UPMC THIRD PARTY COMPUTER SYSTEM ACCESS AGREEMENT

This Agreement (the "Agreement") is made as of the day executed by Third Party, by and between _____ ("Third Party") with its principal place of business at _____ and UPMC, ("UPMC") with its principal place of business at 200 Lothrop St, Pittsburgh, Pennsylvania 15213. The term "Third Party" applies to both Third Party and its staff ("Third Party Staff"). UPMC and Third Party may be referred to individually as a "Party" or together as the "Parties."

WHEREAS, for Third Party to provide services with, to or on behalf of UPMC or requires access to UPMC Confidential Information that is subject to a separate agreement between the parties (the "Purpose");

WHEREAS, to further the Purpose, UPMC may provide Third Party with access to UPMC computer systems and information that UPMC considers to be confidential, including identifiable health information of UPMC patients ("UPMC Confidential Information"); and

WHEREAS, the Parties acknowledge that UPMC is a "covered entity" as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and

WHEREAS, Third Party agrees that its access to UPMC computer systems and UPMC Confidential Information is predicated on its compliance with the terms set forth in this agreement.

NOW, THEREFORE, in consideration of the mutual covenants set forth herein, Third Party agrees to be legally bound as follows.

SECTION 1 – THIRD PARTY CATEGORIES

1.1. Third Party is recognized as an organization whose Purpose is described by one of the following categories (check one that applies):

☐ Provider: A Third Party that requires access to UPMC computer systems in order to obtain patient information that is necessary for providing care to those patients that have been referred to UPMC by Provider or is referred patients by UPMC ("Referral Relationship"). A Provider may include, but is not limited to, Physician Practices, Hospitals, Long Term Care Facilities, Nursing Homes, etc.

☐ Sponsor: A Third Party that requires access to UPMC computer systems as part of an agreement to sponsor a research study.

☐ Vendor: A Third Party that requires access to UPMC computer systems in order to provide UPMC with a service.

☐ Educational Institutions: A Third Party that requires access to UPMC computer systems in order to support the training of its students while performing clinical education activities at UPMC facilities.

☐ Partner: A Third Party that has partnered with UPMC to achieve the Purpose.

☐ Monitor: A Third Party that has been granted access to UPMC computer systems for the Purpose of monitoring a research study.

☐ UPMC Health Plan: A Third Party that requires access to UPMC's EPIC physician practice management system ("EPIC System") for the purpose of scheduling Health Plan member appointments with UPMC Providers.

SECTION 2- GENERAL THIRD PARTY REQUIREMENTS

2.1. Third Party Responsible for its Staff. Third Party shall inform Third Party Staff of their responsibilities under this Agreement. Third Party shall also ensure that all Third Party Staff being granted access to UPMC computer systems and UPMC Confidential Information sign and comply with the "UPMC Confidentiality Agreement for Third Party Staff Accessing UPMC Information Systems" that is attached as Exhibit "A". Third Party acknowledges that access to UPMC computer systems and information by Third Party Staff is governed by laws applicable to the facility where access occurs.

2.2. Property Rights. All UPMC Confidential Information is and shall remain the property of UPMC. Third Party agrees that it acquires no title or rights to UPMC Confidential Information, including any de-identified information derived from such UPMC Confidential Information.

2.3. Limitations on Access. Third Party's access to UPMC computer systems and UPMC Confidential Information is limited to information that is necessary to accomplish the Purpose.

2.4. Issuance of Unique Accounts. UPMC will issue a unique user account to each of Third Party Staff Members requiring access to UPMC computer systems and UPMC Confidential Information. Third Party Staff is not permitted to share or use another staff member's account(s).

2.5. Appropriate Use. Third Party is responsible for the appropriate use and safeguarding of user accounts and passwords for UPMC computer systems.

2.6. Notification of Change in Account Requirements. Third Party shall inform the UPMC staff member sponsoring the account(s) in writing in the event that Third Party or Third Party Staff having user accounts no longer have a need to use UPMC computer systems or have access to UPMC Confidential Information, or if the Third Party Staff access requirements change.

