Child Trends' Research Data Security Policy

Updated March 2016

Purpose

Child Trends' Research Data Security Policy is designed to ensure that all project staff, including subcontractors and consultants, understand the importance of keeping data confidential and understand how to do so for all projects. Keeping data secure is part of our obligation to protect study participants from harm that could occur to them if identifying information about them were disclosed. As such, this policy complements the Child Trends Human Subjects Research Protection Policy. This data security policy is also designed to ensure that we comply with the standards set forth by organizations and funders who may allow us to use their data.

What This Policy Does Not Cover

This policy addresses the security of research-related secure data, such as data that contain personally identifiable information (PII) of research participants, but does not address operational data, such as data from human resources or financial operations. The security of those data is addressed in Child Trends' forthcoming Operational Data Security Policy.

In addition, human subject protections outside of data security are overseen by the Child Trends Institutional Review Board and their related policies. Though some research projects at Child Trends may not require IRB approval, all projects and work must comply with the appropriate and relevant standards for data security.

Roles and Responsibilities

Researchers (all who work on projects, including subcontractors and vendors) and administrative staff have responsibilities for implementing this policy. The main parties are identified below.

- **Data Security Committee Chair** (Jennifer Manlove)
  The Data Security Committee Chair (DSCC) is a senior research staff member appointed by the vice president (VP) overseeing research. The DSCC is responsible for ensuring 1) we meet the specifications of data security agreements with the National Center for Education Statistics (NCES), 2) that we annually train staff on data security and this policy (e.g., presentation at all-staff meeting, video, or quiz) and that staff remain up to date in their training with tracking assistance from the compliance office, 3) that we annually audit the effectiveness of the data security procedures in place, 4) that we answer questions from staff about data security concerns, and 5) that we update this policy at least every three years. The DSCC may invite one to five staff to serve on a Data Security Committee that supports the chair's role.

- **Head of Compliance** (Kathleen Skinner)
  The head of compliance or her staff designee shall 1) ensure we meet the specifications of any data security agreements with data providers other than NCES, 2) work with the IRB to maintain a list of the names of the datasets that include personally identifiable information (levels 2 or 3), the location of the datasets, the requirements of housing and using those datasets, and any relevant agreements including data-sharing agreements and team member user agreements; 3) maintain a list of which trainings are needed for which staff for all datasets (except NCES, which will be tracked by the DSCC or her designee), track which staff have participated in relevant trainings and notify the individual, DSCC, and VPs when anyone falls out of compliance so that the DSCC may follow-up with those staff; 4) ensure that subcontractors and consultants are appropriately trained consistent with the agreements, in coordination with the DSCC, and 5) ensure that the timely destruction of secure data is planned and occurs according to plan. In the event of a breach, the head of compliance will also initiate the involvement of an attorney.

Child Trends research staff working with states or federal entities are responsible for knowing and abiding by the regulations of these entities.

- **Information Technology** (FedSolutions)
  The office of information technology (IT) is responsible for upholding or exceeding the levels of data security outlined in this policy (e.g., ensure that passwords and screen-saver timeout are compliant), responding to any auditing or other issues raised in a timely manner, and following the incident protocol in the event of a data security breach. IT should notify Child Trends of opportunities to improve our data security or if any of our protections are not up to industry standards. IT is also responsible for making sure that any IT staff working on the Child Trends account are knowledgeable about and uphold this policy and the related agreements.

- **Overseer of IT** (Chief Financial Officer, Karen Calloo)
  The individual responsible for overseeing IT shall ensure that the requirements of this policy and any related data security agreements are written into our contract with the IT vender and that the vendor is held accountable for the implementation of the policy.

- **Project Directors**
  Project Directors (PDs) are responsible for 1) ensuring that all relevant research activities are reviewed by the IRB and all data collected, obtained, housed, or used by the project complies with this policy and any applicable agreements or regulations, as appropriate; 2) ensuring that their team members, including subcontracting staff, are up-to-date on IRB and data security trainings, for notifying the head of compliance of project staff changes, and for initiating the process of removing access to secure data when team members leave the project or fall out of compliance; and 3) immediately notifying IT, the DSCC, the head of compliance, and the VP for research in the event of a data breach or possible data breach.

- **All Staff**
  All staff are expected to treat data security as a critical requirement of our work, to follow the requirements outlined here and basic common practice (e.g., do not give out passwords, do not leave secure data room unlocked), and to notify the appropriate parties immediately if a breach of secure data is suspected (see breach protocol, below).

