against it or incurred by it. Further, in the event of such unauthorized disclosure, and without prejudice to any of its other rights against Physician as a result thereof, Hospital may terminate the access of Physician to the Program, without notice to Physician.

Article V.

Section 5.1. Disclaimer of Warranties. Hospital makes no representation, warranty or guaranty, express or implied, including (without limitation) any warranty of merchantability or fitness for particular purpose with regard to the Program or the Equipment supplied to Physician pursuant to this Agreement. Should the Program or any of the Equipment fail or be inaccurate, under no circumstances shall Hospital be liable for any loss of profits to Physician or for special, consequential, or exemplary damages (all of which are hereby expressly waived by Physician as a part of the consideration to Hospital for this Agreement), even if Hospital has been advised of the possibility of such damages.

Article VI.

Section 6.1. No Assignment. This agreement may not be assigned by Physician without the prior written consent of Hospital which consent may be withheld in Hospital's sole discretion.

Section 6.2. Fees and Expenses. If any action at law or in equity is brought in respect of any provision of this Agreement, the prevailing party shall be entitled to reasonable attorney's fees, costs and expenses, in addition to any other remedy or relief to which such party may be entitled.

Section 6.3. Agreement Term. The term of this Agreement shall commence on the date it is signed as indicated below, and shall continue until termination as herein provided. Termination shall occur (a) upon 30 days written notice from either party to the other, or (b) by Hospital without notice as provided in Section 2.2 or 4.2 hereof. Physician's obligations under Section 3.2 and Article IV of this Agreement, and the disclaimer and waiver under Section 5.1 of this Agreement, shall continue and be unaffected by any such termination.

Section 6.4. Notices. Any notice required or permitted to be given under this Agreement shall be in writing and shall be deemed properly addressed and postpaid, to the address specified below the signature lines for each of the parties, or at such other address as may be specified in writing.

Section 6.5. Divisions and Headings. The divisions of this Agreement into articles and sections and the use of captions and headings in connection therewith are solely for convenience and shall have no legal effect in construing the provisions of this Agreement.

Section 6.6. Severability. In the event any provision of this Agreement is held to be invalid, unlawful, or unenforceable for any reason and in any respect, such invalidity, unlawfulness, or unenforceability shall in no event affect, prejudice or disturb the validity of the remainder of this Agreement, which shall be and remain in full force and effect, enforceable in accordance with its terms.

Section 6.7. Choice of Law: Place of Performance. This Agreement shall be construed in accordance with the laws of the State in which Hospital is located.

Section 6.8. NO REQUIREMENT TO REFER. NOTHING IN THIS AGREEMENT SHALL BE CONSTRUED TO REQUIRE PHYSICIAN TO ADMIT PATIENTS TO HOSPITAL OR TO UTILIZE HOSPITAL TO PROVIDE INPATIENT, OUTPATIENT OR ANY OTHER SERVICES TO PATIENTS, TO ORDER ANY GOODS OR SERVICES FROM HOSPITAL, OR OTHERWISE GENERATE BUSINESS FOR HOSPITAL. NOTWITHSTANDING ANY UNANTICIPATED EFFECT OF ANY PROVISION OF THIS AGREEMENT, NEITHER PARTY WILL KNOWINGLY OR INTENTIONALLY CONDUCT HIMSELF IN SUCH A MANNER AS TO VIOLATE THE PROHIBITION AGAINST FRAUD AND ABUSE IN CONNECTION WITH THE MEDICARE AND MEDICAID PROGRAMS (42 USC SECTION 1320A-7B).

EXECUTED this _____ day of _____, 20_____.

Hospital: St David's Healthcare Partnership
By (signature): _____
Print Name: _____
Title: _____

Physician Signature: _____

Print Physician Name: _____

Physician Address: _____

ST. DAVID'S HEALTHCARE
HEALTH INFORMATION MANAGEMENT SERVICES DEPARTMENT

NOTICE OF PARTICIPATION
ELECTRONIC SIGNATURE PROGRAM

I, _____, wish to participate in the Electronic Signature
(Name of Physician)

Program to authenticate medical record reports and/or orders. The reports/orders will be electronically signed via the Hcare Horizon Patient Folder utilized at St. David's Healthcare.

