DATA USE AND TRANSFER AGREEMENT

Project Title:

Recipient Institution: _____

Start Date: _____ **Recipient Principal Investigator:** _____

End Date: _____ **Fee:** $ _____

Data Set(s) Requested: **See Attachment C**

This Data Use and Transfer Agreement ("Agreement") is made and entered into by and between the Recipient Institution and Rutgers, the State University, on behalf of its Center for State Health Policy ("Rutgers") with administrative offices located at 33 Knightsbridge Road, Piscataway, NJ (each referred to herein as a "Party" and collectively as the "Parties").

1. RUTGERS MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, AS TO ANY MATTER WHATSOEVER, INCLUDING WITHOUT LIMITATION, THE OWNERSHIP, ACCURACY, RELIABILITY, MERCHANTABILITY, COMPLETENESS OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATA PROVIDED HEREUNDER OR THE SERVICES PROVIDED HEREIN.

2. The Parties agree that the documents and attachments listed below, are hereby incorporated herein by reference and the provisions of Attachment A shall apply to the Parties as the terms of this Agreement. If there is any conflict with the terms of this Agreement and any documents listed below, the terms of this Agreement shall prevail, followed by the following:

   Attachment A: Standard Terms and Conditions
   Attachment B: Data Management Plan
   Attachment C: Approved Data Request Form
   Attachment D: Research Proposal (the "Project")

3. Each Party intends that an electronic copy of its signature stored in or generated by a software application format shall be regarded as an original signature and agrees that this Agreement can be executed in any number of counterparts, each of which shall be effective upon delivery and thereafter shall be deemed an original, and all of which shall be taken to be one and the same instrument, for the same effect if all Parties hereto had signed the same signature page.

[signature page to follow]

IN WITNESS WHEREOF, the duly authorized representatives of the Parties hereby execute this Agreement as of the Start Date written above.

Rutgers, The State University, on behalf of its Center for State Health Policy

Signature: _____
Name: _____
Title: _____
Date: _____

[Insert Recipient Here]

Signature: _____
Name: _____
Title: _____
Date: _____

Recipient Investigator

Signature: _____
Name: _____
Title: _____
Date: _____

Address for Notice for Recipient

_____
_____
_____
_____
_____
E-Mail: _____

ATTACHMENT A

STANDARD TERMS AND CONDITIONS

1. This Agreement applies to the data set that RUTGERS provides to Recipient for performance of the Project, or any components thereof, ("Data" or "Project Data"), as well as any related information provided by RUTGERS, solely for use by Recipient for the Project only. The Project Data provided to Recipient by Provider will not contain personally identifiable patient information and will not include "Protected Health Information" ("PHI") as defined in 45 C.F.R. section 164.103. Recipient further agree that Project Data will not be used either alone or in conjunction with any other information, in any effort whatsoever in order to contact the individuals from which the Project Data were derived.

2. Recipient shall use and maintain the Project Data, and conduct the Project, in a manner consistent with all applicable State and Federal Laws, including all applicable data, security and privacy laws.

3. Recipient agrees to ensure that the security and privacy of information systems in which the Project Data will be stored or transmitted is aligned with the administrative, physical and technical controls and objectives, as documented in the State of New Jersey Executive Branch, Statewide Information Security Manual, posted at Statewide Information Security Manual (SISM). The SISM is derived from applicable State and federal laws; industry best practices including, but not limited to National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; NIST Special Publication 800-53, the international security and privacy practices aligned with ISO 27001 series, Center for Internet Security (CIS) Top 20 Critical Security Controls; the Cloud Security Alliance, (CSA) Cloud Controls Matrix (CCM); lessons learned; and other New Jersey State Government applicable laws and standards