2.7. Assistance to Administer Accounts. Third Party shall provide all assistance and information necessary for UPMC to administer the Third Party's assigned user accounts.

2.8. Notification of Security Breach. Third Party shall notify the ISD Information Security Group immediately in writing at InformationSecurity@upmc.edu if a Third Party suspects that a non-authorized individual (including Third Party Staff) has learned of a user account password or has inappropriately accessed UPMC computer systems or UPMC Confidential Information.

2.9. Mitigation of a Breach. When applicable, Third Party shall protect all UPMC Confidential Information under this agreement in the same manner as Third Party would protect its own individually identifiable health information. In the event of a breach, Third Party agrees to report any inappropriate use and agrees to mitigate, to the greatest extent possible, any harmful effect of such inappropriate use.

2.10. Assistance. To the extent that UPMC develops automated tools to manage user accounts or what UPMC Confidential Information a Third Party can access, Third Party will assist UPMC in operating these tools.

2.11. Security Controls. When applicable, Third Party shall install, configure and manage appropriate security tools on Third Party's information systems to reduce the threat that parties not subject to the Agreement could use Third Party's information systems to gain unauthorized access to UPMC computer systems or UPMC Confidential Information. Third Party shall also take commercially reasonable measures to maintain its computer equipment, software, and network against intrusions, viruses, worms, or other disabling codes.

2.12. Audits. UPMC reserves the right to audit Third Party's issuance of user accounts. To the extent that UPMC provides Third Party with tools to audit what UPMC Confidential information a Third Party Staff Member has accessed, Third Party will use the tools on a regular basis (no less than weekly) to perform audits to determine if a Third Party Staff Member has inappropriately accessed UPMC Confidential Information. In the event that Third Party suspects that a Third Party's Staff Member has inappropriately accessed UPMC Confidential Information, Third Party shall immediately inform UPMC.

2.13. Assistance with Investigations. Third Party shall provide all assistance and information necessary for UPMC to investigate any suspected inappropriate use of UPMC computer systems or access to UPMC Confidential Information.

2.14. Staff Discipline. Third Party shall provide appropriate training to Third Party Staff Members who will be accessing UPMC computer systems and UPMC Confidential Information, including development of appropriate policies and procedures. Third Party shall discipline any Third Party Staff Members who fail to comply with the terms of this Agreement. Such discipline may include discharge. Third Party shall provide information regarding such discipline to UPMC upon UPMC's request.

2.15. Policies. Third Party shall develop and implement appropriate policies and procedures to comply with this Agreement.

SECTION 3- PROVIDER REQUIREMENTS

3.1. HIPAA Compliance. The Parties acknowledge that Provider is a "covered entity" as defined in HIPAA and, pursuant to the HIPAA Privacy Rule, Provider and UPMC are entitled to share information as necessary in order to perform payment, treatment and care planning activities.

3.2 Permitted Access, Use and Disclosure. Provider and Provider's Staff shall only access UPMC Confidential Information of patients for which a Referral Relationship exists, and is limited to information that is necessary for continuity of care and Provider's treatment.

3.3. Patient Authorization. Prior to accessing, using, or further disclosing UPMC Confidential Information, Provider shall secure any necessary written authorizations from the patient or such individuals who have medical decision making authority for the patient.

SECTION 4- SPONSOR REQUIREMENTS

4.1. On-Site Monitoring. Unless UPMC has implemented a process to review all UPMC Confidential Information accessed by Sponsor on a regular basis, Sponsor Staff will not remotely access UPMC computer systems or UPMC Confidential Information. In such cases, Sponsor Staff shall only access UPMC Confidential Information at UPMC's site through UPMC's computer systems.

