

DATA USE AGREEMENT

Research Title: _____

**Prime Data Recipient
Institution:** _____

Start Date: _____

**Prime Data
Recipient Principal
Investigator:** _____

End Date: _____

**Anticipated Fees
(not to exceed) \$** _____

Data Set(s) Requested: See Attachment C

This Data Use and Transfer Agreement (“Agreement”) is made and entered into by and between the Prime Data Recipient Institution, and the specified Sub-Recipients (collectively, the “Recipient”) 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”) in accordance with the Statewide Integrated Population Health Data Project Act (“iPHD Project Act”), N.J.S.A. 30:4D-65 to -72, and iPHD Policies and Procedures, including those approved by the iPHD Governing Board and those that govern Rutgers’ secure and private handling of data in the iPHD Project. The specific data elements approved for use under this Agreement are identified in Attachment C,

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 “Research”)

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**

[Insert Prime Data Recipient Here]

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

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

Prime Data Recipient Investigator

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

Address for Notice for Prime Data Recipient

E-Mail: _____

[Additional Signature Pages to be appended hereafter as necessary]

ATTACHMENT A

STANDARD TERMS AND CONDITIONS

1. This Agreement applies to the iPHD Research data set that Rutgers provides to Recipient for performance of the Research, or any components thereof, (“Data” or “Research Data”), as well as any related information provided by Rutgers, solely for use by Recipient for the Research only. The Research 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 agrees that Research 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 Research Data were derived.
2. This Agreement is valid for a period starting from the Start Date and ending on the End Date. If extended access is needed, the Recipient must request the extension in writing at least 60 days prior to the DUA end date. Recipient shall use and maintain the -Research Data, and conduct the Research, 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 Research 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 Research Data, including, but not limited to, any access to or sharing of the Research 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 Research 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, Recipient 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 Research 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 include data elements involved; a description of the unauthorized persons known or reasonably believed to have improperly used or disclosed Research Data; a description of where Research 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 Research 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 Research 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 Research 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 Research; which shall contain information on any linking and/or merging of other data sources.
8. Recipient shall not publish or disclose in any manner to the public any Research 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 Research 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 Research Data to those individuals that are strictly necessary for the performance of the Research and that have been informed of and acknowledge the confidential nature of the Research Data and the security requirements contained herein. Specifically, Recipient shall advise its applicable employees of the confidential nature of the Research Data, the safeguards required to protect the Research 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 Research 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 ninety (90) days from the End Date, Recipient shall certify to Rutgers, that Recipient has securely destroyed the Research Data, in a manner that renders the Research 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 Research 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 Research Data will remain with Provider, and the transfer of Research Data grants to Recipient no rights in the Research Data other than those specifically set forth in this Agreement. Provider grants Recipient a nonexclusive license to use the Research Data solely for the Research and the purpose of the Research. Recipient acknowledges that Recipient is hereby prohibited from using the Research Data for any additional scopes or work, sub-protocols or additional research questions or aims that were not included and approved in Research description, included herein and incorporated herein as Attachment D.
14. It is not contemplated that any intellectual property will be developed during the performance of the Research. However, ownership of any intellectual property conceived, developed or discovered during the term of this Agreement and in furtherance of the Research, shall follow inventorship and inventorship shall be determined using principles of United States 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 Research Data within 30 days of publication. Consistent with generally accepted academic standards, Recipient shall give adequate reference to the iPHD and Rutgers in its capacity as manager of the iPHD Research Data. For the avoidance of doubt, no right of manuscript approval is implied by this Section; except that Rutgers may require Recipient to remove any inclusion of Research Data that does not comply with Section 8 herein. 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 Rutgers:

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. 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 liable to Rutgers for any and all acts and omissions made by Recipient in Recipient's use, storage or stewardship of the Research 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 Research Data and any breach of any term or provision herein. Furthermore, Recipient shall remain liable to Rutgers for any third party's use, storage, or destruction; so long as Recipient knowingly or unknowingly shared the Research Data with said third party. If Recipient becomes aware that Recipient has shared the Research Data with a third party that is not identified in Attachment B or Attachment D hereto, Recipient shall inform Rutgers pursuant to Section 4 herein.
22. Recipient further understands that any individual working on the Research, shall not disclose, share, transmit, or allow access to the Research Data to others or reproduce it in any form without the prior written approval from Rutgers, including the depositing of the Research Data (or any elements thereof), into a data repository, warehouse or sharing platform. Furthermore, Recipient shall not upload, share, disseminate, or make available the Research Data (or any portion thereof), to any generative artificial intelligence tools, applications or software.
23. Rutgers acknowledges and understands that merging or linking various data sources beyond Research Data, may be necessary for performance of the Research. For this agreement, merging data shall mean combining two or more data sets, with the objective of increasing the number of data entries but not materially increasing the number of unique data elements across the data entries. For this Agreement, linking data shall mean the combining of two or more data sets with the objective of increasing the number of data elements per data entry, which often requires the sharing of a common unique identifier(s) to accurately identify and expand the applicable data record.
 - a. Recipient may link or merge the Research Data with other data sets (including third party data sets), so long as such mergers and/or linkages does not materially impair Recipient's ability to adhere to and comply with the terms and conditions contained herein, and are permitted by and approved in Attachment B.
 - b. Recipient acknowledges and agrees that the more information Recipient obtains about an individual, it becomes increasingly more likely that the data can be used to identify an individual, even when direct identifiers are absent. Recipient shall use reasonable efforts to ensure that linking additional data to the Research Data does not materially increase the identifiability of any of the subject individuals. Furthermore, Recipient shall not attempt to use the Research Data to identify or attempt to identify the subject individuals except as may be reasonably required for performance of the Research. If any individual becomes identifiable through the merger or linkage of the Research Data, then Recipient shall immediately inform Rutgers, cease use of the merged and/or linked data, and shall await further instruction by Rutgers.
 - c. Recipient hereby represents and covenants that Recipient shall not merge or link, nor shall Recipient ask Rutgers to merge or link, the Research Data with any data sources until Recipient has obtained the necessary permissions or rights from the other data source's owner(s).
 - d. Recipient shall ensure that the Research Data will be removable from any linked or merged data set; and shall remove, destroy and/or delete the Research Data from any merged or linked data set upon the expiration or termination of this Agreement. Recipient shall not undertake any action that could potentially frustrate or hinder the identification and destruction of the Research Data. If in Rutgers sole discretion

Recipient fails to satisfy that all the Research Data is removed from any linked or merged data set, at Rutgers request, Recipient shall destroy any merged and/or linked data set within ten (10) days.

24. If Recipient needs an extension to the End Date or continued access to, or any portion of, the Research Data, Recipient shall notify Rutgers as soon as possible, and the parties will enter into an amendment or a revised DUTA for the continued use or access of the Research Data. Potentially permitted reasoning for the retention of the Proposal Data may include compliance with institutional policies, legal obligations, scientific transparency expectations, journal policies, or to allow for validation studies. For additional clarity:
 - a. Recipient is not permitted to retain any Research Data, in whole or in part, without a fully executed agreement to allow for such. At all times, Recipient shall continue to be a steward of the Research Data and is responsible for the management and security of the retained Research Data.
 - b. Recipient will still be prohibited from sharing, disseminating, or sharing the retained Research Data to other individuals within Recipient's organization or third parties; unless Recipient has received specific written instructions from Rutgers to the contrary.
25. After the End Date, the Research Data may not be used to answer any additional research questions, even if they are within the scope of the approved DUTA. Within 3 months following the termination or expiration of this Agreement, Recipient must destroy the Project Data, pursuant to Section 11 herein and Attachment B, from all laptops, servers and other storage devices or solutions; including hard drives or USB flash drives. After destroying the Project Data, the Recipient must confirm this action by sending a confirmation email to the Rutgers team at iphdproject@ifh.rutgers.edu. The email should state that the Project Data has been destroyed, the Recipient is no longer the custodian of, has access to, or the ability to restore any of the Project Data, and that no individual within Recipient or any third party has access to the Project Data.
26. Recipient shall ensure that prior to sharing any Project Data with a third party, that the third party is obligated to substantially and materially similar terms as contained herein, and that Recipient has the right to enforce the terms herein against the third-party.