4. Recipient shall notify RUTGERS within twenty-four (24) hours of discovery of any privacy or security incident. A privacy or security incident is defined as any incident that violates the privacy or security of the Project Data, including, but not limited to, any access to or sharing of the Project Data in violation of the terms of this Agreement or that has not been approved by RUTGERS. A privacy or security incident is considered "discovered" as of the first day on which the incident is known, or reasonably should have been known, to Recipient or its employees or workforce, excepting the individual committing the privacy or security incident. Any notice of a breach or unauthorized use or disclosure of unsecured Project Data shall include (to the extent reasonably known) the identification of each individual whose information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach or unauthorized use or disclosure as well as any other information that Recipient is required to include in the notice to affected individuals under (N.J.S.A. 56:8-163) either at the time of notice of the breach or unauthorized use or disclosure to RUTGERS or as promptly thereafter as information becomes available.

5. In the event of a breach of privacy or a security incident, Rutgers shall take the following steps: i) ensure that the initial notification to RUTGERS includes contact and component information; a description of the breach or loss with scope, numbers of files or records, type of equipment or media, approximate time and location of breach or loss; description of how the Project Data was physically stored, contained, or packaged (e.g., password protected, encrypted, locked briefcase,

etc.); whether any individuals or external organizations have been contacted; and whether any other reports have been filed; ii) take prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; iii) investigate the privacy or security incident and produce a written report with an initial assessment of the privacy or security incident within seven (7) working days. The report shall should include data elements involved; a description of the unauthorized persons known or reasonably believed to have improperly used or disclosed Project Data; a description of where Project Data is believed to have been improperly transmitted, sent, or used; a description of the probable cause of the privacy or security incident; a detailed corrective action plan including measures that were taken to halt and/or contain the privacy or security incident; and a determination if the privacy or security incident is a breach as defined by N.J.S.A. 56:8-161; and iv) to comply with any additional requested made by RUTGERS in response to such breach, potentially including the notification to impacted individuals.

6. The Parties acknowledge and agree that the Project Data contains sensitive information and that any inadvertent disclosure of such may cause grave or irreparable harm to the Parties or others. Recipient agrees that the Project Data will be maintained at a suitable location where appropriate physical, administrative and technical safeguards will be employed and shall not share, transmit or otherwise disclose the Project Data to any third party or any unauthorized individual within Recipient's Institution.

7. Recipient shall not request or accept receipt of the Data until Recipient has signed the Agreement and submitted approval from its Institution Review Board for performance of the Project.

8. Recipient shall not publish or disclose in any manner to the public any State Agency Data or information on individual level records or PII, statistical tables, or research results, with identifiers. Notwithstanding the foregoing, Recipient may publish results and findings with the aggregates totals from Recipient's analysis of the Project Data; so long as the aggregate findings are sufficiently large enough to prevent the identification of any individual.

9. Recipient shall restrict access to the Project Data to those individuals that are strictly necessary for the performance of the Project and that have been informed of and acknowledge the confidential nature of the Project Data and the security requirements contained herein. Specifically, Recipient shall advise its applicable employees of the confidential nature of the Project Data, the safeguards required to protect the Project Data, and the civil and criminal sanctions for noncompliance with such safeguards.

10. Recipient agrees to adequately train its employees who have access to the Project Data, on privacy and security awareness trainings, that are sufficiently thorough and current to adequately address the expected performance obligations required herein. Recipient shall maintain adequate records of these trainings, evidence of completion for each applicable employee, and shall retain the training records for a period of at least three (3) years.

11. Within thirty (30) days from the End Date, Recipient shall certify to RUTGERS, that Recipient has securely destroyed the Project Data, in a manner that renders the Project Data unreadable, indecipherable and unusable, in accordance with the National Institute of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization.

12. Recipient shall reasonably cooperate with RUTGERS and any third party designated by RUTGERS if RUTGERS or the designated third party is audited with regard to the confidentiality, security and protection of the Project Data. This includes permitting site and record inspections related to program confidentiality during regular business hours by federal or state representatives.

13. Legal title to the Project Data will remain with Provider, and the transfer of Project Data grants to Recipient no rights in the Project Data other than those specifically set forth in this Agreement. Provider grants Recipient a nonexclusive license to use the Project Data solely for the Project and the purpose of the Project.

