

DATA SHARING AGREEMENT
Between
NEW YORK STATE OFFICE OF MENTAL HEALTH
And

This **AGREEMENT** (“Agreement”) dated _____, 20__ (“Effective Date”) is made by the New York State Office of Mental Health, with its principal offices located at 44 Holland Avenue, Albany, New York 12229 (“OMH”), and the _____, with its principal offices located at _____ (“_____”). Each party shall individually be referred to as the “Party” or collectively as the “Parties.”

WHEREAS, [BACKGROUND RECITALS, NATURE OF THE PROJECT; DEFINE “PROJECT”]

NOW THEREFORE, in consideration of the mutual promises and covenants herein set forth, the Parties agree as follows:

ARTICLE 1. TERM AND TERMINATION

- 1.1 **Term.** This Agreement shall commence as of the Effective Date and remain effective until _____, unless sooner terminated or extended by mutual agreement of the parties, in accordance with the terms and conditions stated herein.
- 1.2 **Right of Termination.** Each Party shall have the right to terminate this Agreement in whole or in part, with or without cause, upon thirty (30) days written notice to the other Party.
- 1.3 **Effect of Termination.** Upon termination of this Agreement for any reason, the confidentiality provisions set forth herein shall continue to apply to the Data (as defined below).

ARTICLE 2. PURPOSE AND SCOPE OF AGREEMENT

This Agreement sets forth the terms and conditions governing the arrangement between the Parties for granting access to and sharing the Data, as well as the procedures for security, transfer, use, retention, ownership, and confidentiality of the Data. OMH shall have access to the Data solely for the purposes of _____. The Data will be used to advance the research being conducted for this Project.

ARTICLE 3. DEFINITION AND USE OF DATA

- 3.1 “Data” shall mean _____. The Parties acknowledge and agree that _____ shall retain ownership of any rights it may have in the Data, and OMH

does not obtain any rights in the Data other than as set forth herein.

- 3.2 _____ hereby grants to OMH a limited, non-exclusive, non-transferable and revocable license to access, copy, and use the Data solely for the purposes of the Project, provided such access, copy and use of the Data is made in compliance with all applicable federal, state and local laws and regulations and the terms of this Agreement.

ARTICLE 4. DATA SECURITY, CONFIDENTIALITY AND PRIVACY SAFEGUARDS

- 4.1 **Access Authorization.** OMH shall not use the Data except as expressly authorized under this Agreement, in accordance with applicable laws, rules and regulations. The Data will be used solely to conduct the Project and solely by OMH and OMH's' faculty, employees, fellows, students, and agents that have a need to use, or provide a service in respect of, the Data in connection with the Project and whose obligations of use are consistent with the terms of this Agreement and applicable laws, rules and regulations (collectively, "Authorized Persons"). OMH agrees that it will restrict access to the Data to only those Authorized Persons who need access to the Data to perform tasks in connection with this Agreement.
- 4.2 **Safeguards to Protect the Data.** Except as authorized under this Agreement or otherwise required by law, OMH agrees at all times to retain control over the Data and shall not disclose, release, sell, rent, lease, loan, or otherwise grant access to the Data to any third party, except Authorized Persons, without the prior written consent of _____. OMH shall exercise at least the same degree of care as it uses with its own data and confidential information, but in no event less than reasonable care, to protect the Data from misuse and unauthorized access or disclosure. OMH agrees to establish appropriate administrative, technical, and physical safeguards to prevent unauthorized use of or access to the Data and comply with any other special requirements relating to safeguarding of the Data. Specifically, OMH shall take all reasonable measures to safeguard and keep the Data confidential and secure, including but not limited to (a) storing the Data in access restricted files; (b) creating a password or encryption system to obtain and restrict access to the Data; (c) keeping any hard copy versions of the Data in locked areas with restricted access; and (d) ensuring that only Authorized Persons shall have access to the Data (e) creating a firewall to protect the Data, and (f) reviewing, updating and training Authorized Persons on new security protocols in accordance with current industry standards, so that no third party, other than Authorized Persons, is allowed access to the Data.
- 4.3 **Confidentiality.**
- a. OMH shall maintain the security and confidentiality of all Data it receives in connection with this Agreement, and shall comply with all Federal, State and other governmental security requirements and all applicable laws, rules, and regulations pertaining to the confidentiality, privacy, and security of the Data received, generated, used, or held in the course of its performance under this Agreement including but not limited to, New York State Public Health Law, New York Social Services Law and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and their implementing

regulations.

