DATA SHARING AGREEMENT

This Data Sharing Agreement v3.0 (the "**Agreement**") is entered into by and between _____("**Data Host Institute**" or "name of institution") on one hand and on the other hand, _____ ("**Network Participant**"). Data Host Institute and Network Participant are each referred to herein as a "**Party**" and, collectively, as the "**Parties**."

WHEREAS, Data Host Institute is participating as a lead or participating site for the Maternal and Pediatric Precision in Therapeutics Hub ("MPRINT") (the "Project") to work with data, to connect with outside research partners, and to support data infrastructure;

WHEREAS, as part of managing and coordinating this Project, Data Host Institute may issue queries for, and collect data from, all participants in the Project (collectively "Network Participants") to facilitate the conduct of research in accordance with policies established for the Project ("MPRINT Policies");

WHEREAS, Network Participant may, at its discretion, respond to queries as part of its participation in this Project and send data via the data hosting service provider for retrieval by Data Host Institute and subsequent transfer to other approved Network Participants in the Project (as defined below);

WHEREAS, the Parties seek to enter into this Agreement in order to clarify their responsibilities with respect to the sharing of data by Network Participant.

NOW, THEREFORE, the Parties agree to the following.

I. Definitions

Except as otherwise expressly provided herein, terms used in this Agreement shall be defined as follows:

a. **Aggregate Data:** Aggregated, De-identified, non-Individual Level Data across specified strata of individuals. For example, counts of patients within a stratum that includes a particular age group, gender and diagnosis.

b. **Authorized Users**: Individuals associated with and selected by Network Participant who have been granted access to the Secure File Transfer Method in accordance with minimum standards developed by Data Host Institute. Authorized Users are limited to individuals working for U.S. entities and physically located within the U.S.

c. **Breach**: The acquisition, access, use or disclosure of PHI (as defined herein) in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of PHI, and subject to the exceptions set forth in 45 CFR 164.402.

d. **Confidential State or Federal Agency Data**: Data originating from a state or federal agency provided for use by Network Participant via separate agreement that is deemed confidential by State or Federal statue or regulation.

e. Data: Network Participant Data in the possession of the Data Host Institution.

f. **De-identified Data**: This term has the meaning ascribed to it in the HIPAA Privacy Rule at 45 CFR Section 164.514(a). Processes for de-identifying data are set forth in 45 CFR Section 164.514(b) of the HIPAA Privacy Rule.

g. **HIPAA**: The Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and all implementing regulations, as may be amended from time to time.

h. **HIPAA Privacy Rule**: The HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164), as may be amended from time to time.

i. **HIPAA Security Rule**: The HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), as may be amended from time to time.

j. **Individual Level Data**: Data that are not Aggregate Data. Individual Level Data contain information that is specific to individual patients. Individual Level Data may or may not be De-Identified Data.

k. **Limited Data Set**: This term has the meaning ascribed to it in the HIPAA Privacy Rule at 45 CFR Section 164.514 (e).

l. **Minimum Necessary**: This term has the meaning ascribed to it in the HIPAA Privacy Rule at 45 CFR Section 164.514(d).

m. **Network Participant Data**: Data generated, collected, processed, maintained, held or stored by Network Participant locally in connection with its participation in MPRINT, which comprises only a relatively small fraction of institutional data, and which may be transferred to the Data Host Institute in response to a Query.

n. **Query ("Query")**: A query of Network Participant Data sent from Data Host Institute using a Secure File Transfer Method.

o. **Protected Health Information ("PHI")**: This term has the meaning ascribed to it in the HIPAA Privacy Rule at 45 CFR Section 160.103.

p. **Approved Entity**: An individual or institution who is approved to receive data as part of this project. Approved Entities are limited to individuals working for U.S. entities and physically located within the U.S

q. **Secure File Transfer Method**: A method to securely transfer (i) Queries from the Data Host Institute to the Network Participant, and/or (ii) Network Participant Data from the Network Participant to Data Host Institute in response to a Query. This method will be specified for each Query and Data transfer by Data Host Institute, subject to Network Participant's approval, and may include PopMedNet, sFTP or another secure file transfer method.

r. **Unsecured PHI**: PHI that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5, as the term is defined in 45 CFR 164.402.

II. Responsibilities of Data Host Institute

a. Analytic queries

i. Analytic Queries. Data Host Institute shall issue queries of Network Participant Data seeking return of certain Data in order to prepare for research (each, a "**Pre-Research Query**") or for research purposes (each, a "**Research Query**" and, together with "**Pre-Research Query**", the "**Analytic Queries**"). Each Analytic Query will specify the Data requested, a summary of the objective of the Query and the proposed schedule for return of the Data to Data Host Institute. The Data Host Institute shall work with the entity requesting the Analytic Queries ("Requestor") (and Network Participant) to assure that only the Minimum Necessary amount of Data is requested by an Analytic Query. When applicable, Data Host Institute shall confirm necessary approvals (including approved IRB waivers of the individual authorization requirement and data use agreements, as applicable) are in place prior to transfer of Data received by Data Host Institute from Network Participant to Requestor. Network Participant, Data Host Institute and/or the Requestor may rely on the receipt of another's IRB approval,but is not required to do so. IRB approval for the transfer of Data may be obtained by the Parties and/or the Requestor separately. Relevant Data shall flow as outlined in the "Data Flow Description Documentation" attached hereto as Exhibit A. Pursuant to Section III.a.i (Participation in a Query), participation in Analytic Queries is at the discretion of Network Participant.

