Study to Explore Early Development (SEED)

Data Confidentiality and Security Policy

SEED Data Confidentiality and Security Policy

SEED **Data Confidentiality and Security Policy**

I. Confidentiality Security Statement for SEED

This policy applies to individuals collecting or using data as part of the Study to Explore Early Development (SEED). The policy is intended to be minimal standards for all Centers for Autism and Developmental Disabilities Research and Epidemiology (CADDRE) sites; however, any site may adopt additional policies that are more stringent and adhere to the policies and guidelines of their home institution. If the policies or guidelines of your home institution are incompatible with these policies, it is necessary to contact the CADDRE Project Coordinator for resolution.

This document describes the procedures and practices each CADDRE site intends to use to protect the confidentiality of the data collected or distributed as part of this research study funded by the Centers for Disease Control and Prevention (CDC)/ National Center on Birth Defects and Developmental Disabilities (NCBDDD). The CADDRE Principal Investigator (PI) for this study is Diana Schendel, NCBDDD/CDC. The CADDRE Project Coordinator is Marques Harvey, Battelle/NCBDDD/CDC. The primary contact for each CADDRE site is that site's Principal Investigator(s).

Study personnel (defined in this document as CADDRE Site staff and contractor staff, Data Coordinating Center staff, guest researchers, fellows, research assistants and anyone who has approved access to identifiable study data) is required at all times to maintain and protect the confidential records that may come into their presence and under their control according to these policies and any additional site guidelines, as applicable.

All documents, paper and electronic, for this study containing names and other information identifying a single individual or a single institution and other study files, will be considered confidential materials and will be safeguarded to the greatest extent possible. Because the data are highly sensitive, the security requirement is rated as high. It is the professional and legal responsibility of each individual associated with this study to protect the right to confidentiality of the individuals (i.e. children and their families) in the study.

Extra precaution should be taken to protect the security of the 18 identifying variables cited in the Health Information and Information Portability and Accountability Act (HIPAA). The following are 18 HIPAA identifying variables:

1. Names;
2. All geographic subdivisions smaller than a State; including street address, city, county, precinct, zip code, and their equivalent geocodes; except for the initial three digits of a zip code if according to the current publicly available data from the Bureau of the Census:
    - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;

6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by number three of this section; and
    - The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

II. Safeguarding Measures and Restrictions on Use of Information

A. Confidentiality Designee and Training

Each site must identify a Confidentiality Designee who will receive training in these policies from the CADDRE Project Coordinator, Marques Harvey. Once a site has their designated Confidentiality Designee, that person is responsible for the initial and annual training of other staff members at that site. All study staff working on this project will be required to attend a training session to review these policies and the confidentiality issues particular to this project, and sign the appropriate nondisclosure agreements. This training must take place before any site begins to access or collect identifiable data. The Confidentiality Designee will be responsible for ensuring all site personnel are trained in data confidentiality and security, and that these materials are reviewed on an annual basis. Each site must ensure that there is always a Confidentiality Designee, and changes in assignment of this duty must be communicated to CDC immediately.

B. Confidentiality Statement of Understanding

To assure that they are aware of this responsibility and the penalties for failing to comply, all study personnel who have access to identifiable information related to the project must read and sign a Confidentiality Statement of Understanding, assuring that all identifying information will be kept confidential and will be used only for epidemiologic or statistical purposes.

Attachment A1 is the Confidentiality Statement of Understanding to be reviewed and signed by all **CADDRE site personnel** with access to confidential information related to the project.

Signed agreements will be obtained by the Site's Confidentiality Designee and maintained in the employee's file. Each site's principal investigator must review these and any additional security requirements of that site before any access to identifiable data is granted to the employee. The originals should be retained in files at the project site and readily accessible upon request.

