THIRD PARTY CONNECTION AGREEMENT
WITH THE UNIVERSITY OF CHICAGO HOSPITALS

THIS AGREEMENT (the **"Agreement"**) is made this ____ day of _____, 20__ (the **"Effective Date"**) by and between **The University of Chicago Hospitals** ("**UCH**") and _____ (**"Third Party"**). UCH and Third Party will each individually be referred to as a **"Party,"** and collectively as the **"Parties."**

RECITALS

WHEREAS, UCH and Third Party desire to establish a network connection, over that will be transmitted confidential information, including Electronic Protected Health Information (defined below);

WHEREAS, UCH has established policies and procedures for the transmission of EPHI via network connections, which policies and procedures require particular actions on behalf of the recipient of the EPHI to ensure an appropriate transmission;

WHEREAS, Third Party will take the actions set forth below to ensure this appropriate transmission.

NOW, THEREFORE, in consideration of the mutual promises and covenants set forth in this Agreement, and other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the Parties agree as follows:

Definitions:

"Business Purpose" means the reason UCH is providing Third Party will access via the Network Connection, which reason is _____, and which reason is documented in the contract that is attached hereto as Exhibit 3, if any.

"Confidential Information" means all information of one party concerning its practices, policies, procedures, technology and products and other similar information that is of a confidential nature, and for UCH includes information that UCH transmits on behalf of its affiliates, including The University of Chicago, except that Confidential Information does not include information that is available to the public. Confidential Information includes all summaries, abstracts, and copies of all documents that include or are based upon Confidential Information.

"Electronic Protected Health Information" or "EPHI" is defined in the Business Associate Agreement attached hereto as Exhibit 1.

"Network Connection" a connection between UCH and Third Party that will provide Third Party with access to the following UCH equipment and/or software: _____ [*insert all equipment and/or software that will be connected]* . The

Network Connection will be one of the University of Chicago Hospitals connectivity options listed in Section B of its Network Connection Policy.

"Protected Health Information" or "PHI" is defined in the Business Associate Agreement attached hereto as Exhibit 1.

"Transmitted Information" means the information, including EPHI that is transmitted from UCH to Third Party through the Network Connection. All Transmitted Information is Confidential Information.

1. Right to Use Network Connection; Responsibility. The Third Party represents and warrants that it will only use the Network Connection for Business Purpose, and for no other reason whatsoever. It will take action necessary to instruct its employees and authorized agents of the Business Purpose and of the restrictions in this Agreement. Third Party will be responsible for all acts and omissions of its employees and agents authorized to access Confidential Information, including the Transmitted Information, and use the Network Connection.

2. Ownership of Data. Third Party acknowledges and agrees that UCH owns all right, title, and interest in and to all Confidential Information and EPHI, and that such right, title, and interest will be vested in UCH. Neither Third Party nor any or its employees, agents, consultants or assigns will have any rights in any of the Confidential Information or EPHI or to Use the PHI in any form including, but not limited to, stripped or aggregated information, or statistical information derived from or in connection with the PHI, except as expressly set forth above. Third Party represents, warrants, and covenants that it will not compile and/or distribute analyses to third parties using any PHI without UCH's express written consent.

3. Network Security.

   3.1 Third Party will allow only Third Party employees approved in advance by UCH ("Authorized Company Employees") to access the Transmitted Information, the Network Connection or any UCH equipment. Third Party shall ensure that Authorized Company Employees are not security risks, and upon UCH request, Company will provide UCH with any information reasonably necessary for UCH to evaluate security and privacy issues relating to any Authorized Company Employee. All access to the Network Connection, Transmitted Information, or any UCH equipment is in UCH's complete discretion and may be terminated at any time for any reason whatsoever.

   3.2 Third Party will promptly notify UCH whenever any Authorized Company Employee leaves its employ or no longer requires access to the Network Connection, Transmitted Information, or UCH equipment.

3.3 Third Party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies:

(A) for the protection of its internal network and information, and

(B) that are sufficient to ensure that (i) its use of the Network Connection UCH equipment is secure and is used only for authorized purposes, and (ii) its business records and data are protected against improper access, use, loss alteration or destruction.