ii. Analytic Queries Seeking Return of Aggregate Data. Analytic Queries can seek return of Aggregate Data (for example, counts of individuals meeting certain criteria, or counts of exposures, outcomes or exposure/outcome pairs). At the election of Network Participant, Aggregate Data may be transferred from Network Participant to Data Host Institute with or without the prior execution of a data use agreement between the Requestor and Data Host Institute in the same form as the Data Use and Transfer Agreement attached hereto as Exhibit B, with notice of the same provided by Data Host Institute to Network Participant. Network Participant shall provide prompt notice to Data

Host Institute of its election to ensure Data Host Institute's compliance. Aggregate Data is, by definition, De-Identified Data.

iii. Analytic Queries Seeking Return of De-Identified Individual Level Data. Data Host Institute can issue Queries seeking return of De-Identified Individual Level Data. At the election of Network Participant, De-Identified Individual Level Data will be transferred from Network Participant to Data Host Institute with or without the prior execution of a data use agreement between the Requestor and Data Host Institute. In the event a data use agreement is executed, it will be in the same form as Exhibit B, and notice of the same will be provided by Data Host Institute to Network Participant. Network Participant is not required to transfer Individual Level Confidential State or Federal Agency Data (original or derivative data files) originating from a data use agreement with a state or federal agency if prohibited by that data use agreement.

iv. Analytic Queries Seeking Return of a Limited Data Set. Data Host Institute can issue Queries of Network Participant Data seeking return of a Limited Data Set as part of a MPRINT Query for an approved study. Pursuant to Section III.a.iii (Rights to Share Data) of this Agreement, Network Participant will ensure appropriate permissions and approvals are in place prior to the transmission of any Limited Data Set containing Protected Health Information, and Data will be transferred from Network Participant to Data Host Institute only after Data Host Institute has notified Network Participant that it has executed a data use agreement with Requestor in the same form as Exhibit B.

v. Use Limitation. Data Host Institute shall use Network Participant Data returned from an Analytic Query only (a) in accordance with the Data use specifications and information required in the Query request, (b) as allowed by the informed consent provided by patients, if applicable, and (c) in accordance with the terms of this Agreement. Data Host Institute may only disclose Data to Requestor in accordance with the appropriate IRB's approval as necessary to comply with law and regulation. Data Host Institute will not use or further disclose such Data, except as permitted hereunder or as otherwise required by law. Data Host Institute agrees to enter into agreements with Requestors in the form as contained in Exhibit B, to ensure that Requestor's use or disclosure of the Data provided in response to an Analytic Query is only for the purpose(s) of the Data use specifications information required in the Query request and only in compliance with the terms contained in this Agreement and the requirements set forth in Exhibit B.

vi. Retention. Data Host Institute shall retain Network Participant Data returned from an Analytic Query only for as long as necessary to fulfill the purpose of the Query and in any event, no longer than the Retention Period to allow re-

use of the Data consistent with the justification in the study protocol and/or the Query. During the Retention Period, Data Host Institute shall not store the Data other than as provided herein, and no Data shall be maintained outside of the U.S., either by Data Host Institute itself, or at any off-shore data service provider facility, without first providing thirty-five (35) days advance written notice to Network Participant. At the end of the Retention Period, Data Host Institute shall destroy the Data in accordance with the HIPAA Security Rule. Data Host Institute shall require Requestors to comply with substantially similar retention terms as those contained herein.

b. Test Queries. From time to time, Data Host Institute may issue test Queries (each a "**Test Query**") of Network Participant Data in advance of an Administrative or Analytic Query seeking return of either Aggregate Data, a Limited Data Set for the purpose of beta testing the operability of software programs used in connection with MPRINT and other MPRINT Query enhancements. Depending on the type of Data requested for return, each Test Query shall be subject to the same requirements as set forth above for Analytic Queries, as applicable. With approval from Data Host Institute , Network Participant may elect to return Data containing only simulated Protected Health Information ("**Dummy Data**") in response to a Test Query. In such a case, the Dummy Data shall not be subject to the requirements set forth in this Agreement or HIPAA. Pursuant to Section III.a.i (Participation in a Query), participation in Test Queries is at the discretion of Network Participant.

    i. Retention Period. In the event that Network Participant returns Network Participant Data in a form other than Dummy Data in response to a Test Query, Data Host Institute shall retain such Data only for as long as necessary to fulfill the purpose of the Query, and in any event, no longer than the Retention Period. During the Retention Period, Data Host Institute shall not store the Data other than as provided herein, and no Data shall be maintained outside of the U.S., either by Data Host Institute itself, or at any off-shore data service provider facility, without first providing thirty-five (35) days advance written notice to Network Participant. At the end of the Retention Period, Data Host Institute shall destroy the Data in accordance with the HIPAA Security Rule. Data Host Institute shall require Requestors to comply with substantially similar retention terms as those contained herein.