C. Restrictions on Use of Information

1. Information collected or retrieved by study personnel in the course of conducting the study will be used only for the purposes of carrying out study activities and shall not be divulged or made known in any manner unless approval from the study participant is received (written notice).
2. Study staff is responsible for protecting all confidential records from visual observation, from theft, or from accidental loss or misplacement due to carelessness. All reasonable precautions will be taken to protect confidential data.
3. CDC requires any materials containing personal identifiers that must be sent by authorized study personnel should be sent via first class certified-return receipt mail or commercial carrier service in a sealed envelope stamped "CONFIDENTIAL" on the front.
4. CDC does not recommend the electronic transmission (via fax or e-mail) of records or data containing names or other personally identifying information. However, if a CADDRE site deems it is necessary and allowable to transmit personally identifiable data electronically, they should follow the HIPAA Standard to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. (**4.18 Transmission Security (§ 164.312(e) (1)).** At a minimum, any information e-mailed with identifiers should be encrypted and all precautions taken to ensure that fax machines are in a secure location and are retrieved only by authorized personnel.
5. Study personnel are not to divulge any personal identifying information about study participants to anyone other than authorized project staff on a "need to know" basis appropriate to conduct official business. In general conversation outside the workplace, neither the identifying information, specific details about the data collected, nor the means by which they are collected should be discussed in any detail. Breach of confidentiality due to study personnel knowingly and willfully disclosing confidential information may result in removal from study activities. If a breach of confidentiality is due to unintentional, but careless behavior and/or not following policies to maintain confidentiality of data, the behavior will result in, (at a minimum), a temporary removal from accessing confidential information, and site-specific sanctions will apply. Permanent reassignment to another project is at the discretion of each CADDRE site and in conjunction with site-specific personnel policies (refer to Section IV.B. for more information).
6. When not in use by authorized project staff, all hard copy material and physical media containing confidential data will be stored in locked containers, locked file cabinets, or locked rooms. Access to locked storage areas will be limited to authorized project staff. This procedure will apply to all physical media containing confidential data, including data collections forms, printouts, diskettes, cds/dvds, flash drives, memory cards, laptop computers, and magnetic data tapes. Staff working with confidential materials during forms processing and data handling will have access only to the materials that they are currently processing. When confidential records are in use, they must be kept out of sight of persons not authorized to work with these records.

7. Except as needed for operational purposes, photocopies of confidential records are not to be made. If photocopies are necessary, care should be taken that all copies and originals are recovered from the copy machines and work areas. All confidential paper records will be destroyed as soon as operational requirements permit by burning or shredding the documents.
8. No data (or copies of data) are to be retained by a contractor after completion of the period of performance of the contract, or as specified in the contract for reasonable handling of data on back-up tapes/drives.
9. Unless specifically instructed otherwise for a particular project approved by the Principal Investigator, employees will not be allowed to abstract, collect or process data from a respondent whom they know personally.

D. Enhanced Protection of Computerized Files

In addition to any documents and materials, all study data maintained in electronic storage systems will be protected to maintain confidentiality. The following safeguards shall be implemented to protect files so that the accuracy and the confidentiality of the data can be maintained:

1. **CADDRE Sites:**
   a. Electronic data files will only contain names or other personal identifiers (other than the study identification number) when absolutely necessary for study purposes.

   b. Personal identifiers entered electronically and housed in a secure study location (this does NOT include laptops taken into the field, which must always have password protection and encryption) will be stored in data files that will be maintained under password-protected computer accounts and encrypted whenever possible.

   c. Computer files containing programs, documents, or confidential data will be stored in computer systems that are protected from accidental alteration and unauthorized access. Computer files, whether they are stored on a mainframe computer, a LAN or individual computers, will be protected by password systems, controlled sharing, third party encryption software and routine daily backup procedures. Computer facilities at all sites will be protected from potential fire or water damage.

   d. No personally identifiable data should be stored on a laptop or a portable data storage device, such as a floppy disk, compact disc (cd), USB flash drive, or other such devices unless the data contained within can be encrypted to the FIPS 140-2 standards for the National Institute of Standards and Technology (www.nist.gov).

   e. In addition to these policies, all sites should comply with the data security and storage policies of their institution.

