Security Access Agreement

Thank you for your interest and we look forward to offering you this service.

Facility Contact Information

Facility: ***South Texas Health System***

Customer Support Center: ***(956) 388-2233***

Primary Facility Contact: ***Noe Alvarado***
E-Mail: ***Noe.Alvarado@uhsrgv.com***
Secondary Facility Contact: ***Mirta Espinosa***
E-Mail: ***Mirta.Espinosa@uhsrgv.com***

Phone No.: ***(956) 971-5660/388-2245***
Fax No.: ***(956) 289-5105***
Phone No.: ***(956) 971-5658/388-2244***
Fax No.: ***(956) 289-5111***

PLEASE PRINT ALL INFORMATION

Account Information

(TO BE COMPLETED BY THE REQUESTER)

Date: _____

Account Name: _____

Group (if applicable): _____

Street Address: _____

City: _____ State: _____ Zip: _____

Office Phone: _____ Fax: _____

Email Address: _____

Office Contact 1: _____ Title: _____

Office Contact 2: _____ Title: _____

Type: ☐ Physician ☐ Billing Service ☐ Vendor Support ☐ Consultant ☐ Other_____

Technical contact:

Name: _____ Phone: _____

Email address: _____

Is your technical support in-house or contracted? _____

Service Requested and Reason for Request

(TO BE COMPLETED BY THE REQUESTER)

Check all that apply

Services Requested:

☐ **FUSION (Cerner)** – Cerner is an integrated electronic medical records system that enables physicians, nurses and other authorized users to share data and streamline processes across an entire organization. An on-line electronic chart displays up-to-date patient information in real time, complete with decision-support tools for physicians and nurses. Simple prompts allow swift and accurate ordering, documenting, and billing.

☐ **PACS –** Enables access to digital images such as x-rays, and scans with access to patient's information and ability to compare with previous studies on demand.

Reason for remote access: _____

_____

(other facility specific applications)

Environment Specifications

I have reviewed the requirements (as indicated in the attachment appropriate to my request) for access and confirm that my environment meets the minimum requirements based upon the service requested.

Initial: Yes _____ No _____

Authorized Users

NAME AND TITLE TO BE COMPLETED BY THE REQUESTER.

User ID to be completed by the Facility Coordinator(s).

LIST ALL INDIVIDUALS WHO WILL REQUIRE ACCESS.
PLEASE PRINT LEGIBLY- INFORMATION USED FOR ACCOUNT SETUP.

NAME	TITLE	USER ID (To be completed by Facility Coordinator)

NOTE: All authorized users must sign a UHS Information Security Agreement. These signed agreements should be attached to this form prior to submission.

Authorized Users (cont.)

NAME AND TITLE TO BE COMPLETED BY THE REQUESTER.

User ID to be completed by the Facility Coordinator.

LIST ALL INDIVIDUALS WHO WILL REQUIRE ACCESS.
PLEASE PRINT LEGIBLY- INFORMATION USED FOR ACCOUNT SETUP.

NAME	TITLE	USER ID (To be completed by Facility Coordinator)

NOTE: All requesters must sign a UHS Information Security Agreement. These signed agreements should be attached to this form prior to submission.

Authorized Users (cont.)

NAME AND TITLE TO BE COMPLETED BY THE REQUESTER.

User ID to be completed by the Facility Coordinator.

LIST ALL INDIVIDUALS WHO WILL REQUIRE ACCESS.
PLEASE PRINT LEGIBLY- INFORMATION USED FOR ACCOUNT SETUP.

NAME	TITLE	USER ID (To be completed by Facility Coordinator)

NOTE: All requesters must sign a UHS Information Security Agreement. These signed agreements should be attached to this form prior to submission.

Medical Staff - Authorization

(This area to be completed by the **FACILITY** Medical Staff Office or Community Development Office ONLY)

Physician Name: _____

Group Name: _____

Provider Code: _____ Group Code: _____

I authorize the individual(s) above to have access to the services indicated in the Service Interest section of this agreement.

Signed: _____ Date: _____
(Medical Staff Office Director or designee)

Print Name: _____ Title: _____

Facility CEO Authorization

(THIS AREA IS TO BE COMPLETED BY THE **FACILITY CEO** ONLY)

I authorize the individual(s) above to have access to the services indicated in the Service Interest section of this agreement.