c. Secure File Transfer Method. Data Host Institute must submit all Queries covered by this Agreement to Network Participant through a Secure File Transfer Method.

d. Security of Network Participant Data.

    i. Compliance with the HIPAA Security Rule. Data Host Institute agrees to adopt and use physical, administrative and technical safeguards consistent

with the HIPAA Security Rule to protect any Network Participant Data received from Network Participant pursuant to this Agreement, and to use all reasonable measures, including encryption, to prevent any use or disclosure of Data other than as provided by this Agreement.

ii. Breach. In the event of a known or suspected Breach of Unsecured PHI by Data Host Institute that would trigger notification to individuals or regulators if Data Host Institute were a HIPAA covered entity or business associate (as those terms are defined in HIPAA), or in the event of any use or disclosure of Network Participant Data other than as permitted by this Agreement, Data Host Institute shall notify Network Participant, Network Participant's Authorized User(s) and the Data Host Institute in writing (e.g., email or letter) as soon as possible (and no later than 10 business days) after discovery of the known or suspected Breach or any other use or disclosure of Data other than as permitted by this Agreement. A known or suspected Breach or any other use or disclosure of Data other than as permitted by this Agreement shall be treated as discovered by Data Host Institute as of the first business day on which such known or suspected Breach or other impermissible use or disclosure of Data is known to Data Host Institute or, by exercising reasonable diligence, would have been known to Data Host Institute. Data Host Institute shall provide reasonable assistance to Network Participant and cooperate with Network Participant's implementation of HIPAA's risk assessment process outlined in the HIPAA Breach Notification Rule at 45 CFR §§ 164.400-414. Data Host Institute agrees to take reasonably appropriate steps to prevent further unauthorized disclosure, to investigate and mitigate the Breach or other use or disclosure not permitted by this Agreement, and to reasonably cooperate with Network Participant as it develops any notifications to individuals, regulators or the media that are either required by law or Network Participant policy.

iii. Authorized User(s). Data Host Institute shall provide log-in credentials to Network Participant's Authorized User(s) for the Secure File Transfer Method and shall monitor and maintain a record of access of Network Participant's Authorized User(s). In the event Network Participant changes its Authorized User(s), Network Participant must provide written notice to Data Host Institute, and Data Host Institute shall invalidate the previous Authorized Users' credentials and issue new, distinct credentials to the new Authorized User(s).

e. Network Participant Data Integrity. Once Data Host Institute receives Network Participant Data from Network Participant, Data Host Institute is responsible for assuring that the Data have not been altered or destroyed in an unauthorized manner ("**Integrity**," as such term is defined in HIPAA).

f. Network Participant Identification. Each Query will specify how and/or if Network Participant will be identified to the Requestor. In general, responses to

Queries will contain only Network Participant's arbitrary identifier and not its name or other identifying information, except when Network Participant Data is shared with other MPRINT participants for network transparency and opportunities to identify areas to enhance Data quality, or when expressly authorized by Network Participant. Network Participant may also request additional restrictions aimed at preserving confidentiality pursuant to Section III.g (Network Participant Data Confidentiality) below, and Data Host Institute shall comply with such requests where feasible. Data Host Institute will notify Network Participant if Data Host Institute believes compliance with a requested restriction is not feasible. The Parties will then use good faith efforts to resolve the issue. For clarity and avoidance of doubt, nothing in this Section prohibits Network Participant from withdrawing its participation in a MPRINT Query if the issue is not resolved.

g. No Re-Identification. Except with the express, written permission of Network Participant and IRB approval, Data Host Institute agrees not to re-identify or attempt to re-identify individuals whose information is contained in Aggregate Data, a Limited Data Set or De-identified Data returned to Data Host Institute in response to a Query. Data Host Institute shall not attempt to contact any patient whose information is provided hereunder.

h. Employees and Representatives. Data Host Institute shall assure that its employees and representatives comply with the terms and conditions of this Agreement and assure that its agents and subcontractors to whom the Data Host Institute provides Network Participant Data agree in writing to comply with the same restrictions and conditions that apply to Data Host Institute hereunder.

III. Responsibilities of Network Participant

a. Local Obligation and Authority.

i. Participation in a Query. Network Participant retains discretion over whether it will participate in any Query from Data Host Institute. Such Network Participant is obligated to ensure that its participation in any Query from Data Host Institute is consistent with its own policies.

ii. Network Participant Data Security and Integrity. Network Participant is solely responsible, up to the point when Network Participant initiates transmission in response to a Query by Data Host Institute, for the privacy and security and Data Integrity (as such term is defined in HIPAA) of Network Participant Data. Network Participant shall appoint Authorized User(s) and shall be solely responsible for said Authorized Users' conduct with respect to performing activities related to this Agreement.

iii. Rights to Share Network Participant Data. Network Participant is solely responsible for ensuring that it has all necessary rights, approvals and

consents, where applicable, to disclose Network Participant Data through the Secured File Transfer Method.

iv. Withdrawal of Response. Once Network Participant Data are transmitted to Data Host Institute, such Data may only be removed from a report via a written request by the Network Participant before a report of findings is submitted back to the Requestor.

b. Analytic Query Response. For Analytic Queries in which Network Participant chooses to participate, Network Participant shall return Network Participant Data in accordance with the specifications of the Query.