2. **Information Technology (IT) Security Procedures for the CADDRE Information System (CIS)**

All transactions across the Internet that involve individually identifiable health information will be sent to/from the DCC as encrypted data. Personal identifiers will be transmitted in encrypted form, and then stored in the database in only an encrypted form (all 18 HIPAA 'Safe Harbor' identifiers as applicable). The encryption facility will also be used to ensure that user account credentials never cross the network in decrypted form. Database encryption is being applied to preclude inadvertent exposure of individually identifiable health information to IT system administrators and developers, and to protect confidentiality of individually identifiable health information in the case of system intrusion. These objectives will guide the implementation of the database encryption. No documentation concerning the encryption/decryption secrets will be stored on the database server.

Each SEED site's data stored at the DCC is secured separately from all others. Access to a site's protected data is provided only through the specific accounts for that site's authorized personnel. It is the responsibility of each site to administer its own users' account credentials and specific account privileges (role-based security); the DCC provides the system facilities for this. No means will exist for one site to access the personal identifiable data stored by another site.

E. Dissemination of Research Results

Unless specific parental consent is granted to share identifiers with approved entities, all reports and publications of collected study data will be presented in aggregate form only. The names or other identifiers of participating individuals will not be presented in any publication. Reports will be written so that no person may be individually identified, even indirectly. Reporting of aggregate data will be sensitive to adhere to guidelines of the National Association of Health Data Organizations "Statistical Guidelines for Small Numbers" (www.nahdo.org/hidsc/datareleaseguidelines.aspx).

F. Data Sharing with Other Study Partners

Study data will be electronically transferred via the CADDRE Information System (CIS) to the Data Coordinating Center (DCC). The DCC will not release any data without the approval of the CADDRE Datasharing Committee.

Individually identified data on individuals or establishments (sources, diagnosticians, etc.) will only be shared across study sites or with non-study personnel upon specific approval of the site's appropriate Institutional Review Board(s) (IRBs) (as appropriate) for specific data collection or analysis purposes. The study must be in line with the original purpose for which the study data have been collected, or re-review by local IRB(s) might be necessary. The CDC Confidentiality Officer should be consulted if there are requests that present unusual circumstances or appear problematic. In addition, all sites should reference the "CADDRE Datasharing Guidelines" for additional guidance. There should be no datasharing of the 18 identifying variables cited in the Health Information and Information

Portability and Accountability Act (HIPAA) (see Section I of this document for a list of these variables) without the approval of Data Sharing Committee and local IRBs (as appropriate).

III. Instructions to SEED Personnel Concerning Confidentiality Procedures:

A. General Procedures:

1. All CADDRE or CDC staff who will have any access to confidential data will be required to sign a Confidentiality Pledge (Attachment A1).

2. Use of confidential data, including telephone interviews, data entry, abstraction, and other activities, should always be conducted in the most private setting available.

3. Treat materials containing confidential information as your own sensitive information, such as a driver's license or credit card, and make sure the materials are always in your sight or secured properly.

4. It is the employee's responsibility to make sure that all study materials in his or her possession are protected from loss or theft to the maximum extent possible.

5. Never store passwords or other identifiable information with your computer.

B. Office and Clinic Procedures On-Site:

1. When paper records or computer screens that contain confidential information are in use, they must be kept out of sight of persons not authorized to work with these records.

2. When using the CIS, make sure to activate the password lock when leaving the work area, even if for a short while such as to use the restroom.

3. Keep all files with confidential data in a locked room or area designated for study confidential data when not in use.

4. Lock all file cabinets and offices after business hours and when Study staff are away from the office for extended periods of time (i.e., do not leave paper records on the desk).

C. Procedures for traveling with study materials:

1. When traveling between facilities, paper and electronic records need to be kept in a locked container.

2. All records need to be taken immediately from an off site facility or clinic to the main office after the completion of the visit. In addition, study related materials containing data may not be taken home for any reason or left in an unattended vehicle at any time.

