CHIA.
center for health information and analysis

Data Management Plan for Use of CHIA Data
[Attach to Data Application]

I. INSTRUCITONS

Any Recipients, contractors, or agents receiving CHIA Data ("Data") must complete and execute this Data Management Plan. Certain CHIA Data includes Protected Health Information ("PHI" as defined under the Health Insurance Portability and Accountability Act [HIPAA] and its implementing regulations) and all CHIA Data contains elements that may be used to identify an individual. The Data Management Plan(s) will be incorporated within the Data Use Agreement that must be executed prior to receipt of the Data. You may wish to refer to the Data Use Agreement as you complete this Data Management Plan. This Data Management Plan should be completed by the Chief Information Security Officer, Chief Privacy Officer, legal counsel or another officer with sufficient knowledge of the Agency or Organization's data privacy and security practices and who has authority to bind the Agency or Organization.

NOTE: This Data Management Plan is confidential and will not become a part of the public record.

II. GENERAL INFORMATION

Project Title: (as it appears on Data Application)	
Primary Investigator: (as it appears on Data Application)	
Organization Requesting CHIA Data (Recipient): (as it appears on Data Application)	
Organization Holding CHIA Data under this Data Management Plan: (must be listed as an Agent/Contractor on Data Application)	

III. CERTIFICATIONS

The undersigned certifies and agrees as follows:

- The Data will be **encrypted at rest on storage media (backup tapes, local hard drives, network storage, et al) with at least AES-256 standard or stronger**.
- The Data will **be encrypted in transit consistent with the approved method(s) described in this Data Management plan at section V.3-b**.
- Anti-virus software or service is active on any server or endpoint containing the Data.
- If a Covered Entity or Business Associate under HIPAA, the Agency or Organization is in full compliance with the privacy and security requirements of HIPAA; trains all staff who access PHI on the requirements of HIPAA; and has Business Associate Agreements with all non-employees who access PHI.
- The Agency or Organization has policies and procedures in place to address:
    - The sharing, transmission and distribution of PHI
    - The physical removal, transport and transmission of PHI
    - The physical possession and storage of PHI
    - The destruction of PHI upon the completion of its use
    - Confidentiality agreements with all individuals, including contractors, who will access PHI
    - Agreements governing the use and disclosure of PHI with all non-employees who will access PHI

IV. RESPONSIBLE PARTIES

Please identify the following individuals within your Agency or Organization:

1. The individual responsible for organizing, storing and archiving the Data. This individual is the Custodian of the CHIA Data required under Article XI of the Data Use Agreement.

Name:	
Agency/Organization:	
Title:	
Phone:	
Address, City/Town, State, Zip Code:	
Email:	
Reports to (name and title):	

2. The individual(s) responsible for the research team using the Data, including ensuring each individual (i) has a signed confidentiality agreement, (ii) accesses and uses only the minimal Data necessary to achieve the research purpose, (iii) accesses the Data only on a secured server according to Applicant's policies. This individual is also responsible for maintaining the access log required under Article II, Section 5 of the Data Use Agreement.

Name:	
Agency/Organization	
Title:	
Phone:	
Address, City/Town, State, Zip Code:	
Email:	
Reports to (name and title):	

3. The individual responsible for notifying CHIA of any breach of the Data Use Agreement or this Data Management Plan.

Name:	
Organization:	
Title:	
Phone:	
Address, City/Town, State, Zip Code:	
Email:	
Reports to (name and title):	

4. The individual responsible for ensuring the Data is destroyed upon termination of the Data Use Agreement, completing the Data Destruction Form and providing that Form to CHIA.

Name:	
Organization:	
Title:	
Phone:	
Address, City/Town, State, Zip Code:	
Email:	
Reports to (name and title):	

V. DATA SECURITY AND INTEGRITY

Agents or contractors that will have access to or store the CHIA Data at a location other than the Recipient's location, or in an off-site server and/or database, must complete a separate Data Management Plan.

1. *Physical Location of the Data*:

    a. Please provide the delivery address for the Data, as well as the full address, including building and floor, of each location where Data will be delivered and stored.

Delivery:

Organization:			
Street Address:	City:	State:	ZIP Code:
Office Telephone *(Include Area Code)*:			

Storage:

Organization:			
Street Address:	City:	State:	ZIP Code:
Office Telephone *(Include Area Code)*:			

    b. Will the Data be stored by the third party on a system in the cloud (reachable via the Internet)?
    ☐ Yes ☐ No

        i. If you answered yes to (b): Has this Cloud Service Provider passed a FedRAMP 3PAO assessment *for the specific cloud system* which will host the data*?*
        ☐ Yes ☐ No

        ii. If you answered yes to (b): What is the name of the provider *and* the FedRAMP level the specific cloud system hosting the data is operating at?