ATTACHMENT B
DATA MANAGEMENT PLAN

[To Be Attached Hereafter]

DATA MANAGEMENT PLAN for Recipients with direct access to iPHD data

Recipient Name:

Recipient Role:

- Prime data recipient with direct access to iPHD data
- Subrecipient/collaborator with direct access to iPHD data

Please note that subrecipients/collaborators without direct access to iPHD data are not required to complete the Data Management Plan

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 or tap here to enter text.

1.2. Describe how your organization maintains a current inventory of data files.

Click or tap 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 or tap here to enter text.

1.4. Provide details about whom and how your organization will notify the iPHD of any project staffing changes.

Click or tap 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 or tap here to enter text.

1.6. Describe the infrastructure (facilities, hardware, software, other) that will secure the iPHD data files.

Click or tap here to enter text.

1.7. Describe the policies and procedures regarding the physical possession and storage of iPHD data files.

Click or tap here to enter text.

1.8. Describe your organization's physical and technical safeguards used to protect iPHD data files (including physical access and logical access to the files).

Click or tap 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 or tap here to enter text.

- 2.2. Describe how your organization will tailor and restrict data access privileges based on an individual's role on the research team.**

Click or tap here to enter text.

- 2.3. 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 or tap here to enter text.

- 2.4. Are additional organizations involved in analyzing the data files provided by iPHD (if Yes, please list the organizations, list the appropriate contact and email address)?**

Click or tap 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 or tap here to enter text.

- 2.5. 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 or tap here to enter text.

- 2.6. Please list all software solutions, vendors or other entities that will be used to store, access and analyze the iPHD data (and provide the country or origin for each).**Click or tap here to enter text.

- 2.7. If you are using any cloud storage solution, please identify which cloud solution that you will implement and confirm the physical location (by country) where the servers will be located.** Click or tap 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 or tap here to enter text.

- 3.2. Explain how your organization's data management plans are reviewed and approved.**

Click or tap here to enter text.

- 3.3. 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 policies and procedures to dispose of data files upon completion of its research.

[Click or tap 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 or tap 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 or tap 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 or tap here to enter text.](#)

5. Data Mergers and Linkages

- 5.1. Will non-iPHD data be merged or linked with iPHD data?

Yes

No Skip to next section

- 5.2. List all non-iPHD datasets approved for linkage/merger by the iPHD Governing Board.

Note: Linkages involving iPHD data require prior approval. Any linkage not explicitly disclosed in the application and approved by the Governing Board is not permitted.

[Click or tap here to enter text.](#)

- 5.3. If applicable, describe how you will link and/or merge the iPHD data with- non-iPHD data sources and the software or technical environment where the data will be linked and/or merged. *Note: Person-level linkages may not be conducted by the researcher in order to mitigate re-identification risk. Researchers are limited to conducting linkages at the ZIP-code level or higher, provided this linkage was approved by the iPHD Governing Board* [Click or tap here to enter text.](#)

- 5.4. If you are requesting linking iPHD data with non-iPHD person-level data from a previous study or a current study, please explain whether an informed consent form was deployed and whether that consent form allows for the use of personally identifying information for linking with iPHD data.

ATTACHMENT C
APPROVED DATA REQUEST FORM

[To Be Attached Hereafter]

ATTACHMENT D
RESEARCH PROPOSAL (“THE RESEARCH”)

[To Be Attached Hereafter]