Signed: _____ Date: _____
(CEO/Managing Director or designee)

Print Name: _____ Title: _____

This authorization agreement must be signed by the CEO/Managing Director of the facility, or his/her designee, where access is requested.

****

Information Security and Privacy Agreement

Universal Health Services Facilities and other UHS subsidiaries (collectively, "UHS" or "UHS companies") are committed to maintaining high standards of confidentiality. The responsibility to preserve the confidentiality of information in any form (electronic, verbal, or written) rests with each User granted access to UHS information systems who may have access to Confidential Information, including Protected Health Information (PHI), Electronic Protected Health Information (ePHI), employee information, physician information, vendor information, medical, financial, or other business-related or company confidential information. Any information created, stored or processed on UHS systems, or systems maintained on UHS' behalf by a vendor or other individual or entity, is the property of UHS, as is any information created by or on behalf of UHS, whether written, oral or electronic. UHS reserves the right to monitor and/or inspect all systems that store or transmit UHS data, the data stored therein, as well as all documents created by or on behalf of UHS.

Definitions:

Agreement means this *UHS Information Security and Privacy Agreement*.

Confidential Information means confidential information that is created, maintained, transmitted or received by UHS and includes, but is not limited to, Protected Health Information ("PHI"), Electronic Protected Health Information ("ePHI"), other patient information, Workforce member information, employee, physician, medical, financial and other business-related or company private information in any form (e.g., electronic, verbal, imaged or written).

Protected Health Information ("PHI") means individually identifiable health information that 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. PHI can be oral, written, electronic, or recorded in any other form.

Electronic Protected Health Information ("ePHI") means Protected Health Information in electronic form.

User means a person or entity with authorized access to any UHS network and/or other information systems, including computer systems.

Workforce means employees, volunteers, trainees, and persons whose conduct, in the performance of work for UHS, are under the direct control of UHS, whether or not they are paid by UHS. Workforce also include management and employed medical staff.

I HAVE READ AND UNDERSTAND THIS ENTIRE AGREEMENT, AND I AGREE TO THE FOLLOWING:

(Note: Please initial each line in the space provided after reading it.)	***Initials:***
1. I understand it is my personal responsibility to read, understand and comply with all applicable UHS company policies and procedures, including Security policies. I understand that these policies provide important information about the acceptable use of information systems, protection from malicious software, Mobile device usage, and data encryption, and other important information. If I am provided access to PHI or ePHI, I also	

	agree to comply with the Privacy policies.	
2.	I have been provided access to the Security (and Privacy policies as applicable).	
3.	I agree not to disclose any PHI, ePHI or any other Confidential Information obtained by accessing the UHS network and/or other information systems, including computer systems, or otherwise to any unauthorized party. I agree not to access or use any PHI, ePHI or any other Confidential Information unless I am authorized to do so. I agree that all patient-related information shall be held to the highest level of confidentiality.	
4.	I agree to access the UHS network and/or other information systems, including computer systems, only for purposes related to the scope of the access granted to me.	
5.	I understand that UHS regularly audits access to information systems and the data contained in these systems. I agree to cooperate with UHS regarding these audits or other inspections of data and equipment, including UHS inquiries that arise as a result of such audits.	
6.	I agree that I will not share or disclose User IDs, passwords or other methods that allow access to UHS network and/or other information systems, including computer systems, to anyone, at any time, nor will I share my account(s). I also agree to store all UHS company-related data onto the system servers rather than on hard drives of individual workstations, personal computers or other devices.	
7.	I agree to contact my supervisor (or for non-employees, the applicable UHS Department Director or Business Contact) and IS Security Officer immediately if I have knowledge that any password is inappropriately revealed or any inappropriate data access or access to Confidential Information has occurred.	
8.	I understand that Confidential Information includes, but is not limited to PHI, ePHI, other patient information, employee, physician, medical, financial and all other business-related or company private information (electronic, verbal or written).	
9.	I agree that I will not install or use software that is not licensed by UHS (or that is otherwise unlawful to use) on any UHS information systems, equipment, devices or networks. I understand that unauthorized software may pose security risks and will be removed by UHS.	
10.	I agree to report any and all activity that is contrary to this Agreement or the UHS Security or Privacy policies to my supervisor, Department Director, IS Security Officer or Privacy Officer.	
11.	I understand that for employees this form will be part of the employee file at UHS and that failure to comply with this Agreement and the UHS Security and Privacy policies may result in formal disciplinary action, up to and including termination. I understand that for non-employees, failure to comply with this Agreement and the UHS Security and Privacy policies may result in revocation of access and the termination of any agreements or relationships with UHS.	
12.	I understand that all information and/or data transmitted by or through or stored on any UHS device, or system maintained on any UHS company's behalf by a vendor or other individual or entity, will be accessible by UHS and considered the property of UHS, subject to applicable law. I understand this includes, without limitation, any personal, non-work related information. I do not have any expectation of privacy with regard to information on any UHS network and/or other information systems, including computer systems, and understand that UHS has no obligation to maintain the privacy and security of	