SECTION 5- VENDOR REQUIREMENTS

5.1. HIPAA Compliance. Vendor agrees that to the extent that Vendor has access to UPMC patient information, Vendor shall comply with UPMC's HIPAA Business Associate terms and conditions, including any future modifications thereto, that are found at:

http://www.upmc.com/about/Partners/supply-chain/Pages/guidelines-for-associates.aspx

SECTION 6- EDUCATIONAL INSTITUTION REQUIREMENTS

6.1. Education Institution Responsible for its Users. Educational Institution shall inform Educational Institution Users (including students, staff, and faculty) of their responsibilities under this Agreement. For the purpose of this agreement, Educational Institution Users are Third Party Staff. Educational Institution shall also ensure that all Educational Institution Users being granted access to UPMC computer systems and UPMC Confidential Information shall (a) first successfully complete UPMC's standard staff training for privacy and information security, and (b) sign and comply with the "UPMC CONFIDENTIALITY AGREEMENT FOR THIRD PARTY STAFF / STUDENTS ACCESSING UPMC INFORMATION SYSTEMS" that is attached.

6.2. Tracking of Training and Agreements. Educational Institution shall maintain evidence of all Educational Institution Users (including students, staff, and faculty) having successfully completed UPMC's standard staff training for privacy and information security. Such evidence shall be maintained for a period of five (5) years from the date of graduation or termination of the Educational Institution Users. Educational Institution shall maintain signed copies of the "UPMC Confidentiality Agreement for Educational Institution Users Accessing UPMC Information Systems" for a period of five (5) years from the date of graduation or termination of the Educational Institution Users.

SECTION 7- PARTNER REQUIREMENTS

7.1. HIPAA Compliance. It is agreed that Partner shall have no access to UPMC Confidential Information.

SECTION 8- MONITOR ACCESS REQUIREMENTS

8.1. On-Site Monitoring. Unless UPMC has implemented a process to review all UPMC Confidential Information accessed by Monitor on a regular basis, Monitor Staff will not remotely access UPMC computer systems or UPMC Confidential Information. In such

cases, Monitor Staff shall only access UPMC Confidential Information at UPMC's site through UPMC's computer systems.

SECTION 9- UPMC HEALTH PLAN ACCESS REQUIREMENTS

9.1. Patient Authorization. Prior to accessing UPMC Confidential Information to accomplish the Purpose, the Health Plan shall secure any necessary written authorizations from the patient or such individuals who have medical decision making authority for the patient.

9.2. Notification of Change in Account Requirements. The Health Plan shall use UPMC's IMS system to add, modify or revoke user accounts of Health Plan Staff as appropriate to accomplish the Purpose and consistent with the terms of this agreement. The Health Plan agrees that it shall immediately revoke a Health Plan Staff Member's user account(s) upon the termination of the Health Plan Staff Member or if the Health Plan Staff Member no longer requires access. UPMC reserves the right to audit the Health Plan's issuance of user accounts.

SECTION 10 - UPMC'S RIGHTS

10.1. Periodic Reviews. UPMC shall perform regular reviews to determine if Third Party's access to UPMC computer systems and UPMC Confidential Information is consistent with the Purpose.

10.2. Revocation of Accounts for Lack of Use. UPMC shall revoke any account if it is not used for a period of ninety (90) days.

10.3. Annual Review of Access Requirements. UPMC shall review the UPMC computer system access requirements of all Third Party Staff on an annual basis.

10.4. Revocation of Accounts Due to Inappropriate Use. UPMC may immediately suspend or terminate a Third Party's access to UPMC computer systems and UPMC Confidential Information in the event that the Third Party or its Staff uses UPMC computer systems or UPMC Confidential Information in a manner that is inconsistent with this Agreement.

10.5. Revocation of Access for Any Reason. UPMC reserves the right to terminate Third Party's access to UPMC's facilities, UPMC computer systems, and UPMC Confidential Information at any time without cause or notice.

10.6. Protection of UPMC Computer Systems. UPMC will take all appropriate and necessary steps to protect UPMC computer systems and UPMC Confidential Information from potential threats or misuse. Such steps may impact Third Party's ability to use UPMC computer systems and UPMC Confidential Information.