The unique identifier (PIN) that has been assigned to me for purposes of electronic signature is official and confidential. I certify that I will not disclose the identifier assigned to me to any other person or permit another person to use it.

In the event I misuse the electronic signature, I understand that my use will be terminated and my PIN inactivated. Misuse as defined by CMS is "that the physician has allowed another person or persons to use his/her personally assigned identifier"

HCA security regulations state that a security violation exists when a user has allowed another person or persons to use his/her PIN. Security violations will be reported to the appropriate hospital committees and/or Administrative persons as addressed by facility security policies and procedures.

I agree to review each entry or document on-line prior to affixing my electronic signature. I understand that I am responsible for the content of all medical record entries that I authenticate electronically.

I agree to sign the Confidentially Agreement to use the Hcare Horizon Patient Folder

Physician Signature

Date

Print Physician Name



Personal Identification Number (PIN) Request for Electronic Signature

Provider Name (please print): _____

I am fully aware that sharing my PIN with another individual is a direct breach of security, and is a misdemeanor according to the Texas Computer Crime Statute. This is especially relevant if any reports are signed illegitimately using my PIN code.

I understand that **this request form will be shredded once the PIN is activated and that no one will have access to that number.** If this number is forgotten a new PIN will have to be requested.

**** We recommend that your PIN be a 4 digit number, if it is alpha characters it will be case sensitive.

PIN REQUESTED: _____

eScription (PIN)

Please list an alternate PIN for eScription. This system identifies you solely by your PIN and, hence, doesn't allow duplicates. In the event that the PIN you have chosen for Electronic Signature doesn't work we will utilize the pin below. Be aware that we may have to contact you for an additional pin if the one below is also already in use.

PIN REQUESTED: _____



Electronic Signature Security Agreement

Provider Name (please print): _____

I have been fully trained on the Policies and Procedures regarding Electronic Signature. I understand that all results that are finalized with my user-defined Personal Identification Number (PIN) are equivalent to that of my legal, handwritten signature. **PERFORMANCE OF ELECTRONIC SIGNATURE THROUGH INPUT OF MY PIN INDICATES THAT I HAVE REVIEWED THE DOCUMENT EITHER IN HARD COPY OR ONLINE.** All final report documents that were signed by me online are legitimate medical record documents via my electronic authorization.

I understand that all documents signed via the electronic signature function will be finalized with "Signature On File" placed on the signature line. Any subsequent printed documents with "Signature On File" affixed on the signature line will be deemed as legal copies.

I am fully aware that any sharing of my PIN code with another individual is a direct breach of security, and is a misdemeanor according to the Texas Computer Crime Statute. This is especially relevant if any reports are signed illegitimately using my PIN code.

I will not record my PIN in any manner as this increases the possibility of accidental disclosure.

I understand that failure to maintain confidentiality in access and/or use of my PIN will result in immediate revocation of the electronic signature privileges being granted herein.

I agree to sign the "Confidentiality and Security Agreement," which will be kept on file by the Partnership Information Services.

Provider Signature: _____ Date: _____

Provider Confidentiality and Security Agreement

I understand that the facility or business entity (the “Company”) at which I have privileges or for which I work, volunteer or provide services manages health information as part of its mission to treat patients. Further, I understand that the Company has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients’ health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning information, or any information that contains Social Security numbers, health insurance claim numbers, passwords, PINs, encryption keys, credit card or other financial account numbers (collectively, with patient identifiable health information, “Confidential Information”).

In the course of my affiliation or employment with the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company’s Privacy and Security Policies, which are available on the Company intranet (on the Security Page) and the Internet (under Ethics & Compliance). I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information or Company provided systems.