IV. Loss of Study Materials Containing Confidential Data:

1. General Procedures:

a. In the event that any study materials are lost or stolen, contact your supervisor immediately and inform him or her as to whether any materials containing identifying information were included.

b. In the case of theft, contact the local authorities, as appropriate.

c. The site's Principal Investigator (PI) should immediately contact their site IRB representative and the CDC Project Officer, Diana Schendel.

d. In the case that identifying information is lost or stolen; the PI should also contact data sources and/or participants to work with them in an effort to prevent or minimize potential harm to individuals at risk for having their data compromised.

e. The PI should determine how to handle notification of the disclosure, based on the agreements made with the sources and on the policies and regulations of their institutions and state(s).

f. Letters and/or contacts with data sources and/or participants should include information about the data security procedures that were in place, their implementation, and remediation actions taken by the CADDRE site following the loss or theft.

g. The site PI should keep CDC advised on this matter and be prepared to respond to inquires regarding this event.

h. If the study materials are recovered the site will still need to notify their sources and/or participants. There is still the possibility that the information has been compromised.

i. The site PI should provide a written summary to CDC describing the steps taken to resolve the issue.

2. Levels of Information Loss and Consequences:

a. Unavoidable Loss: Unavoidable loss of data is defined as loss of data following reasonable steps to protect its security by following these policies at a minimum. This type of loss should result in, at a minimum:

- A review of the confidentiality and security policies with all employees accessing identifying data;
- A record of the incident for the Site's and CDC's files;
- An organizational review of the Site's and SEED Data Confidentiality and Security Policy.

b. Loss Due to Negligence: Loss of data due to study personnel negligence by not following the above-mentioned policies should result in, at a minimum:

- Immediate removal of access to identifying or sensitive materials pending incident review procedures;
- A record of the incident should be placed in the personnel file and

forwarded to CDC;

- Additional site-specific personnel procedures may apply including permanent removal from duties where identifying information is accessible or termination from SEED employment.

c. Breach by Personnel: Active divulging of information could be in the form of a verbal disclosure, or in giving unauthorized personnel access to identifying data. Breach of confidentiality due to divulging confidential information by personnel will result in:

- Release from working on SEED;
- Reassignment to another project is at the discretion of each CADDRE site in conjunction with site-specific personnel policies*;*
- A record of the incident should be placed in the personnel file and forwarded to CDC.

A1 Confidentiality Statement of Understanding for SEED Personnel

I, _____, through my involvement with and work on the Study to Explore Early Development (SEED), will have access to data collected by CADDRE. By virtue of my affiliation with this project, I have access to confidential information and use of data about respondents generally perceived as personal and private. As a condition of this access and my participation in this project I am required to comply with requirements specified in the *SEED Data Confidentiality and Security Policies*.

I understand that access to this confidential information and data carries with it responsibility to guard against unauthorized use. To treat information as confidential means not to divulge it to anyone who is not a project member, or to cause it to be accessible to anyone who is not a project member. Anything not specifically named as public information is considered confidential.

I agree to fulfill my responsibilities on this project in accordance with the following policies:

1. I agree to not permit non-project personnel access to these data in any manner, including electronic or hard copy.

2. I agree to not disclose, or make known in any manner, information about study participants (i.e. children and their families), including identity, to non-project personnel.

3. I agree to protect all identifying information and study materials in my possession from loss or theft to the maximum extent possible.

4. I agree that in the event that confidential information is disclosed inadvertently, I will (a) advise the Project Coordinator of the incident who will report it to the Study's Principal Investigator, (b) safeguard or destroy the information as directed by the investigator, and (c) not inform any other person of the disclosed information.

My signature below indicates that I have carefully read and understand this agreement and the confidential nature of all records to be handled in regard to this project. As a(n) (_____)(investigator, study coordinator, research assistant, interviewer, abstractor, clinician, guest researcher, programmer, etc.), I understand that I am prohibited from disclosing any such confidential information that has been obtained under this project to anyone other than authorized staff of the project. I understand that any disclosure in violation of this Confidentiality Pledge may lead to my removal from working on SEED and additional employment penalties may apply.

Name (printed): _____

Signature: _____ Date: _____

Copy placed in personnel file ___