10.7. Third Party Responsible for Cost. UPMC is not responsible for costs incurred by Third Party in connection with it complying with this agreement or accessing UPMC computer systems or UPMC Confidential Information.

10.8. Compliance Audits. UPMC reserves the right to perform reasonable audits to ensure that Third Party has complied with this agreement.

SECTION 11- GENERAL TERMS

11.1. Term. This Agreement shall be for a term of one year. UPMC, at its sole discretion, may extend the Agreement for subsequent terms.

11.2. WARRANTY. ALL UPMC Confidential Information IS PROVIDED ON AN "AS IS" BASIS AND WITHOUT ANY WARRANTIES OR INDEMNIFICATIONS. UPMC DISCLAIMS ALL WARRANTIES WHETHER WRITTEN, ORAL, EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, ANY WARRANTY OF DATA ACCURACY OR COMPLETENESS, THAT ACCESS TO UPMC Confidential Information WILL BE AVAILABLE AT ANY TIME, INTELLECTUAL PROPERTY INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

11.3. Interpretation. Any ambiguity in these terms and conditions shall be resolved in a manner that permits UPMC to comply with the Privacy Rule.

11.4. Regulatory Compliance. Third Party shall take such actions as are necessary for Third Party and UPMC to comply with applicable federal, state or local statutes, or regulations promulgated by regulatory agencies or accrediting organizations either existing or future ("Regulations"). Third Party shall perform such work at Third Party's own expense. Such actions will be completed within the times specified for compliance within the Regulations. UPMC shall have the right at all times to review and inspect the steps taken and procedures implemented by Third Party to assure compliance with such Regulations. In the event that UPMC in good faith determines that Third Party's compliance with such Regulations has not or cannot be accomplished by the timeframes required by the Regulations, UPMC may terminate this Agreement without liability or penalty.

11.5. UPMC's Remedies Third Party acknowledges that its breach of this Agreement will cause irreparable damage to UPMC and hereby agrees that UPMC shall be entitled to seek injunctive relief under this Agreement, as well as such further relief as may be granted by a court of competent jurisdiction in connection with any breach or enforcement of Third Party's obligations under this Agreement or the unauthorized use, access or disclosure of UPMC Confidential Information.

11.6. Amendment. This Agreement may not be modified or amended, except in writing as agreed to by both Third Party and UPMC.

11.7. No Additional Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than UPMC and Third Party any rights, remedies, obligations, or liabilities whatsoever.

11.8. Notices. All notices under this Agreement shall be in writing. All notices shall be addressed to the appropriate addresses noted below. Notices shall only be given via registered or certified mail and shall be deemed effective and given as of the date actually received.

If to Third Party:

_____

_____

_____

Attention: _____

If to UPMC:

Office of Patient and Consumer Privacy

200 Lothrop Street

Pittsburgh, PA 15213

11.9. Governing Laws. Since UPMC's commitments regarding the treatment of Confidential Information are specific to the state in which services are rendered, applicable federal laws and the laws of such state will govern the parties obligations and commitments with respect to Confidential Information.

11.10. Captions; Amendment; Successors. Captions contained in this Agreement are for convenient reference only. This Agreement shall inure to the benefit of and be binding upon UPMC and Third Party and their respective successors and assigns.

11.11. Survival. Third Party's obligations regarding the use, access, disclosure, and protection of UPMC Confidential Information shall indefinitely survive the termination of this Agreement.

[REMAINDER OF PAGE LEFT INTENTIONALLY BLANK]

IN WITNESS WHEREOF, intending to be legally bound hereby, UPMC and Third Party have executed this Agreement as of the date and year first above mentioned.

UPMC

Name: John P. Houston, Esq.
Title: Vice President, Privacy and Information Security & Associate Counsel

Third Party

By: _____

Name: _____

Title: _____

Date: _____