Information Security and Privacy Agreement

St. Mary's Regional Medical Center 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