the information. I understand that UHS reserves the right to monitor and/or inspect all systems that store or transmit UHS data, the data stored therein, as well as all documents created by or on behalf of UHS.	
13. I agree to comply with UHS requirements to encrypt electronic Confidential Information in accordance with UHS security policies, including the requirement that encryption software be installed on all UHS-owned laptop computers and that emails transmitted over an electronic network outside of UHS be encrypted, as described in the UHS Security policy *Data Encryption and Decryption.*	
14. I agree that all devices used by me that are connected to a UHS network and/or other information systems, including computer systems, whether owned by me or not, will be continually running approved and updated anti-virus software.	
15. I will follow the requirements for Users described in all UHS Security policies, including but not limited to the UHS Security policy *Acceptable Use Policy.*	

The UHS Information Security and Privacy Policies are available through my supervisor, manager, UHS business contact or the UHS Corporate Compliance Office.

By signing this Agreement, I understand and agree to abide by the conditions imposed above.

_____ _____

Signature Print Name

_____

Date

Please check appropriate box:

☐ ***Employee*** ☐ ***Non-Employee***

If Non-Employee, please provide your employer (or practice name) and your title/position below:

_____

Employer or Practice Name **Title/Position**

Form Revision Date: October 26, 2011

Health Information Data Access Agreement

This Health Information Data Access Agreement ("Agreement") is entered into by and between: _____ ("Healthcare Provider") and _____ ("Facility"), as of _____ ("Effective Date").

RECITALS

WHEREAS, Healthcare Provider desires to have direct electronic and/or remote access to certain protected health information of Facility's patients that have a health care relationship with Healthcare Provider or its physicians, members, employees or agents ("PHI"), for treatment and other permitted purposes under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), subject to other applicable laws; and WHEREAS, the parties desire that access be provided by the Facility under terms and conditions that will protect the privacy and security of the PHI, as well as Facility's proprietary interest in the PHI.

TERMS AND CONDITIONS

1. Term and Termination: This Agreement shall begin on the Effective Date and run for one (1) year. The term will automatically renew for additional one-year terms unless terminated earlier. The Healthcare Provider may terminate this Agreement with thirty (30) days' prior written notice. Facility may terminate this Agreement immediately either in its entirety or with respect to one or more authorized users with or without cause, including without limitation, breach of this Agreement, which shall include but not be limited to unauthorized or improper access to, or disclosure of, any of the PHI by Healthcare Provider, its physicians, members, employees, or other agents.

2. User Access: Authorized users will be limited to physicians and ancillary providers who are members in good standing of Facility's medical staff and to employees or other agents of the Health Care Provider, who will be supervised and authorized by the Health Care Provider to access the PHI only for the purposes set forth in this Agreement ("Authorized Users"). Healthcare Provider will provide a list of Authorized Users to Facility and will notify Facility immediately upon an Authorized User's termination or other long term or permanent departure from the Health Care Provider. Facility will provide Authorized Users with an individual access code. Each Authorized User must read and sign a UHS *Information Security and Privacy Agreement* to be provided by the Facility prior to being provided access. Healthcare Provider agrees that the access codes are the equivalent of a legal signature and that Healthcare Provider will be responsible for all work done using its Authorized Users' access codes. Healthcare Provider and its Authorized Users will not disclose access codes to anyone or use an access code not assigned to them.

3. Permitted Purposes: Healthcare Provider agrees not to use or disclose the PHI except as permitted or required by this Agreement or as required by law. Healthcare Provider may access the PHI through its Authorized Users only on a need-to-know professional basis for the patients for whom its healthcare providers are either: (a) attending physician, (b) consulting physician, (c) covering physician, (d) primary care physician, (e) other direct health care provider according to Facility records; (f) researcher authorized by the Facility to access certain PHI.