c. Test Query Response. For Test Queries in which Network Participant chooses to participate, Network Participant shall return Network Participant Data or, with prior approval from Data Host Institute, may elect to return Dummy Data in accordance with the specifications of the Query.

d. Review of Results; Low Cell Counts. For MPRINT Queries in which Network Participant chooses to participate Network Participant shall return low cell counts of Network Participant Data so that accurate counts of the availability of MPRINT's total results can be obtained. In the event that Network Participant returns cell counts <11, Data will be masked and aggregated with Data returned from other MPRINT participants before it is shared with a Requestor.

e. Use of MPRINT's Secure File Transfer Method. For MPRINT Queries in which Network Participant chooses to participate, Network Participant must respond to such MPRINT Queries using the specified Secure File Transfer Method. Network Participant assumes no responsibility or liability for the availability, operation or maintenance of the specified Secure File Transfer Method.

f. Network Participant Data Confidentiality. Network Participant, in preparing a response to an Administrative, Matching Assessment, Analytic or Test Query, may require that reports, descriptions or other materials created by MPRINT or a Requestor from its Network Participant Data not describe institution-level results if Network Participant believes it would be possible to identify its organization through specific characteristics of the populations or practice patterns. However, Network Participant acknowledges that any such requirements may preclude Network Participant's participation in a particular Query.

IV. Term and Termination

a. Term. This Agreement shall become effective on the date of the last signature below (the "**Effective Date**") and shall expire on December 31, 2027 unless renewed by mutual agreement of the Parties.

b. Termination.

i. Termination by Network Participant. This Agreement shall automatically terminate immediately upon Network Participant's written notice to Data Host Institute of its intent to end its participation in this project.

ii. Termination by a Coordinating Center. MPRINT may withdraw as a Party from this Agreement if that Party ceases to serve as a coordinating center by providing written notice to Network Participant and the other non-terminating Party. Such withdrawal shall become effective as of the date of the terminating Party's notice, and the Agreement shall remain in full force and effect as it relates to Network Participant and the other non-terminating Party.

iii. Termination by Any Party. Network Participant or Data Host Institute may terminate this Agreement with or without cause upon thirty (30) days prior written notice to the other Parties.

c. Survival. The obligations of the Parties set forth in the following sections shall survive termination of this Agreement: within Section II (Responsibilities of Data Host Institute), subsections a.iv (Use Limitation), a.v (Retention), b.v (Use Limitation), b.vi (Retention), e.i (Compliance with the HIPAA Security Rule), e.ii (Breach), f (Network Participant Data Integrity), and h (No Re-Identification); within Section III (Responsibilities of Network Participant), subsection a.iv (Withdraw of Response); within Section IV (Term and Termination), subsection c (Survival); and within Section VI (Miscellaneous), subsections a (Indemnification; Limitation of Liability; and Insurance OR Liability; Limitation of Liability; and Insurance) and, as applicable, b (Network Participant Institutional/State Requirements).

V. Amendment.

a. Changes. From time to time, any Party may need to amend this Agreement to respond to changes in applicable law. Any such amendments shall take effect upon the sooner of the effective date of the change precipitating the amendment or thirty (30) days after notice by one Party to the others of the need for the amendment, and unless otherwise required by such change, shall only apply to Queries and transfers of Network Participant Data made after the time the change becomes effective. In the event that Network Participant disagrees any such amendment, it may terminate this Agreement upon written notice to the other Parties in accordance with Section IV.b (Termination).

b. Other Amendments. Except as provided in Section V.a, (Changes) the Parties may amend this Agreement only by a written agreement signed by all Parties.

VI. Miscellaneous

[Alternate language options: Each Network Participant should insert one of the following two bracketed Options to appear as Section VI.a.]

[Option 1]

a. Indemnification; Limitation of Liability; and Insurance.

i. To the extent permitted under applicable law, each Party (the "**Indemnifying Party**") will indemnify, defend and hold harmless the other Parties and any of their affiliates, and their respective trustees, officers, directors, employees and agents ("**Indemnitees**") from and against any third-party claim, cause of action, liability, damage, cost or expense (including, without limitation, reasonable attorney's fees and court costs) arising out of or resulting from negligence, willful misconduct or breach of this Agreement on the part of the Indemnifying Party or any employee, subcontractor, agent or person under the control of the Indemnifying Party. Notwithstanding the foregoing, the Indemnifying Party shall have no obligation to the extent of the other Parties' negligence, willful misconduct or breach of this Agreement. Notwithstanding any other terms or conditions of this Agreement, no state agency or corporation deemed to be nonprofit under the laws of its jurisdiction shall be deemed to waive any privileges or immunities that might be available to it under applicable law.

ii. Except for any such damages arising from breach of a Party's indemnification obligations under this Section, under no circumstances will any Party be liable to another Party for any indirect or consequential damages of any kind, including lost profits (whether or not the Parties have been advised of such loss or damage) arising in any way in connection with this Agreement.

iii. Each Party shall maintain in force at its sole cost and expense with reputable insurance companies, insurance of a type and in an amount reasonably sufficient to protect against liability hereunder. In addition to such insurance and/or in the alternative, a Party may maintain a program of self-insurance to protect against the same. Each Party shall have the right to request the appropriate certificates of insurance from the other Parties for the purpose of ascertaining the sufficiency of such coverage. Notwithstanding any other terms or conditions of this Agreement, no state/federal public institution that is an instrumentality of a state/federal government shall be required to comply with the insurance requirements of this Section so long as such institution relies on the applicable law of its state/federal jurisdiction to protect and limit its liability as an instrumentality of such state/federal government.