- **Vice President for Research** (Natalia Pane)
  The Vice President for Research is responsible for appointing and overseeing the DSCC, updating this policy as needed including identifying and accommodating updates to data security as mandated by the federal government or as identified by increasing industry standards (working with IT, DSCC, and others), working with the Head of Compliance to ensure that no staff that are out of compliance are allowed access to secure data, being the point of contact should a breach occur, and establishing the importance of data security in the culture of the organization.

In the Event of a Data Breach

In today's world, despite the safeguards many organizations have in place, breaches of secure data are an all too common event. As a result, we must not only guard against such breaches, but also prepare in the event one occurs. Breaches differ in severity; examples include:

- An unauthorized individual attains access to a secure drive (e.g., by using someone else's password).
- A client sends PII data unencrypted through email to the wrong persons (although not our fault, we would still have to address the breach).
- An employee leaves and has taken PII data with her.
- A subcontractor housing CT secure data is hacked.
- A stack of surveys with PII information are lost at the data collection site.
- A laptop with newly collected PII data saved on the hard drive is stolen.

As soon as any employee or team member suspects a data breach, the team member should immediately notify the VP for Research (Natalia Pane), the Head of Compliance (Kathleen Skinner), the relevant project director, and the DSCC.

The staff member should also notify the IT vendor (FedSolutions) if the breach is related to technology. The Communications protocol for Crisis Communications will then take effect. The head of compliance will be responsible for involving an attorney as soon as possible and when appropriate.

Data Security Levels

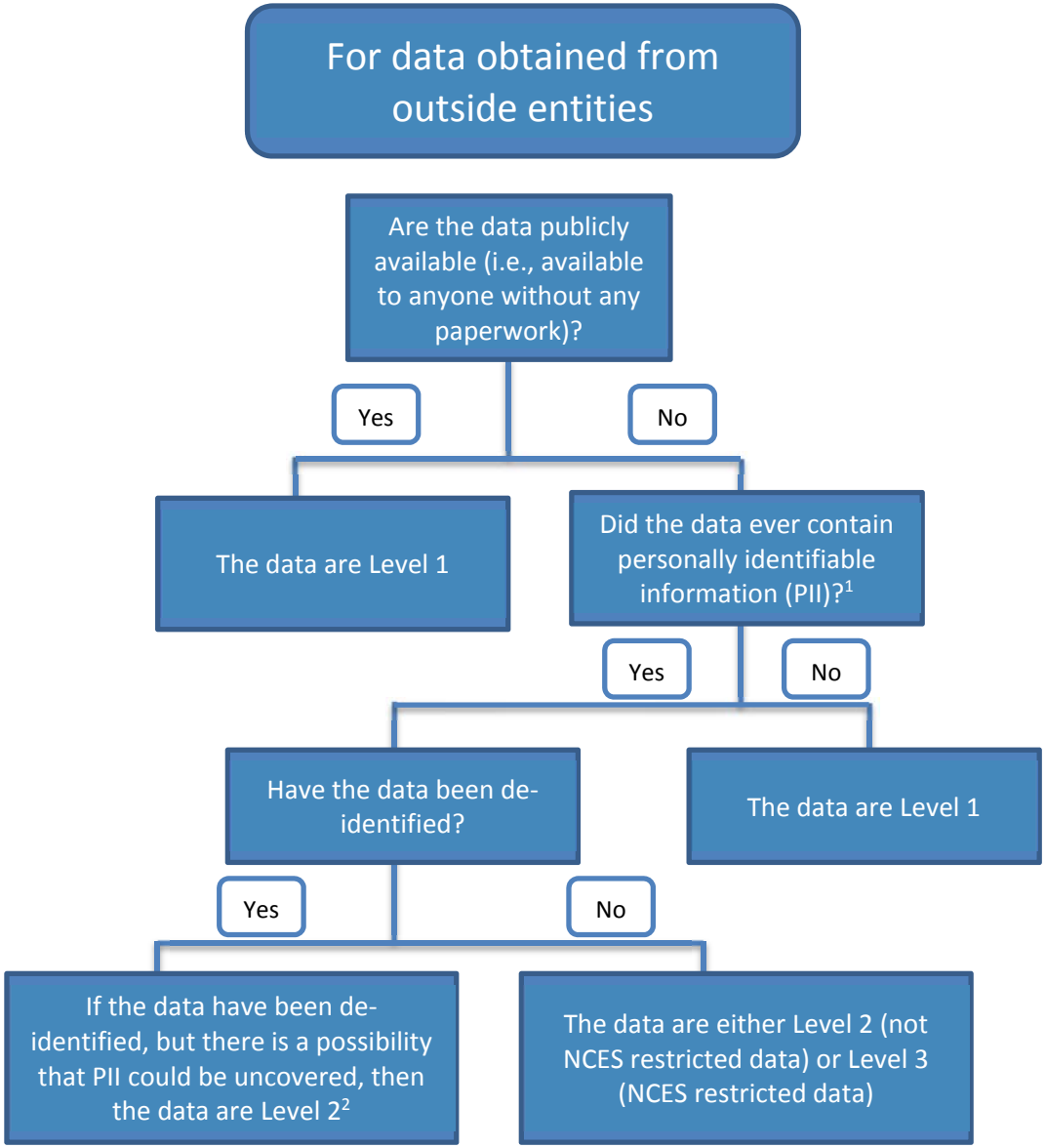
Child Trends' research data security policy is summarized in the table below. The standards contained in this table were adapted from the U.S. Department of Health and Human Services (HHS) and the National Center for Education Statistics (NCES). These represent standards *required* by the respective funding agencies. Standards are provided for the following elements of data security:

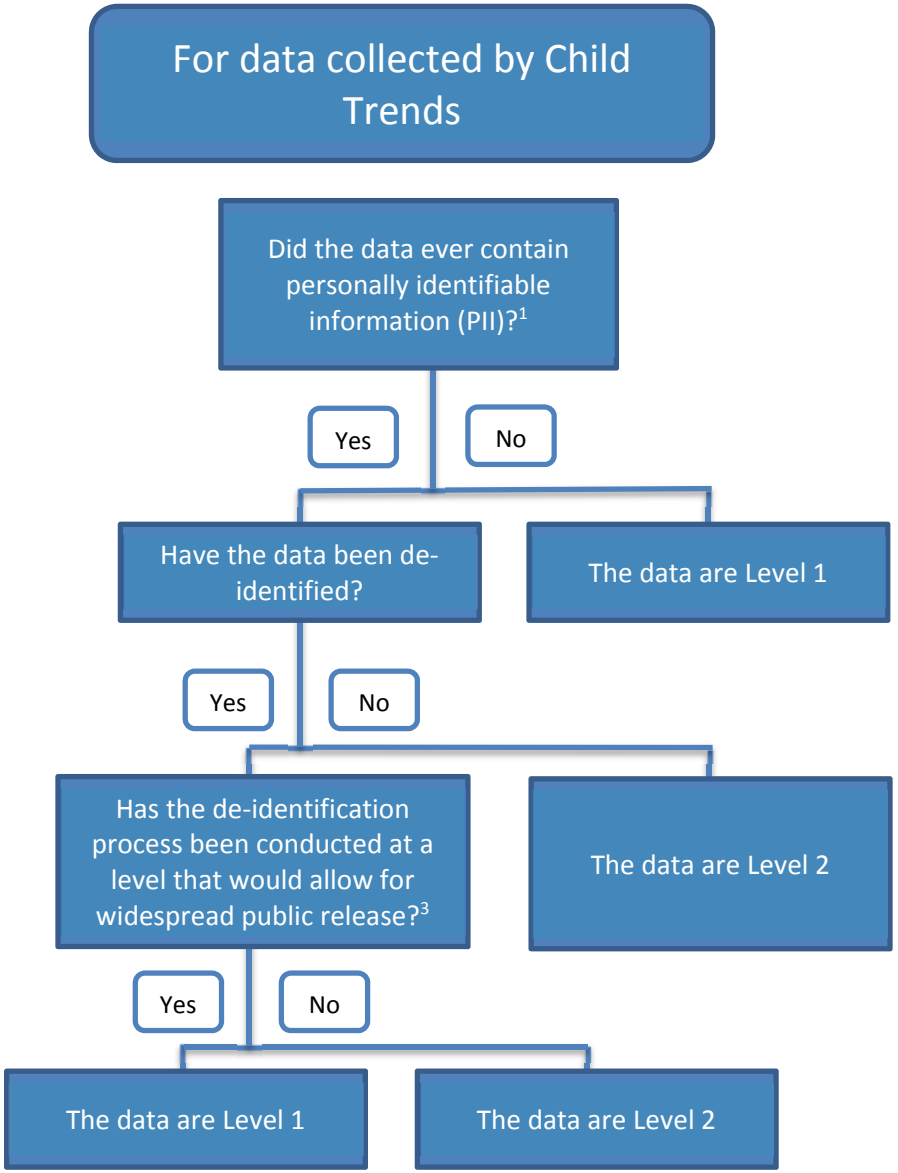
- Using passwords and screensavers
- Downloading and installing software
- Reporting viruses
- Securing physical facilities
- Maintaining confidentiality
- Collecting and receiving data
- Storing data after collection/receipt
- Sharing data
- Accessing data remotely
- Backing up data
- Removing data
- Using subcontractors/consultants
- Training