4. Confidentiality and Disclosure of PHI: Healthcare Provider warrants that the PHI accessed by its Authorized Users will be kept confidential and not be further disclosed to anyone other than the patient or his/her authorized representative, except as required by law. Healthcare Provider agrees that if it has a legal obligation to disclose any of the PHI to a third party, it will notify Facility promptly, in advance of the proposed disclosure date, so that the rights of Facility and the individual to whom the PHI relates will not be prejudiced. If Facility or the individual objects to the release of such PHI, Healthcare Provider agrees to provide reasonable assistance as Facility or the Individual may request in connection therewith, including reasonable assistance with information necessary to prepare protective orders or other materials in connection with the objection. Disclosures prohibited by law (including but not limited to information protected by HIPAA or the federal regulations on Alcohol and Drug Abuse Patient Records at 42 C.F.R. Part 2) are prohibited under this Agreement.

5. Security: Healthcare Provider agrees to use appropriate and reasonable administrative, physical and technical safeguards to prevent unauthorized use or disclosure of the PHI. Healthcare Provider agrees to take prompt action to correct any deficiencies and to mitigate, to the extent practicable, any harmful effect of an unauthorized access, use, disclosure, modification or destruction of the PHI by Healthcare Provider, its staff,

physicians, members, employees, contractors, agents, or others. Healthcare Provider represents that it has provided HIPAA Privacy and Security training to all staff, physicians, members, employees, and other applicable agents.

6. Miscellaneous

6.1 Healthcare Provider acknowledges that the PHI and other information created, transmitted, stored or processed on information systems of, or that are maintained for, Facility or any of its affiliates, is the property of Facility or its affiliate. Facility does not guarantee access, which shall be subject to all applicable licenses. The access and data is provided on an "as is" basis and Facility is not responsible for any interruptions, errors or omissions in the data or information provided. Healthcare Provider, for itself and its Authorized Users, agrees to release and hold Facility and its affiliates harmless from and against any and all damages Healthcare Provider may incur related to the inability to access, errors in, or omissions of the PHI.

6.2 Healthcare Provider shall be responsible for any negligence or breach of the terms of this Agreement by Healthcare Provider or any of its physicians, members, employees, contractors or other agents, and agrees to indemnify, defend and hold harmless Facility and its parent corporations, subsidiaries and related entities, their directors, officers, agents, servants, and employees from and against all claims, causes of action, liabilities, judgments, fines, assessments, penalties, damages, awards or other expenses of any kind or nature whatsoever, including, without limitation, attorney's fees, incurred by any of them and relating to or arising out of any negligence or breach of the terms of this Agreement by Healthcare Provider or any of its physicians, members, employees, contractors or agents.

6.3 Healthcare Provider is solely responsible for adequately safeguarding the PHI in accordance with applicable law. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA and other applicable privacy laws. The parties agree to take such action as is necessary to amend this Agreement to comply with changes in laws, regulations and government agency guidance.

6.4 In the event of a conflict between a provision of this Agreement and any other agreement between the parties, this Agreement shall control. The rights and obligations of each party under Sections 3, 4, 5, 6.1, 6.2, first sentence of 6.3, and choice of law provision in 6.6 shall survive termination.

6.5 This Agreement shall inure to the benefit of, and be binding upon, the parties and their respective successors and assigns. There are no third parties to this Agreement and nothing herein is intended for the benefit of a third person. Except as provided specifically herein, this Agreement may not be assigned, modified or amended except by an instrument in writing executed by both parties.

6.6 This Agreement constitutes the entire agreement between the parties on this subject matter and supersedes all other proposals, understandings or agreements, whether written or oral, regarding the subject matter hereof. This Agreement shall be governed and construed by the laws of the state where Facility is physically located without regard to laws relating to choice of law or conflicts of law. The parties agree that the benefits to Facility and Healthcare Provider under this Agreement do not require, are not payment for, and are not in any way contingent upon the admission, referral, or any other arrangement for the provision of any item or service offered by either party pursuant to the terms of this Agreement.

IN WITNESS WHEREOF, the parties hereby set their hands and seals as of the Effective Date.

(HEALTHCARE PROVIDER)	(FACILITY)
By: _____	By: _____
Name & Title: _____	Name & Title: _____
Date: _____	Date: _____