- b. OMH shall not disclose, re-disclose, release, sell, rent, lease, loan, or otherwise grant access to the Data in any individually identifiable form, or in a form in which an individual could reasonably be identified, to anyone not immediately involved with the work under this Agreement without prior written approval of _____ or as permissible under applicable laws, rules, and regulations.
- c. OMH shall ensure that Authorized Persons who have access to the Data are aware of the confidentiality and security requirements and restricted use of the Data and the penalties for its unauthorized access, use or release and that Authorized Persons receive training from time to time regarding existing and updated confidential, privacy and security protocols.
- d. OMH shall ensure that all confidential information contained in or derived from the Data will remain confidential even after this Agreement expires and even when an Authorized Person is not working with the Data (including post-employment).
- e. In the event of any breach, as defined below, involving the Data or any reports, drafts, information, plans, or documents derived from the Data, furnished to, prepared by, assembled, or used by OMH, the Authorized Person, or any of OMH's employees, agents, volunteers, consultants, or vendors/contractors, OMH will (a) advise _____ of the incident within 24 hours of discovery, (b) safeguard or destroy the information that would identify the individual, (d) forward a written incident report to _____ expeditiously and not (re)disclose the identity of the individual to anyone else, (e) work with _____ security compliance officers, as applicable, to ensure all required protocols are followed related to review and follow-up actions; and (f) take reasonable steps to remediate the cause or causes of such breach, and provide written notice to _____ of such steps. For the purposes of this subsection, a breach is a situation or event which, intentionally or unintentionally, results in any of the Data being improperly released or removed from OMH's custody or where there is other evidence of willful/intentional or accidental/unintentional misuse.
- f. Notwithstanding any inconsistent provision in this Agreement, OMH shall not be liable for disclosure of the Data to the extent disclosure is required by virtue of court order, subpoena, other validly issued administrative or judicial notice or order, or pursuant to applicable law; provided that, in such event OMH has given _____ prompt notice of its receipt of the court order, subpoena, other validly issued administrative or judicial notice or order, or request pursuant to applicable law so that _____ may seek a protective order or other appropriate remedy and/or waive compliance with the provisions of this Agreement. The Parties shall cooperate with each other to obtain a protective order or other appropriate remedy, and if _____ cannot obtain a protective order, other appropriate remedy, or otherwise fail to quash the legal process requiring disclosure, OMH shall disclose the Data only to the extent strictly necessary to satisfy the request.
- g. The Parties acknowledge that: the material breach of this Agreement may cause irreparable damage for which recovery of damages would be inadequate; the damages

flowing from such material breach may not be readily susceptible to measurement in monetary terms; and, to the extent permitted by applicable law, any affected Party shall be entitled to immediate injunctive relief restraining any breach hereof, as well as such further relief as may be granted by a court of competent jurisdiction.

h. Nothing in this Agreement shall be deemed to limit the Parties' remedies at law or in equity for any such breach by either Party of any term of this Agreement.

4.4 **Supervision of Data.** The Data and all records/reports derived from the Data shall remain under the immediate supervision and control of the Authorized Persons in a manner that will protect the confidentiality of the Data and all information and records derived from the Data. OMH will further ensure that unauthorized persons cannot retrieve any such information and records by computer, remote terminal, or other means.

4.5 **Data Transfer.** The Data shall be securely transferred between the Parties using a method developed jointly by the Parties' technical staff, with approval of the Parties' cyber-security managers or other authorized staff.

4.6 **Data Retention/Disposition.** The Data shall be retained by OMH for a period of at least six (6) years after the sooner of the termination of this Agreement or upon completion of the Project, whichever occurs first. As soon as the purposes for the Data regarding any individual have been accomplished, OMH will destroy or cause to be destroyed the Data without a trace, in accordance with NIST Standard SP-800-88 Appendix A (Minimum Sanitation Recommendations), in order to prevent unauthorized access or use thereof.