[Option 2]

a. Liability; Limitation of Liability; and Insurance.

i. Each Party shall be responsible for its own negligent acts and omissions under this Agreement.

ii. Under no circumstances will any Party be liable to another Party for any indirect or consequential damages of any kind, including lost profits (whether or not the Parties have been advised of such loss or damage) arising in any way in connection with this Agreement.

iii. Each Party shall maintain in force at its sole cost and expense with reputable insurance companies, insurance of a type and in an amount reasonably sufficient to protect against liability hereunder. In addition to such insurance and/or in the alternative, a Party may maintain a program of self-insurance to protect against the same. Each Party shall have the right to request the appropriate certificates of insurance from the other Parties for the purpose of ascertaining the sufficiency of such coverage. Notwithstanding any other terms or conditions of this Agreement, no state/federal public institution that is an instrumentality of a state/federal government shall be required to comply with the insurance requirements of this Section so long as such institution relies on the applicable law of its state/federal jurisdiction to protect and limit its liability as an instrumentality of such state/federal government.

[End alternate language section]

b. Network Participant Institutional/State Requirements. The Parties acknowledge and agree that Network Participant and this Agreement may be subject to certain institutional and/or state law requirements which must be included herein. Accordingly, the Parties agree as follows:

i. *[Insert title of requirement (underlined) with requested language OR mark* "Reserved"].

c. No Warranties. All Network Participant Data sent to Data Host Institute pursuant to this Agreement by Network Participant is provided "AS-IS." Network Participant expressly disclaims any and all warranties regarding such Data s pursuant to this Agreement, including, without limitation, warranties of accuracy, completeness, fitness for a particular use or any other express or implied warranties.

d. Relationship of the Parties. Nothing contained in this Agreement shall constitute, or be construed to create, a partnership, joint venture, agency or other relationship between the Parties other than that of independent contractors to the Agreement.

The Parties acknowledge that Data Host Institute is not a business associate, as that term is defined in the HIPAA regulations, of Network Participant.

e. Assignability. In no event shall any Party assign any of its rights, powers, duties or obligations under the Agreement without the written consent of the other Parties, which shall not be unreasonably withheld, and any attempt to do so shall be void.

f. Severability. Any provision of this Agreement that proves to be invalid, void or illegal ("**Invalid**") shall in no way affect, impair or invalidate any other provision of the Agreement and such other provisions shall remain in full force and effect, unless the declaration of invalidity materially (i) impairs the ability of a Party to perform its obligations, (ii) impairs the benefits received by a Party, or (iii) adversely affects a primary purpose of the Agreement (collectively, "**Impairment**"). If an Invalid provision causes Impairment, the Parties agree to cooperate in making a good faith effort to replace such provision with one that is valid and that will achieve the original intent of the Parties. If the Parties are unable to agree upon a replacement provision when an Impairment results from an Invalid provision, then a Party may terminate its participation in the Agreement upon written notice to the other Parties in accordance with Section IV.b (Termination).

g. Enforceability. The Agreement shall be enforceable only by the Parties hereto, and their successors pursuant to a valid assignment pursuant to this Agreement. In all other respects, this Agreement is not intended, nor shall it be construed, to create any third party beneficiary rights.

h. Notices. Any notices (except those required under Section II.e.ii (Breach) to individuals) shall be deemed effectively given when personally received by the intended recipient, and shall be sent by (a) email transmission with non-automatic acknowledgment from the recipient indicating receipt; (b) express or overnight courier with proof of delivery; or (c) United States Postal Service, certified or registered mail with signed return receipt, addressed to the person or persons identified herein.

For Data Host Institute
[Name of Organization]
Attn: [Contact Person Name]
[Contact or Organization Address]

For Network Participant:

_____
_____
_____

h. Signing Authority. Each person signing the Agreement hereby represents that he or she is authorized to enter into the Agreement on behalf of the Party for which he or she is signing.

i. Counterparts and Electronic Signature. This Agreement may be executed in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same Agreement. Delivery of an executed signature page to the Agreement by facsimile transmission or PDF will be as effective as delivery of a manually signed counterpart.

j. Entire Agreement. This Agreement constitutes the full and complete understanding of the Parties hereto with respect to the subject matter hereof and supersedes all prior understandings and agreements with respect to such subject matter including, as applicable, the MPRINT Data Sharing Agreement previously executed by the Parties, which is hereby terminated as of the date of full execution of this Agreement. Any handwritten modifications to this Agreement shall be null and void unless such modifications are initialed by all Parties.

[NEXT PAGE IS SIGNATURE PAGE]

In witness whereof, Data Host Institute and Network Participant have entered into this Agreement as of the Effective Date.