14. It is not contemplated that any intellectual property will be developed during the performance of the Project. However, ownership of any intellectual property conceived, developed or discovered during the term of this Agreement and in furtherance of the Project, shall follow inventorship and inventorship shall be determined using principles of United Stated Intellectual Property Law.

15. Recipient agrees to submit to RUTGERS copies of all reports, publications, articles, journals or other public disclosures that reports upon or using the Project Data within 30 days of publication. Recipient shall give adequate reference to RUTGERS as the provider of the Project Data under currently generally accepted academic standards. For the avoidance of doubt, no right of manuscript approval is implied by this Section. Recipient must provide all reports as required by RUTGERS as delineated on the applicable website, as may be updated from time to time.

16. Neither Party shall use the name, insignia, trademark, trade name, logo, abbreviation, nickname, or other identifying mark or term of the other party for any purpose, except as required by law, without the prior written consent of the other party, provided however, that the parties may use the name of the other party in its routine listings of sponsored projects, as required on grant applications, and as required by scientific journals for publication.

17. Notices under this Agreement shall be in writing and sent by public courier and addressed as follows:

    To Recipient:
    Rutgers, the State University
    Attention: Research Contract Services
    33 Knightsbridge Road, 2nd Floor East
    Piscataway, NJ 08954

18. This Agreement is governed by the laws of the United States, and the State of New Jersey, excluding conflict-of-law provisions.

19. This Agreement shall remain effective until the End Date listed in the Agreement. RUTGERS may immediately terminate this Agreement with written notice to Recipient for any reason RUTGERS may desire. Termination of this Agreement shall not relieve Recipient of the obligations arising hereunder.

20. Neither party may assign or transfer this Agreement or any of the rights, duties or obligations hereunder without the prior written consent of the other party, whose consent shall not be unreasonably withheld. Any attempted assignment without such consent shall be null and void.

21. Recipient acknowledges and agrees that Recipient shall be solely liable to RUTGERS for any and all acts and omissions made by Recipient in Recipient's use, storage or stewardship of the Project Data and any breach of any term or provision herein. Recipient shall reimburse RUTGERS for any cost, liability, damage or fee incurred by RUTGERS resulting from Recipient's use, storage or stewardship of the Project Data and any breach of any term or provision herein.

ATTACHMENT B

DATA MANAGEMENT PLAN

[To Be Attached Hereafter]

DATA MANAGEMENT PLAN for iPHD Users

1. PHYSICAL POSSESSION AND STORAGE OF iPHD DATA FILES

1.1. Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).
Click here to enter text.

1.2. Describe how your organization maintains a current inventory of data files.
Click here to enter text.

1.3. Describe how your organization binds all members (i.e., organizations, individual staff) of research teams to specific privacy and security rules in using iPHD data files.
Click here to enter text.

1.4. Provide details about whom and how your organization will notify the iPHD of any project staffing changes.
Click here to enter text.

1.5. Describe your organization's training programs that are used to educate staff on how to protect data files.
Click here to enter text.

1.6. Describe the infrastructure (facilities, hardware, software, other) that will secure the iPHD data files.
Click here to enter text.

1.7. Describe the policies and procedures regarding the physical possession and storage of iPHD data files.
Click here to enter text.

1.8. Describe your organization's system or process to track the status and roles of the research team.
Click here to enter text.

1.9. Describe your organization's physical and technical safeguards used to protect iPHD data files (including physical access and logical access to the files).
Click here to enter text.

2. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

2.1. Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of iPHD data files.
Click here to enter text.

2.2. If your organization employs a data tracking system, please describe.

Click here to enter text.

2.3. Describe the policies and procedures your organization has developed for the physical removal, transport and transmission of iPHD data files.
Click here to enter text.

2.4. Describe how your organization will tailor and restrict data access privileges based on an individual's role on the research team.
Click here to enter text.