4.7 **Restrictions on Use of Data.** OMH may **NOT**:

- a. Use the Data for any purpose other than to effectuate the purpose of this Agreement, in furtherance of the Project;
- b. Examine or permit any other entity to examine the Data unless such examination is required by Authorized Person in the performance of his/her official duties or responsibilities;
- c. (Re)disclose any identifying or personal information (as applicable) in the Data to any unauthorized person, including other staff;
- d. Enable or permit the Data to be accessed by any person who does not have a direct need and purpose for working with the Data;
- e. Enable or permit the Data to be accessed by any person who does not consent to abide by all the terms of this Agreement;
- f. Except as provided below or prohibited by law, any Data delivered pursuant to this Agreement is understood to be provided "AS IS." _____MAKES NO REPRESENTATIONS AND EXTEND NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. REGARDING THE ACCURACY OR COMPLETENESS OF THE DATA OR THAT THE USE OF THE DATA WILL NOT INFRINGE ANY

PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OMH ACKNOWLEDGES AND AGREES THAT _____ SHALL NOT BE LIABLE TO OMH FOR ANY DAMAGES, LOSSES, LIABILITY RESULTING FROM ANY RELIANCE UPON, ACCESS TO OR USE OF THE DATA OR THIS AGREEMENT. THE PARTIES FURTHER AGREE THAT NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE DATA OR THIS AGREEMENT. Notwithstanding the foregoing to the contrary, each Party, to the best of its knowledge and belief, has the right and authority to provide the Data to OMH for use in the Project.

- 4.8 **Cooperation and Mitigation.** The Parties shall cooperate with each other regarding any remediation that, in their discretion, determine to be necessary to (a) address any applicable reporting requirements, and (b) mitigate any effects of such unauthorized use or disclosure of the Data, including measures necessary to restore goodwill with stakeholders, including research subjects, collaborators, governmental authorities and the public.
- 4.9. **Agents and Subcontractors.** OMH will ensure that any agents, including subcontractors to whom it provides Data, agree to the same restrictions and conditions set forth in this Agreement. _____ and OMH agree that the Parties and their officers, employees, agents, consultants, contractors, subconsultants and/or subcontractors, including Authorized Persons, are independent contractors and not employees of the other Party or any department, agency or unit thereof, nor will they hold themselves out as, or claim to be, officers or employees of the other Party, or any department, agency or unit thereof.
- 4.10 **Liability.** The Parties acknowledge and agree that OMH and the State are self-insured for its general liability exposure, workers compensation and automobile liability. In accordance with Article II of the New York Court of Claims Act, they shall be liable For damage or injury arising from negligent actions caused by an officer of OMH or the State or its employees acting within the scope of their respective employment. The State's self-insured funds could be drawn down if a judgment of liability is made under The provisions of the New York Court Claims Act, or in the case of small claims, an acknowledgement of liability has been made by the Attorney General and the Comptroller of the State of New York. The State's obligation with respect to any such claims are subject to the availability of lawful appropriations, as required by Section 41 of the New York State Finance Law.

ARTICLE 5. MODIFICATION

The Parties agree that no extension, modification or waiver of any provision of this Agreement shall be valid unless in writing pursuant to an amendment executed by duly authorized representatives of the Parties.

ARTICLE 6. ASSIGNMENT

Neither Party shall delegate any duties or assign any of its rights under this Agreement without the prior express written consent of the other Party. Neither Party shall subcontract any part of the work hereunder without the written consent of the other Party. Any purported delegation of duties, assignment of rights or subcontracting under this Agreement without the prior express written consent of the other Party is void.

ARTICLE 7. NOTICES

All notices and requests required or permitted to be made under this Agreement by any Party to the other shall be in writing, directed to the address of the parties as follows, either in person, by courier, by facsimile (and promptly confirmed by personal delivery or courier), or by certified mail, return receipt requested, and shall be effective upon delivery:

[insert notice information]

ARTICLE 8. SURVIVAL

Notwithstanding any other provision of this Agreement, the following sections shall survive termination of this Agreement: 1.3 and 4.1 – 4.8 and 4.10.

ARTICLE 9. ENTIRE AGREEMENT

Unless otherwise specified, this Agreement and the below listed Attachments embody the entire understanding between the Parties regarding the transfer of the Data to OMH for the Project:

- I. Attachment 1: Data-specific Terms and Conditions Fully Identifiable Data
- II. Attachment 2: Data-specific Terms and Conditions Limited Data Set
- III. Attachment 3: Data-specific Terms and Conditions De-Identified Data About Human Subjects

ARTICLE 10. NO THIRD-PARTY BENEFICIARY

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties, any rights, remedies, obligations, or liabilities whatsoever.