Data Host Institute

By:_____

Name:

Title:

Network Participant:

[NAME]

By:_____

Name: _____

Title: _____

[Optional IRB signature block added if necessary and required by Network Participant. Otherwise, please delete.]

Read and Acknowledged by Network Participant's Institutional Review Board:

[IRB NAME]

By:_____

Name: _____

Title: _____

Exhibit A

Data Flow Documentation

This Data Flow Documentation ("**Documentation**") describes and illustrates how data flows through the MPRINT Hub in response to a research question (a MPRINT Query) from the time a Query is sent from the Data Host Institute to Network Participants, until the time data resulting from the Query is released by Network Participants and delivered to Requestor by Data Host Institute. Only the physical aspects of the movement of data through the network are addressed is this Documentation, but not the legal, administrative or regulatory requirements for data transfer or use of the data by the Requestor.

Please note that unless otherwise specified, all capitalized terms used in this Documentation have the same meaning assigned to them as in the Data Sharing Agreement to which it is attached.

I. DESCRIPTION.

A. MPRINT Data Network Architecture. The MPRINT data network uses a distributed architecture in which there is no central data repository. Instead, networks must standardize locally-held electronic health data in accordance with the MPRINT "Common Data Model". Queries are programmed by Data Host Institute, and distributed to networks using a Secure File Transfer Method.

B. MPRINT Common Data Model. In the MPRINT Common Data Model, which is based on the FDA Sentinel Initiative Common Data Model (www.sentinelsystem.org), each partner network securely collects and stores data behind its own firewall, and maps it to the same consistent format (i.e., with the same variable name, attributes, and other metadata). It leverages standard terminologies and coding systems for healthcare (including ICD, SNOMED, CPT, HCPSC, and LOINC) to enable interoperability with, and responsiveness to, evolving data standards.

C. Issuing a Query. Data Host Institute will issue any Query and send these to the network through a Secure File Transfer Method after its review and approval of a Requestor's request.

D. Response to a Query. A Network Participant receives all Queries through a Secure File Transfer Method. A Network Participant may respond to queries by returning their data through the Secure File Transfer Method, but can choose to not response to any Query. Data is not sent directly to a Requestor from a Network Participant in response to a Query, but is first retrieved by Data Host Institute from the Secure File Transfer Method.

E. Transfer of Data and Delivery to Requestor. After Data Host Institute retrieves all Network Participant Data, the data is then transferred to the Requestor following execution of a HIPAA-compliant data use agreement, as applicable.

EXHIBIT B

DATA USE AND TRANSFER AGREEMENT

This Data Use and Transfer Agreement ("**Agreement**") is entered into as of the date of the last signature below ("**Effective Date**") by and between:

or

☐ [Name of Organization]

and

_____[Name of contracting party]____ ("**RECIPIENT**")

([Name of Organization] and RECIPIENT together referred to herein as the "**Parties**").

WHEREAS, in its role as Data Host Institute, Data Host Institute is in possession of certain Network Participant Data (as defined below) received from Network Participant(s) (as defined below) who have agreed to share their patient health information in response to a MPRINT Query pursuant to the terms of a three-party Data Sharing Agreement ("**DSA**") entered into by and among Data Host Institute and Network Participants;

WHEREAS, RECIPIENT may be a Network Participant or from an institution or entity external to MPRINT;

WHEREAS, RECIPIENT has, where required by law or institutional policy, requested and received approval from its Institutional Review Board ("**IRB**") for receipt of patient health information for the following purpose (the "**Purpose**"):

Research Project Name: _____ (the "**Project**")
Protocol #: _____
IRB #: _____ *Approval Date:* _____
Principal Investigator: _____
Purpose (insert meaningful description of data requested, use and research justification): ____
_____
_____
_____
_____

WHEREAS, Data Host Institute shall disclose Network Participant Data (as defined below) to RECIPIENT, subject to the terms and condition contained in this Agreement, in a form identified below (all forms referred to hereinafter as "**the Data**"):

☐ a De-identified Data set containing no individual patient identifiers constituting, which is not subject to the requirements of HIPAA (as defined below); or

☐ a Limited Data Set of Protected Health Information ("**PHI**") (as further defined below), so that RECIPIENT is a "Limited Data Set Recipient" as defined in HIPAA, and is therefore subject to the requirements of HIPAA; or

☐ a Data set containing more PHI than permitted in a Limited Data Set under HIPAA, and is therefore subject to the requirements of HIPAA.

NOW, THEREFORE, the Parties agree to the provisions of this Agreement in order to address the requirements of HIPAA, to protect the interest of both Parties, and to comply with the terms of the DSA and MPRINT Policies.