3.4 Third Party will perform those responsibilities identified as such in Exhibit 2.

4. Notifications. Third Party shall promptly notify UCH in writing upon a change in the user base for the work performed over the Network Connection or whenever a change in the connection and/or functional requirements of the Network Connection is necessary.

5. Payment of Costs. Each party will be responsible for all costs incurred by it to perform its obligations under this Third Party Connection Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

6. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to the other Party's Confidential Information." Third Party will not make any copies of any Confidential Information except with the express written permission of UCH. Within thirty (30) days of UCH's request for the return of Confidential Information in its possession, or if directed by UCH in writing, destroy the Confidential Information and cause an officer of Third Party to certify to UCH in writing that all Confidential information has been destroyed. Third Party and its employees, agents, subcontractors and any other individuals permitted by Third Party to access any computer system, network, file, data or software owned, leased, or licensed by UCH will (i) use all reasonable security practices and take all reasonable security measures necessary to protect the security of all such computer systems, networks, files, data and software, and (ii) abide by UCH's system security requirements and guidelines.

7. Term, Termination and Survival. This Agreement will remain in effect until the later of (a) the termination of the Network Connection, the return of all Confidential Information and EPHI, or (b) the termination of the services. Sections 2, 6, 7, and 8, and Exhibit 1.

8. Miscellaneous. Unless otherwise stated in this Agreement, this Agreement may only be amended by the mutual written consent of Third Party and UCH. The invalidity or unenforceability of any term of this Agreement will not affect the validity or enforceability of any other term of this Agreement. The term "including" used in this Agreement will

mean "including but not limited to." Third Party may not assign or transfer any of its rights and obligations under this Agreement without the prior written consent of UCH. No assignment will relieve Third Party of the performance of any accrued obligation that it have under this Agreement. No waiver of any term, provision, or condition of this Agreement whether by Third Party's or UCH's conduct or any other way in any one or more instances will be deemed to be or construed as a further or continuing waiver of such term, provision, or condition, or of any other term, provision, or condition of this Agreement. The law of Illinois will govern this Agreement, and Third Party will submit to the jurisdiction of the courts of Cook County, Illinois and governing bodies of Illinois.

IN WITNESS WHEREOF, the signatory represents that he/she is a duly authorized representative of Third Party and executes this Agreement on behalf of Third Party.

The University of Chicago Hospitals	**[*insert name of Third Party]***
By:_____	By:_____
Name:_____	Name:_____
Title:_____	Title:_____
_____	_____
Date	Date

EXHIBIT 1
THIRD PARTY STANDARDS

Third Party will abide by the following standards. Third Party will:

Guarantee that the VPN connection is only used for the purposes set forth in this Agreement

Use best practices to maintain a secure enterprise network free from programming devices or instructions (e.g., viruses, key locks, back doors, trap doors, etc.) that could (a) disrupt use of the, infect or defraud UCH's system, equipment or software or (b) destroy or damage data or make data inaccessible or delayed, except for file and purge routines necessary to the routine functioning of a UCH system.

Repair or apply applicable security patches to known security vulnerabilities as soon as possible, test and verify that the patches work, and notify UCH immediately of the need for such change.

Use industry standard encryption algorithms and best practice configurations to ensure security of the transmissions (for example at September 2005, AES and 168 bit 3DES), or use its own encryption and configuration policies if recognized as an industry standard by a technology standard organization (for example IEEE and RFC).

Identify and maintain a log of all personnel ever provided access to the VPN connection and provide the log upon reasonable request of UCH.

Notify UCH at least fourteen (14) days prior to any desired change to the VPN connection and work cooperatively with UCH to effectuate the change. If a circumstance necessitates an urgent change, then Vendor will notify UCH immediately upon it knowledge of the need for such change.

Notify UCH as soon as possible of any changes in Vendor's password policy or changes in the information provided to UCH as part of the VPN connection process.

Monitor, log and audit the VPN connection to verify compliance with this Agreement and to provide documentation upon UCH's reasonable request.