2. *Data Privacy Training and Awareness:*

    a. Has every individual who will access the Data received training on the proper handling of protected health information and/or personal data within the last year?
    ☐ Yes ☐ No

3. *Encryption of Data*:

   a. Will all CHIA Data at rest be encrypted on storage media (backup tapes, local hard drives, network storage, et al) with **encryption at least AES-256 or stronger.** *All Recipients of CHIA Data must encrypt data at res. A Data Management Plan indicating otherwise will not be approved and returned for revisions.*
   ☐ Yes ☐ No

   b. Will CHIA Data be transmitted by your Agency or Organization over the Internet?
   ☐ Yes ☐ No

   If you answered yes to (b): which of the following if any are used when transmitting data over the internet? If selecting *other* please describe the method in space provided below.
   ☐ SSL (meets or exceeds TLS 1.1 or TLS 1.2) ☐ SFTP ☐ other

4. *Information Security:*

   a. Does your Agency or Organization have published information security policies which are followed and accessible to all staff accessing or handling CHIA Data?
   ☐ Yes ☐ No

   b. Has every individual who will access the CHIA Data received cyber security awareness training in the last year?
   ☐ Yes ☐ No

   c. Has your Agency or Organization experienced a breach of PHI or Personally Identifiable Information in the last seven (7) years?
   ☐ Yes ☐ No

      i. *If you answered yes to (c): how was the breach resolved and what steps were taken to prevent a recurrence?*

5. *Technical and Physical Controls:*

   a. Are all the user accounts that log on to any machine (server or endpoint) that accesses the Data uniquely assigned to individual users (i.e., the user accounts are not shared)?
   ☐ Yes ☐ No

   b. Is an audit log maintained of all user log-ons to the system hosting the CHIA Data?
   ☐ Yes ☐ No

c. What is the minimum password length and character complexity (uppercase, lowercase, numeric, and special characters) required for new passwords on the user accounts logging on to the system accessing the CHIA Data?

d. Describe any additional authentication technical security controls you employ to defend the system against unauthorized logon, e.g. maximum failed login attempts, lockout period, etc.:

e. Do you run a current version of a commercial off-the-shelf anti-virus or anti-malware product on the server that will host the CHIA Data?
☐ Yes ☐ No

f. If the CHIA Data will be on a server or network accessible storage drive, then check all the security features present in the room containing CHIA Data:
   i. ☐ Recorded video
   ii. ☐ Access log of all individuals entering the room
   iii. ☐ Secure server rack
   iv. ☐ Access control limiting access only to authorized individuals

g. What additional specific physical or technical safeguards (not mentioned in prior answers) will be used to *mitigate* the risk of unauthorized access to CHIA Data?

h. When was the last information security risk assessment performed in your Agency or Organization? Who conducted it?

i. When was the last IT audit performed in your Agency or Organization? Who conducted it?

VI. DATA DESTRUCTION

The Recipient attests that the CHIA Data and all copies of the CHIA Data used by the Applicant or its employees, contractors, or agents will be destroyed upon Project Completion or termination of the Data Use Agreement. All data destruction must conform to the requirements of M.G.L. c. 93I and to the Data Use Agreement. Please specify below the technical measures you will use to meet these requirements.

VI. ATTESTATION

By submitting this Data Management Plan, the Agency or Organization attests that it is aware of its data use, privacy and security obligations imposed by state and federal law *and* confirms that it is compliant with such use, privacy and security standards. The Agency or Organization further agrees and understands that it is solely responsible for any breaches or unauthorized access, disclosure or use of CHIA Data, including, but not limited to, any breach or unauthorized access, disclosure or use by its agents.

By signature below, I attest: (1) to the accuracy of the information provided herein; (2) that the Agency or Organization agrees to hold and/or access CHIA Data at all times in compliance with all provisions of this Data Management Plan and the Data Use Agreement; and (3) to my authority to bind the Agency or Organization undersigned as an authorized signatory of the Organization.

Signature: (Authorized Signatory for Organization holding CHIA Data)	
Printed Name:	
Title:	
Organization Holding CHIA Data:	
Date:	