Child Trends categorizes secure data into three levels and builds the multi-tiered data security policy around these levels. The levels of data security are defined according to the funder, sensitivity, and presence of personally identifiable information (PII) in the data. Specifically:

- Level 1: Minimum Standard.
    - This is the baseline level of data security to which all Child Trends staff must adhere. This level of data security is applicable to researchers not currently working with data and those working with public, non-restricted use data files.
- Level 2: Strict Standard
    - This is the level when using data that include PII. Files may include administrative or restricted use data files as well as data collected by Child Trends, the federal government, state governments, or other entities.
- Level 3: NCES Standard
    - Researchers working with restricted use data from the U.S. Department of Education, Institute of Education Sciences (IES), National Center for Education Statistics (NCES) are required to adhere to Level 3 requirements. Those working with NCES on a project funded by HHS are also required to adhere to the standards listed for Level 3. Note that these standards are *mandated* by NCES for contractors and grantees.

To identify the level of your data, answer the following questions:





[1] Either now or before a de-identification process. The definition of PII is available on page 5. Note that PII includes information that can be triangulated to identify an individual. For example, if a study of school attitudes does not collect student names, but does collect race/ethnicity and grade level information, and there are only five Native American children in the district in five different grades, it would be possible to identify the students by triangulating the information; thus, you have PII.

[2] Due to the potential of triangulating multiple pieces of information in order to identify an individual, it can be extremely difficult to de-identify data in a way that eliminates all possibility of disclosure of an individual's identity.

[3] In other words, have the data been masked or aggregated to an extent that it would be impossible to identify an individual? Could you ethically post this data on a public website?

Child Trends research staff working with states or federal entities are responsible for knowing and abiding by the regulations of these entities.

Important: Please note that whenever 1) a licensing agreement with a data provider for the use of their data or 2) when a contract with a funder for a project involving the collection of original data dictates data security procedures that are stricter than those described in Child Trends policy, project staff MUST adhere to the requirements of the data provider/funder.

Child Trends' data security committee will work with principal investigators or project directors to determine which level of data security is most appropriate for their project given their data source, the presence of personally identifiable information (PII), the sensitivity of the data, and the funder. Once this level of data security is determined, the project director will consult the Research Data Security Policy to determine what data security measures are necessary. The project director will then assign one member of their research team to oversee the implementation of the project's data security plan. Additionally, Child Trends' IT provider has access to all data and Child Trends has a blanket confidentiality agreement with the IT provider for Level 1 and Level 2 data. Select staff at the IT provider also have access to Level 3 data.

Definitions

- **Personally Identifiable Information (PII):** "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.…" (OMB).[4] If the data include names, social security numbers, or addresses, for example, these data are personally identifying. The data may also be personally identifying even if they do not include this type of information. For example, let's say a study of school attitudes does not collect student names, but does collect race/ethnicity, and grade. If there are only five Native American children in the district and each is in a different grade, you now have PII. Due to the potential of triangulating multiple pieces of information in order to identify an individual, it can be extremely difficult to de-identify data in a way that eliminates all possibility of disclosure of an individual's identity. For this reason, data should be de-identified to the extent possible, and even after de-identification occurs we foresee that most data should be treated as Level 2 for data security purposes. Consult the IRB or data security committee if you need help assessing whether your data include PII.
- **Remote work server**: This server allows users to gain access to files on the Child Trends network from a remote location. A user who connects to the network from any connection outside a Child Trends office must first connect to the secure VPN network (i.e., NetExtender). If the user is using a Child Trends computer, no additional steps are necessary. If the individual is using a non-Child Trends computer, then it is necessary to connect to the work server through Remote Desktop Connection to access network files.
- **Remote access computer**: Any computer (PC or desktop) used to access Child Trends' network from outside of Child Trends' offices.
- **Data safe:** A safe secured in a separate, locked space that is used for storing CDs or other electronic forms of data. Only people who have permission from the data security committee and who have signed an NCES affidavit are permitted to have access to the data safe.
- **NCES secure data room:** The office within Child Trends' suite that is used for analysis of NCES restricted data. The computers in this room are not networked to non-NCES shared drives or the internet.

