SAMPLE SCHIEX USER AGREEMENT

Updated March 27, 2013

THIS USER AGREEMENT (hereinafter "agreement") is entered into with _____, a Participant in the South Carolina Health Information Exchange or SCHIEx (the "Participant") by the undersigned employee, physician, employee or agent of a physician, contractor, and/or consultant (such person who is executing being hereinafter referred to as the "undersigned"). The undersigned agrees to comply with all Company policies and procedures regarding acceptable use of all Company resources, including but not limited to personal computers, email, voicemail, phones, and the internet.

ACKNOWLEDGMENT AND AGREEMENT: Participant will issue the undersigned a unique username and they will select a unique password and when appropriate, will be issued a token for remote access. Using this unique access code, the undersigned will be granted access to patient information through the Participant's Electronic Health Record ("EHR"), including access to the South Carolina Health Information Exchange ("SCHIEx") via Participant's Participation Agreement with SCHIEx. In consideration for such access, the undersigned acknowledges and agrees to the following:

(1) I have read and understand Participant's Electronic Health Records Access Policy. I agree to abide by its terms, and I am aware that violations of this policy may subject me to disciplinary action, including discipline up to and including discharge from employment, as well as legal action.

(2) As an individual with access rights to SCHIEx via Participant's EHR, I have a duty to protect the confidentiality of patient information. Therefore, I shall treat any patient information that I am exposed to within the course of my interactions with Participant, including patient information accessed through the EHR system, as highly confidential. I understand and agree that patient information should not be accessed by or disclosed to anyone whose current professional duties do not require such access. I understand that my obligations under this agreement continue after termination of my employment with Participant.

(3) I will not access, use or disclose patient information in a manner that would violate State or Federal laws, including but not limited to HIPAA.

(4) I will not use information from the South Carolina Immunization Registry unless required for treatment or as authorized by law. I will contact the Department of Health and Environmental Control Immunization Division at 1-800-439-4082 if I have any questions about accessing the Registry or using Registry information.

(5) I understand that the use of the my username or password by anyone other than me is forbidden under any circumstances. I will not disclose my username or password and will not write down or otherwise document this information so that it could be obtained or accessed by others. I agree that I will only access Participant's EHR through my own

username and password. I will not attempt to learn or access any information using another user's credentials. If I learn or have reason to believe that others may know my username or password, I understand that it is my obligation to immediately notify Participant's Site Administrator. If I learn or have reason to believe that any person has made or attempted any unauthorized access to Participant's EHR, I will immediately report this information to my direct supervisor and Participant's Site Administrator.

(6) When I access patient information through the EHR system, I will not allow any unauthorized person to view the patient information. When I leave the physical vicinity of a device upon which I have logged onto the EHR system, I will ensure that I properly log out or secure the system. I understand that I will be held accountable for all activities undertaken using my credentials if I fail to logoff the EHR system.

(7) I understand that I am only authorized to utilize Participant's EHR system including access to patient information via SCHIEx, in connection with those patients with whom I or my employer/contractor have a direct treatment relationship or when my job responsibilities require such access. This expressly prohibits me from accessing my own personal medical records or those of family members, friends, colleagues, or anyone of public interest. At no time shall I utilize the EHR system for any reason other than its intended use, which is to perform professional duties respecting my and/or Participant's patients.

(8) I will ensure that appropriate security measures are implemented and maintained respecting any device I utilize to access the EHR system. I agree that I will not cause or permit any patient information to be electronically downloaded, forwarded, saved (to CD's, DVD's, USB drives, portable hard drives, etc.) or otherwise stored on any such device (other than to Participant's own electronic medical record of the patient). I will take all reasonable and practical measure to minimize the risk of unauthorized access to the electronic health record system through such PC, device or system. In addition, I acknowledge and agree that I will not print any patient information unless necessary and any patient information that is printed must be stored in a secure locked area when not in use and properly disposed of (shredded, not discarded in trash) when the paper copy is no longer needed.

(9) I am aware that Participant reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the Participant's EHR system at any time, with or without notice, and I expressly consent to such monitoring. I am aware that the use of passwords or codes, the placement of data in "personal" folders or other electronic storage, and written indications on e-mail or other electronic communications of "confidential" or "private" does not restrict the Participant's right to access such communications. I further understand that I have no expectation of privacy with regard to any use of the Participant's EHR system. Participant has the right to revoke my access to Participant's EMR at any time.

(10) Should I access or attempt to access any patient information other than that belonging to those patients with whom I or my employer/contractor have a direct

treatment relationship shall constitute a breach of this agreement, for which Participant may seek such legal action and damages as may be allowable under applicable law. Additionally, any such breach or violation of this agreement shall subject me to disciplinary action by Participant, including, but not limited to termination of employment, revocation of the my privilege to utilize the EMR system and, in the case of physicians, corrective action under the Participant's medical staff bylaws and/or applicable rules and practices. In the case of the group practice for which the person(s) committing the breach is employed, suspension or termination of the entire group's privileges to utilize the EMR may result.

_____ _____

Name (Signature) **Date**

_____ _____

Name (Printed) **Department**

ADDITIONAL PHYSICIAN OR BUSINESS ASSOCIATE AGREEMENT

(1) Any physician or business associate who designates an employee or contractor for purposes of having a username and password issued to such employee shall have the responsibility to immediately notify Participant's Site Administrator in the event the employment of such employee is terminated or in the event of any other change in circumstances that would make such employee's continued access to the EHR system potentially inappropriate.

(2) Any physician or business associate requesting that a username and password be issued to their contractors or other 3rd party business partners (for example, billing contractors) accepts responsibility for ensuring their partners adhere to all of Participant's security and privacy policies and procedures when handling confidential patient information. In addition, any breach of privacy or security that results from any act or omission by such a partner may result in disciplinary action taken against the sponsoring medical staff member, and/or their group practice. The security practices of business partners should be periodically reviewed to ensure that patient information in their possession is adequately protected and properly disposed of when no longer needed, especially when the outsourced relationship has expired or been otherwise terminated.

_____ _____

Signature of Authorizing Physician (if Above is an employee of a physician not employed by Participant) **Date**

_____

Name (Printed)

_____ _____

Authorizing Agent (if above is a contractor Or outsourced billing agent) **Date**

_____

Name (Printed)