1. **DEFINITIONS**. Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in HIPAA. In the event of any inconsistency between the provisions of this Agreement and mandatory provisions of HIPAA, as amended, the HIPAA provisions shall control. Where provisions of this Agreement are different from those provided in HIPAA, but are permitted by HIPAA, the provisions of this Agreement shall control. The following terms shall have the meaning ascribed to them below and in the DSA:

    a. **Breach**: The acquisition, access, use or disclosure of PHI (as defined herein) in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the PHI, and subject to the exceptions set forth, in 45 CFR 164.402.

    b. **HIPAA**: The Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act (HITECH), and all implementing regulations, as may be amended from time to time.

    c. **HIPAA Privacy Rule**: The HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164), as may be amended from time to time.

    d. **HIPAA Security Rule**: The HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), as may be amended from time to time.

    e. **Network Participant**: An individual site or organization that is a party to the three-party DSA by and amongst Data Host Institute, which contributes Network Participant Data to MPRINT at its discretion in response to a query by Data Host Institute for permitted use by a Requestor.

    f. **Network Participant Data ("Data")**: Data generated, collected, processed, maintained, held or stored by Network Participant locally in connection with its participation in MPRINT, which may be transferred to Data Host Institute in response to a MPRINT Query.

g. **MPRINT Query**: A query of Network Participant Data that uses a Secure File Transfer Method.

h. **Protected Health Information ("PHI")**: Individually identifiable health information as more fully defined in the HIPAA Privacy Rule at 45 CFR Section 160.103.

i. **Requestor**: An individual who may or may not be affiliated with Network Participant or another participant in MPRINT, but who is authorized by a Network Participant or another participant in MPRINT to develop and submit a request for a MPRINT Query and receive the results.

j. **Unsecured PHI**: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5, as the term is defined in 45 CFR 164.402.

2. **HIPAA APPLICABILITY**. The Parties acknowledge and agree that if the Data contains no PHI, then its use and disclosure is not subject to the requirements of HIPAA. The Parties further acknowledge and agree that if the Data contains PHI, then its use and disclosure is subject to the applicable requirements of HIPAA.

3. **APPROVAL CERTIFICATION**. As applicable, and to the extent required by law and the institutional policy of the Network Participant(s) from whom the Data originated, each Party certifies that it has obtained IRB approval for RECIPIENT's right to use and disclose the Data provided to RECIPIENT MPRINT for the Purpose described herein, and/or that such IRB approval is based on valid individual subjects' authorization or a waiver of the authorization requirement. RECIPIENT accepts responsibility and liability for any unauthorized disclosure of the Data following RECPIENT's receipt of such Data pursuant to this Agreement.

4. **PERMITTED USE**. Data Host Institute will provide the Data to RECIPIENT in the form identified herein, as either a De-identified Data Set, a Limited Data Set, or a Data set containing more PHI than permitted in a Limited Data Set, as indicated above. RECIPIENT agrees that it shall treat the Data in confidence and shall avoid disclosure of the Data to any other person, firm or corporation unless necessary to complete the Purpose. RECIPIENT shall have the right to use the Data only for its analysis related to the Project and not for any other purpose, including commercial use or otherwise. The Data may be shared with RECIPIENT's Project Team Members, or it employees, agents and subcontractors only on a need-to-know basis, and shall not be shared with any third party without the express written prior consent of Data Host Institute. In the event RECIPIENT discloses the Data to its authorized agents or subcontractors who have a need to use and access the Data to enable RECIPIENT to fulfill the Purpose, RECIPIENT will ensure that such agents or subcontractors enter into an agreement with no less restrictive terms than those contained herein including, but not limited to, those addressing data privacy, security, and breach notification.

5. **RESTRICTIONS ON USE**. RECIPIENT agrees that the Data it receives will not be used in any manner not allowed by the informed consent and/or authorization provided by individual subjects, if applicable, or in any manner inconsistent with the Purpose, or with the terms of RECIPIENT's IRB's approval of RECIPIENT's use and receipt of the Data. RECIPIENT further agrees that it, any Project Team Members identified herein, and any other employees, agents and subcontractors to whom it discloses the Data, will not use or further disclose the Data other than as permitted by this Agreement, or as otherwise required by law or regulation. RECIPIENT shall not, or attempt

to, re-identify the individuals to whom the Data pertains, or attempt to contact such individuals. RECIPIENT also shall not attempt to identify the Network Participant(s) from whom the Data originated. No license or additional rights are provided to RECIPIENT in connection with the Data under any patent applications, copyrights, trade secrets or other proprietary rights of MPRINT, Data Host Institute or the Network Participants.

6. **DATA SECURITY**. Regardless of whether the Data contains PHI, all Data disclosed by Data Host Institute. Data Host Institute shall be maintained by RECIPIENT under appropriate administrative, physical and technical safeguards, including encryption while in transit, to protect the confidentiality and integrity of the Data, and its electronic and physical security from misuse or inappropriate disclosure. RECIPIENT shall use all reasonable measures to prevent any use or disclosure of the Data other than as provided in this Agreement, and shall protect the Data in strict confidence in the same manner as it would protect its own confidential information.

7. **COMPLIANCE WITH LAWS**. RECIPIENT will ensure that the Project for which the Data is received is conducted in accordance with all federal, state, and local laws and regulations applicable to the Project, and RECIPIENT will comply with the same.

8. **REPORTING**. RECIPIENT shall promptly report to Data Host Institute any use or disclosure of the Data not provided for in this Agreement of which RECIPIENT becomes aware, regardless of whether the Data contains PHI. Data Host Institute shall promptly inform the Network Participant(s) from which such Data originated of such unauthorized use or disclosure. RECIPIENT will take reasonable steps to limit any further such use or disclosure.