[4] See OMB http://www.whitehouse.gov/omb/memoranda/m03-22.html

	Level 1: Minimum Standard Public, Non-Restricted Data OR Other non-PII	Level 2: Strict Standard PII, Restricted Use Data (non-NCES) Administrative Data with PII De-identified data that could include PII through triangulation (see pg. 5 for definitions)	Level 3: NCES Standard NCES Restricted Data
Using Passwords & Screensavers	Passwords must contain a minimum of eight characters, including at least three of the following four types of characters: 1) one upper case letter, 2) one lower case letter, 3) one number, and 4) one non-alpha-numeric character. Passwords should not be dictionary words, names, or personal data. Passwords must be changed every 90 days, after an event of suspected compromise, or upon system installation. This password update will be automatically enforced. To change your password, hit CTRL+ALT+DEL and select "Change a password." Passwords must not be reused until at least 6 other passwords have been used. Password must be committed to memory or stored in a secure office space. After 5 incorrect attempts at entering a password, users will be locked out for 15 minutes or until they contact IT. Passwords should not be shared, unless with IT staff for the purposes of troubleshooting or system setup. If passwords are shared with IT staff, passwords should be changed immediately after IT staff are done assisting you. Screensavers are set to lock the computer or remote work server after a period of inactivity.	Same requirements as column 1; in addition: Users working in a public location are encouraged to lock their screen any time they leave their workstation.	Same as column 1; in addition the screensavers on computers in the secure data room should be a marquee setting with text: "Anyone who violates the confidentiality provisions of this Act shall be found guilty of a class E felony and imprisoned up to five years, and/or fined up to $250,000."
Downloading and Installing Software	Users must obtain permission from the system administrator before installing or downloading any non-business software. Staff should check with the IT provider if they are unsure about the security of a program. Rules for downloading and installing software only apply to computers owned by Child Trends.	Same requirements as column 1.	Same requirements as column 1.
Reporting Viruses	Users must inform IT or other designated staff immediately of any different or out of the ordinary behavior that a computer or application exhibits, or any virus detected. All Child Trends computers are protected by antivirus software. No user action is required to update or maintain the software. If you remotely access the Child Trends work server from a non-Child Trends PC, you need to have anti-virus protection.	Same requirements as column 1.	Same requirements as column 1.
Securing Physical Facilities	Child Trends suites are only accessible through key cards.	Same as column 1; in addition: Paper and portable media with secure data should be kept in a locked drawer/file cabinet. Users must ensure that no data is visible when others are present. If a computer or device is stolen or lost while a user is actively logged in to the remote work server, the user must report that loss immediately to IT, who will terminate the active remote session (all unsaved work will be lost). Losses should also be reported to the program area director.	All work with NCES data must be done in the NCES secure data room, which is not networked to non-NCES shared drives or the internet. The NCES secure data room must remain locked when unattended. The NCES secure data room can be accessed by staff on the NCES secure data license through a code punched into a number key pad. Only individuals on the Child Trends NCES license are allowed in the secure data room (except in the rare case in which building maintenance needs to be performed. In this instance, the maintenance person may work in the room as long as they are always accompanied by a