2.5. Describe the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).
Click here to enter text.

2.6. Are additional organizations involved in analyzing the data files provided by iPHD?
Click here to enter text.

If so, please indicate below how these organizations' analysts will access the data files:

- ☐ VPN connection
- ☐ Will travel to physical location of data files at requesting organization
- ☐ Request that a copy of the data files be housed at second location
- ☐ Other: Click here to enter text.

2.7. If an additional copy of the data will be housed in a separate location (including cloud-server backups), please describe how the data will be transferred to this location and identification of these additional locations. (Also, please ensure you have included information on this organization's database management under the appropriate subsections of the database management plan.)
Click here to enter text.

3. DATA REPORTING AND PUBLICATION

3.1. Who will have the main responsibility for notifying the iPHD of any suspected incidents wherein the security and privacy of iPHD data may have been compromised? Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of iPHD data.
Click here to enter text.

3.2. Explain how your organization's data management plans are reviewed and approved.
Click here to enter text.

3.3. Explain whether and how your organization's data management plans are subjected to periodic updates during the DUA period.
Click here to enter text.

3.4. Please attest to cell suppression principle of not publishing or presenting tables with cell sizes less than ten (10); and if above ten (10), you hereby agree to review the draft publication and based upon the nature and context of the work product, the numerical value is sufficiently large enough to prevent the identification of any individual. ☐ I agree.

4. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

4.1. Describe your organization's process to complete the Certificate of Disposition form and policies and procedures to dispose of data files upon completion of its research.
Click here to enter text.

4.2. Describe your organization's policies and procedures used to protect iPHD data files when individual staff members of research teams (as well as collaborating organizations) terminate their participation in research projects (which may include staff exit interviews and immediate access termination).
Click here to enter text.

4.3. Describe policies and procedures your organization uses to inform iPHD of project staffing changes, including when individual staff member's participation in research projects is terminated, voluntarily or involuntarily.
Click here to enter text.

4.4. Describe your organization's policies and procedures to ensure original data files are not used following the completion of the project.
Click here to enter text.

Complete only if collaborating organizations will have access to data files

Please note – All questions may not apply but are dependent upon the data sharing arrangement between the organizations involved in the research study.

(Information that should be indicated for <u>each</u> collaborating organization that will have access to iPHD data files.)*

A. Access to Files

1. What is the name of the collaborating organization?*
   Click here to enter text.
2. How will the collaborating organization access the iPHD data (secure VPN, a physical copy on site at the collaborating organization, traveling to the DUA holder's site, etc.)?*
   Click here to enter text.
3. Who are the researchers from the collaborating organization? Indicate if each researcher will have access to raw data, analytic files, or output with cell sizes less than 11. (*Please ensure that these individuals and data access rights are listed in the Project Staff list.*)*
   Click here to enter text.
4. What binding agreements are required of the researchers from the collaborating organization?*
   Click here to enter text.
5. What training is required of researchers from the collaborating organization?*
   Click here to enter text.
6. How will the collaborating organization notify the DUA holder of changes in staff who are participating on the research team?*
   Click here to enter text.
7. Will the researchers from the collaborating organization abide by the DUA holder's project rules or the policies of their employing organization?*
   Click here to enter text.

B. Physical Copies of Files

Please note - if the collaborating organization will maintain a separate copy of the iPHD data, the collaborating organization is required to complete a full Data Management Plan.

1. Will a separate copy of the iPHD data be housed at the collaborating organization's location?
   Click here to enter text.
2. How will the collaborating organization receive the iPHD data (shipment from the DUA holder, collaborating organization will request an additional copy directly from iPHD, the collaborating organization will transport the data, etc.)?
   Click here to enter text.

ATTACHMENT C

APPROVED DATA REQUEST FORM

[To Be Attached Hereafter]

ATTACHMENT D

RESEARCH PROPOSAL ("THE PROJECT")

[To Be Attached Hereafter]