ARTICLE 11. ADDITIONAL PROVISIONS

11.1. **Governing Law**. This Agreement shall be governed by and construed in accordance with the laws of the State of New York without regard to choice of laws or conflict of law principles and the laws of the United States, where applicable.

11.2. **Jurisdiction and Venue**. The Parties agree that any and all claims arising under or related to this Agreement shall solely be heard and determined either in the courts of the State of New York. The Parties hereby waive personal service by personal delivery and agrees that service of process may be made by overnight courier or post-paid certified mail directed to the Parties at the Parties' addresses set forth in the Notice section of this Agreement, deemed effective upon receipt with the same effect as though personally served.

11.3. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement. This Agreement may also be executed in counterpart facsimile or scanned signatures, each of which facsimile or scanned signature of a party shall be deemed to be the original signature of such party.

11.4. **Interpretation.** In the event of any conflict between the terms of this Agreement and the terms of any schedule or attachment hereto, it is understood that the terms of this Agreement shall be controlling with respect to any interpretation of the meaning and intent of the Parties. In addition, any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to maintain the confidentiality and security of the Data.

11.5. **Headings.** The headings and other captions in this Agreement are for convenience and reference only and shall not be used in interpreting, construing or enforcing any of the provisions of this Agreement.

11.6. **Severability.** If any provision of this Agreement is found by a proper authority to be unenforceable or invalid, such unenforceability or invalidity shall not render this Agreement unenforceable or invalid as a whole and, in such event, such provision shall be changed and interpreted so as to best accomplish the objectives of such unenforceable or invalid provision within the limits of applicable law or applicable court decisions.

11.7. **Publicity.** No Party shall use any other Parties' name, trademarks, or other logos in any publicity, advertising, or news release without the prior written approval of an authorized representative of that Party. The Parties agree that each party may disclose factual information regarding the existence and purpose of the relationship that is the subject of this Agreement for other purposes without written permission from the other party provided that any such statement shall accurately and appropriately describe the relationship of the parties and shall not in any manner imply endorsement by the other party whose name is being used.

11.8. **Intellectual Property Ownership.** The Parties hereby acknowledge that this Agreement does not constitute a grant by any Party to the other(s) of any license or right to any Party's intellectual property existing as of the effective date of this Agreement. If any party develops any new intellectual property in connection herewith, the Parties shall enter into a separate definitive agreement regarding the ownership of that new intellectual property.

1.9. **Compliance with Laws.** The Parties shall comply, at its own expense, with the provisions of all applicable local, state and federal laws, rules and regulations, including, but not limited to, those applicable to the Parties as an employer of labor. The Parties shall further comply, at its own expense, with all applicable rules, regulations and licensing requirements pertaining to this Agreement.

[The remainder of this page has been deliberately left blank; signatures to follow on next page]

DRAFT

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year appearing below their respective signatures.

NYS OFFICE OF MENTAL HEALTH

By: _____

Name:

Title:

Attachment 1
Data Transfer and Use Agreement

1. [Description of protocol]

2. Description of Project: OMH IRB Protocol(s) (include name and numbers);

3. Data Disposition Requirements upon the termination or expiration of the Agreement:
Disposition Requirements set forth in Article ____ of this Agreement.

DRAFT

Attachment 2
Data Transfer and Use Agreement
Data-specific Terms and Conditions: Other: Fully Identifiable Data

Additional Terms and Conditions:

The additional terms and conditions are as set forth below and agreed upon between the Parties:

1. Nothing herein shall authorize the Recipient to use or further disclose the Data in a manner that would violate the requirements of OMH under 45 CFR 164.514.
2. Recipients shall not use or further disclose the Data other than as permitted by this Agreement or as otherwise required by law.
3. Recipients shall report to OMH any use or disclosure of the Data not provided for by this Agreement within 5 business days of when it becomes aware of such use or disclosure.
4. Recipients will not use the Data, either alone or in concert with any other information, to make any effort to identify or contact individuals who are or may be the sources of Data without specific written approval from _____ and appropriate IRB approval, if required pursuant to 45 CFR 46. Should Recipients inadvertently receive identifiable information or otherwise identify a subject, Recipients shall promptly notify OMH and follow _____'s reasonable written instructions, which may include return or destruction of the identifiable information.
5. By signing this Agreement, Recipients provide assurance that relevant institutional policies and applicable federal, state, or local laws and regulations (if any) have been followed, including the completion of any IRB or ethics review or approval that may be required.
6. The parties agree to take such action as is necessary to amend this Agreement, from time to time, in order for _____ - to remain in compliance with the requirements of HIPAA.
7. Recipients and their employees, agents, subcontractors and any other individual permitted by Recipients to access the data will: (i) use all reasonable security practices; and (ii) take all reasonable security measures necessary to protect the security and privacy of the data.
8. Recipients will be solely responsible for the selection, implementation, and maintenance of its security procedures and policies: (a) for the protection of its internal network and information, and (b) that are sufficient to ensure that (I) the data is used only for authorized purposes, and (II) its systems and data are protected against improper access, use, loss alteration or destruction.

9. Recipients will not use unencrypted devices such as desktop, laptop, including external media, such as USB thumb drives (aka “flash drives”) or external hard drives, or cloud storage systems (such as OneDrive, Google Drive, Dropbox, etc.) to store any OMH data.
10. Any mobile device (i.e., laptop, phone, tablet, etc.) used to store OMH data, must have full disk encryption enabled.
11. All network communications containing patient, employee, agent, student, or other personally identifiable information, or system administrator credentials will be encrypted using industry-standard encryption mechanisms implemented through widely used and tested libraries and using AES-256, Data Authentication using at least SHA1 and Handshake encryption using at least RSA-2048 but preferably 4096), or use its own encryption and configuration policies if recognized as an industry standard by a technology standard organization (for example IEEE and RFC).
12. Recipient will comply with the following transmission standards:
 - Data to Recipient: Recipient will use either SFTP/SCP or FTP over SSL/TLS (FTPS) methods to allow OMH to transmit data to Recipient. If one of these secure methods is not used, then Recipient will notify OMH, and OMH will then transfer the data in an encrypted format to above standards.
 - Information from Recipient: Recipient will use either SFTP/SCP or FTP over SSL/TLS (FTPS) methods to transmit data to OMH. If one of these secure methods is not used, then Recipient will encrypt the information before transmitting the information to above standards.
13. Upon expiration of this agreement, the data transferred to Recipient shall be deleted by Recipient per NIST Standard SP-800-88 Appendix A (Minimum Sanitization Recommendations), unless both parties extend the agreement prior.

Attachment 3
Data Transfer and Use Agreement
Data-specific Terms and Conditions: Limited Data Set

Additional Terms and Conditions:

1. Nothing herein shall authorize the Recipient to use or further disclose the Data in a manner that would violate the requirements of OMH under 45 CFR 164.514.
2. Recipient shall not use or further disclose the Data other than as permitted by this Agreement or as otherwise required by law.
3. Recipient shall report to the OMH any use or disclosure of the Data not provided for by this Agreement within 5 business days of when it becomes aware of such use or disclosure.
4. OMH is a HIPAA Covered Entity, and the Data will be a Limited Data Set as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). In accordance with Section 164.514(e)(2) of the HIPAA Privacy Rule, the Data shall exclude the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
 - Names;
 - Postal address information, other than town or city, State, and zip code;
 - Telephone numbers;
 - Fax numbers;
 - Electronic mail addresses;
 - Social security numbers;
 - Medical record numbers;
 - Health plan beneficiary numbers;
 - Account numbers;
 - Certificate/license numbers;
 - Vehicle identifiers and serial numbers, including license plate numbers;
 - Device identifiers and serial numbers;
 - Web Universal Resource Locators (URLs);
 - Internet Protocol (IP) address numbers;
 - Biometric identifiers, including finger and voice prints; and
 - Full face photographic images and any comparable images.

If the Data being provided is coded, the OMH will not release, and the Recipient will not request, the key to the code.

5. Recipient will not use the Data, either alone or in concert with any other information, to make any effort to identify or contact individuals who are or may be the sources of Data without specific written approval from OMH and appropriate IRB approval, if required pursuant to 45 CFR 46. Should Recipient inadvertently receive identifiable information

or otherwise identify a subject, Recipient shall promptly notify OMH and follow OMH's reasonable written instructions, which may include return or destruction of the identifiable information.