9. **BREACH NOTIFICATION**. Following the discovery of a Breach of Unsecured PHI contained in the Data received from Data Host Institute, RECIPIENT shall notify Data Host Institute of such known or suspected Breach pursuant to the terms of 45 CFR § 164.410 and cooperate in Data Host Institute's and, if applicable, the Network Participant(s)' from whom the data originated, Breach analysis procedures, including risk assessment, if requested, and any mitigation processes. RECIPIENT may conduct its own risk assessment and mitigation processes, provided however, that such action doesn't conflict with or affect those of Data Host Institute. RECIPIENT understands and agrees that the Network Participant(s) from whom the Data containing PHI originated may, at its/their discretion, participate in Data Host Institute's Breach analysis procedures and risk assessment. A Breach shall be treated as discovered by RECIPIENT as of the first day on which such Breach is known to RECIPIENT or, by exercising reasonable diligence, would have been known to RECIPIENT. RECIPIENT will provide such notification to Data Host Institute and if required, RECIPIENT's IRB, without unreasonable delay and in no event later than Five (5) business days after discovery of the Breach in order for Data Host Institute to provide notice to the Network Participants of the known or suspected breach, and to comply with its contractual obligations under the DSAs with the Network Participant(s). Such notification will contain the elements required in 45 CFR § 164.410. Data Host Institute, in consultation with the Network Participant(s) from whom the Data originated, shall determine any required actions with respect to any such Breach. RECIPIENT shall cooperate and comply with such actions required by Data Host Institute and Network Participant(s) including, but not limited to, the development of any notifications to individuals, regulators or the media that are either required by law or Network Participant(s)' policy(ies).

10. **ACCESS AND INSPECTION**. From time to time upon reasonable notice, or upon a reasonable determination by Data Host Institute that RECIPIENT has breached this Agreement, Data Host

Institute may inspect the facilities, systems, books and records of RECIPIENT where and in which the Data is maintained, at mutually agreeable times, to monitor compliance with this Agreement. The fact that Data Host Institute inspects, or fails to inspect, or has the right to inspect, RECIPIENT's facilities, systems and procedures does not relieve RECIPIENT of its responsibility to comply with this Agreement, nor does Data Host Institute's (a) failure to detect or (b) detection of, but failure to notify RECIPIENT or to require RECIPIENT's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of Data Host Institute's enforcement or termination rights under this Agreement. The Parties' respective rights and obligations under this Section 10 shall survive termination of the Agreement for as long as the Data is maintained in Recipient's possession until returned to Data Host Institute or destroyed in accordance with Section 11 (Retention).

11. **RETENTION**. RECIPIENT shall retain the Data only for as long as necessary to fulfill the Purpose, and in any event no longer than five (5) years or the time required by Data Host Institute that is consistent with the research justification in the Protocol (the "**Retention Period**"). RECIPIENT shall not store the Data during the Retention Period other than as provided herein, and shall not be maintained outside of the U.S. either by RECIPIENT itself, or at any data service provider facility outside of the U.S. At the end of the Retention Period, RECIPIENT shall destroy the Data in accordance with the HIPAA Security Rule. If return or destruction is not feasible, RECIPIENT shall inform Data Host Institute of the reason it is not feasible and shall continue to extend the protections of this Agreement to such Data and limit further use and disclosure of such Data to those purposes that make the return or destruction of such Data infeasible.

12. **TERM AND TERMINATION.** This Agreement shall become effective on the Effective Date, and shall continue during the Retention Period, unless otherwise terminated by applicable law or regulation. This Agreement shall terminate upon completion of the Project. Should RECIPIENT receive Data containing PHI and commit a material breach of this Agreement, which is not cured within thirty (30) business days after RECIPIENT receives notice of such breach from Data Host Institute, then Data Host Institute will discontinue disclosure of the Data containing PHI and will report the breach to the Network Participant(s) from whom the Data originated and to the Secretary, United States Department of Health and Human Services.

13. **USE OF A PARTY's NAME**. Neither Party will use the name, trademark, logo, symbol, or other image of the other Party, a Network Participant from whom the Data originated or that Party's or Network Participant's employee or agent in advertising, publicity, or otherwise without the prior written consent of the other Party or Network Participant.

14. **NOTICE**. Any notices (except those required under Section 9 to individuals) shall be deemed effectively given when personally received by the intended recipient, and shall be sent by (a) email transmission with non-automatic acknowledgment from the recipient indicating receipt; (b) express or overnight courier with proof of delivery; or (c) United States Postal Service, certified or registered mail with signed return receipt, addressed to the person or persons identified herein.

Data Host Institute
Address and contact info

As to RECIPIENT:

_____
_____
_____
_____

15. **MODIFICATION.** Any alteration, modification, or amendment to this Agreement must be in writing and signed by both Parties.

16. **ASSIGNMENT.** This Agreement may not be assigned by either Party without the prior written consent of the other.

IN WITNESS WHEREOF, Data Host Institute entering this Agreement and RECIPIENT have signed or caused this Agreement to be signed as of the dates indicated below.

Recipient

[NAME]

By:_____

Name: _____

Title: _____

Date:_____

[Name of Organization (Data Host Institute)]

By: _____

Name: [Name of Representative]

Title: [Title of Representative]

Date:_____