General Rules

1. I will act in accordance with the Company’s Code of Conduct at all times during my relationship with the Company.
2. I understand that I should have no expectation of privacy when using Company information systems. The Company may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.
3. I understand that violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company’s policies.
4. I have no intention of varying the volume or value of referrals I make to the Company in exchange for Internet access service or for access to any other Company information.
5. I have not agreed, in writing or otherwise, to accept Internet access in exchange for the referral to the Company of any patients or other business.
6. I understand that the Company may decide at any time without notice to no longer provide access to any systems to physicians on the medical staff unless other contracts or agreements state otherwise. I understand that if I am no longer a member of the facility’s medical staff, I may no longer use the facility’s equipment to access the Internet.

Protecting Confidential Information

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Confidential Information home with me unless specifically authorized to do so as part of my job.
2. I will not publish or disclose any Confidential Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Company business and within the permitted uses of Confidential Information as governed by regulations such as HIPAA.
3. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized. I will only reuse or destroy media in accordance with Company Information Security Standards.
4. In the course of treating patients, I may need to orally communicate health information to or about patients. While I understand that my first priority is treating patients, I will take reasonable safeguards to protect conversations from unauthorized listeners. Such safeguards include, but are not limited to: lowering my voice or using private rooms or areas where available.
5. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.
6. I will secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with industry-approved security standards, such as encryption.

Following Appropriate Access

1. I will only access or use systems or devices I am officially authorized to access, will only do so for the purpose of delivery of medical services at this facility, and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

2. I will only access software systems to review patient records or Company information when I have a business need to know, as well as any necessary consent. By accessing a patient's record or Company information, I am affirmatively representing to the Company at the time of each access that I have the requisite business need to know and appropriate consent, and the Company may rely on that representation in granting such access to me.
3. I will insure that only appropriate personnel in my office, who have been through a screening process, will access the Company software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.
4. I will accept full responsibility for the actions of my employees who may access the Company software systems and Confidential Information.
5. I agree that if I, or my staff, stores Confidential Information on non-Company media or devices (e.g., PDAs, laptops) or transmits data outside of the Company network, that the data then becomes my sole responsibility to protect according to federal regulations, and I will take full accountability for any data loss or breach.

☐ *Doing My Part – Personal Security*

1. I understand that I will be assigned a unique identifier (e.g., 3-4 User ID) to track my access and use of Confidential Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.
2. I will ensure that members of my office staff use a unique identifier to access Confidential Information.
3. I will:
 - a. Use only my officially assigned User-ID and password (and/or token (e.g., SecurID card)).
 - b. Use only approved licensed software.
 - c. Use a device with virus protection software.
4. I will never:
 - a. Disclose passwords, PINs, or access codes.
 - b. Use tools or techniques to break/exploit security measures.
 - c. Connect unauthorized systems or devices to the Company network.
5. I will practice good workstation security measures such as locking up diskettes when not in use, using screen savers with activated passwords appropriately, and positioning screens away from public view.
6. I will immediately notify my manager, Facility Information Security Official (FISO), Director of Information Security Operations (DISO), or Facility or Corporate Client Support Services (CSS) help desk if:
 - a. my password has been seen, disclosed, or otherwise compromised
 - b. media with Confidential Information stored on it has been lost or stolen;
 - c. I suspect a virus infection on any system;
 - d. I am aware of any activity that violates this agreement, privacy and security policies; or
 - e. I am aware of any other incident that could possibly have any adverse impact on Confidential Information or Company systems.

☐ *Upon Termination*

1. I agree to notify my Physician Support Coordinator within 24 hours, or the next business day, when members of my office staff are terminated, so that user accounts to Company systems are appropriately disabled in accordance with Company standards.
2. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company.
3. Upon termination, I will immediately return any documents or media containing Confidential Information to the Company.
4. I understand that I have no right to any ownership interest in any Confidential Information accessed or created by me during and in the scope of my relationship with the Company.

By signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Provider Signature	Facility Name and COID	Date
Provider Printed Name	Business Entity Name	