6. By signing this Agreement, Recipient provides assurance that relevant institutional policies and applicable federal, state, or local laws and regulations (if any) have been followed, including the completion of any IRB or ethics review or approval that may be required.
7. The parties agree to take such action as is necessary to amend this Agreement, from time to time, in order for the OMH to remain in compliance with the requirements of HIPAA.
8. Recipient and its employees, agents, subcontractors and any other individual permitted by Recipient to access the data will: (i) use all reasonable security practices; and (ii) take all reasonable security measures necessary to protect the security and privacy of the data.
9. Recipient will be solely responsible for the selection, implementation, and maintenance of its security procedures and policies: (a) for the protection of its internal network and information, and (b) that are sufficient to ensure that (I) the data is used only for authorized purposes, and (II) its systems and data are protected against improper access, use, loss alteration or destruction.
10. Recipient will not use unencrypted devices such as desktop, laptop, including external media, such as USB thumb drives (aka "flash drives") or external hard drives, or cloud storage systems (such as OneDrive, Google Drive, Dropbox, etc.) to store any OMH data.
11. Any mobile device (i.e., laptop, phone, tablet, etc.) used to store OMH data, must have full disk encryption enabled.
12. All network communications containing patient, employee, agent, student, or other personally identifiable information, or system administrator credentials will be encrypted using industry- standard encryption mechanisms implemented through widely used and tested libraries and using AES-256, Data Authentication using at least SHA1 and Handshake encryption using at least RSA- 2048 but preferably 4096), or use its own encryption and configuration policies if recognized as an industry standard by a technology standard organization (for example IEEE and RFC).
13. Recipient will comply with the following transmission standards:
 - Data to Recipient: Recipient will use either SFTP/SCP or FTP over SSL/TLS (FTPS) methods to allow OMH to transmit data to Recipient. If one of these secure methods is not used, then Recipient will notify OMH, and OMH will then transfer the data in an encrypted format to above standards.
 - Information from Recipient: Recipient will use either SFTP/SCP or FTP over SSL/TLS (FTPS) methods to transmit data to OMH. If one of these secure methods is not

used, then Recipient will encrypt the information before transmitting the information to above standards.

14. Upon expiration of this agreement, the data transferred to Recipient shall be deleted by Recipient per NIST Standard SP-800-88 Appendix A (Minimum Sanitization Recommendations), unless both parties extend the agreement prior.

DRAFT

Attachment 4
Data Transfer and Use Agreement
Data-specific Terms and Conditions: De-identified Data about Human Subjects

Additional Terms and Conditions:

1. The Data will not include personally identifiable information as defined in NIST Special Publication 800-122. If the Data being provided is coded, the OMH will not release, and the Recipient will not request, the key to the code.
2. If OMH is a Covered Entity, the Data will be de-identified data, as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).
3. Recipient will not use the Data, either alone or in concert with any other information, to make any effort to identify or contact individuals who are or may be the sources of Data without specific written approval from OMH and appropriate IRB approval, if required pursuant to 45 CFR 46. Should Recipient inadvertently receive identifiable information or otherwise identify a subject, Recipient shall promptly notify OMH and follow OMH’s reasonable written instructions, which may include return or destruction of the identifiable information.
4. By signing this Agreement, Recipient provides assurance that relevant institutional policies and applicable federal, state, or local laws and regulations (if any) have been followed, including the completion of any IRB or ethics review or approval that may be required.
5. Recipient shall promptly report to the OMH any use or disclosure of the Data not provided for by this Agreement of which it becomes aware.
6. Recipient and its employees, agents, subcontractors and any other individual permitted by Recipient to access the data will: (i) use all reasonable security practices; and (ii) take all reasonable security measures necessary to protect the security and privacy of the data.
7. Recipient will be solely responsible for the selection, implementation, and maintenance of its security procedures and policies: (a) for the protection of its internal network and information, and (b) that are sufficient to ensure that (I) the data is used only for authorized purposes, and (II) its systems and data are protected against improper access, use, loss alteration or destruction.
8. Upon expiration of this agreement, the data transferred to Recipient shall be deleted by Recipient per NIST Standard SP-800-88 Appendix A (Minimum Sanitization Recommendations) or any industry-accepted successor standards, unless both parties extend the agreement prior.
9. Recipient shall not use or further disclose the Data other than as permitted by this Agreement or as otherwise required by law.