	Level 1: Minimum Standard Public, Non-Restricted Data OR Other non-PII	Level 2: Strict Standard PII, Restricted Use Data (non-NCES) Administrative Data with PII De-identified data that could include PII through triangulation (see pg. 5 for definitions)	Level 3: NCES Standard NCES Restricted Data
			Child Trends employee on the NCES license). Keep materials (printed output, etc.) that contain any personally identifiable information in a locked filing cabinet (if printing is mandatory) and shred the copies when finished using them. The data security committee should contact IES in case of suspected and confirmed breaches of security.
Maintaining Confidentiality	*Not applicable.*	Access to secure drives should be requested through the IT provider but will only be allowed once the Program Area Director (PAD) approves the user. A signed and completed confidentiality agreement for all data users is required by the IRB in some cases (see the IRB committee for more information). Note: Some projects may require signatures on additional confidentiality agreements/forms.	Employees must have an affidavit of nondisclosure on file with NCES prior to accessing NCES restricted data. Contact the data security committee to be added to the NCES license. Employees must read and understand the NCES security procedures before using data. Employees should have 3 documents on file, which you should be able to give someone during a spot check/audit: (1) Child Trends' license (2) Child Trends' data security plan form (3) A copy of your NCES affidavit. Employees should be able to tell an auditor that: Jennifer Manlove is the Principal Project Officer, the IT provider is responsible for day-to-day security of NCES data, and that Carol Emig is the Senior Official on our NCES license. Employees must be able to remember (and be able to tell an inspector) that anyone who violates the confidentiality provisions of this Act shall be found guilty of a class E felony and imprisoned up to five years, and/or fined up to $250,000. Data users are required to send any documents based on NCES licensed data to the IES data security office prior to dissemination to non-licensed individuals, cc'ing Jen Manlove (see 'sharing data' for more information).
Collecting and Receiving Data	*No requirements.*	A Child Trends computer or other device that meets security requirements must be used for data collection. Any PII collected should be saved to a secure drive as soon as possible. Any project collecting Level 2 data through an online survey platform (e.g., SurveyMonkey, SurveyGizmo, etc.) should restrict access to the data (e.g. by acquiring your own license) to prevent unauthorized access. Level 1 data can be collected using a Child Trends-wide account. No data should be saved to an external media device, such as a flash drive or voice recorder, unless the device is password protected. Encrypted devices are preferred if they are affordable and available. These devices can be obtained by either using project	When submitting a request for new data, please cc Jen Manlove. For information on how to request new or additional NCES data sets, contact the data security committee.

	Level 1: Minimum Standard Public, Non-Restricted Data OR Other non-PII	Level 2: Strict Standard PII, Restricted Use Data (non-NCES) Administrative Data with PII De-identified data that could include PII through triangulation (see pg. 5 for definitions)	Level 3: NCES Standard NCES Restricted Data
		funds or through discussion with the Overseer of IT. Current devices without password-protection capabilities may continue to be used until they need to be replaced. When new devices need to be acquired, they must have password-protection capabilities. Data should never be transferred from external devices to a non-Child Trends computer. Data should never be shared or transferred on Basecamp. Child Trends has a secure FTP site for sending and receiving level 2 data. Please contact IT for additional information.	
Storing Data After Collection/Receipt	*No requirements.*	Electronic data must be stored either on the secure server or in the data safe. In addition, document-level password protection is required for an additional layer of security for (1) consent forms that contain PII (names and/or contact information) and (2) files that are used as a "key" for PII and participant identifiers (i.e. "linking files"). Different passwords must be used for consent forms and linking files. It is encouraged that consent forms be scanned into one document. If they are stored in multiple documents, one password should be used for all of that project's consent forms. While a project is active, all secure project files (data, consent forms, linking files, etc.) should be stored in the project's folder on the secure drive. After the project ends, consent forms, linking files, and any other project-specific IRB files (along with passwords) should be transferred from the project folder to the IRB folder on the secure drive so they can be retained for the three years we are required to keep IRB-related documentation. Contact the IRB Committee for more information. Non-electronic data (e.g., data on paper) should be stored in a locked cabinet, and the location should be registered with the IRB in the IRB monitoring tool. Paper copies of linking files must be stored separately from other project files/data (different locked filing cabinets).Contact the IRB Committee for more information. Note: Every effort should be made to store data electronically ONLY and shred any hard copies of data. This includes the storage of consent forms.	All data CDs, DVDs, flash drives, disks, or tapes containing NCES data must be kept in the data safe. The data safe is in a locked cabinet in the locked NCES secure data room. Restricted data must be stored on the secure server in the NCES secure data room. The data safe is locked at all times and can be accessed by only a limited number of staff through a code punched into a number key pad. Please contact the data security committee if you need access to materials in the data safe.
Sharing Data	*No requirements. Sharing of data is permitted.*	Project staff must not disclose or share data on individual study participants with individuals/entities outside the project team (i.e., third parties), nor may they transmit or give data on individual study participants to third parties, unless allowed under the licensing agreement or IRB. When sharing is permitted and PII are not needed by the third party, Child Trends will de-identify individual data (such as names, birth dates, social security numbers, etc.) prior to sharing the data. Note that some de-identified data can still contain PII through triangulation (see notes about this on page 5). When sharing is permitted and PII are needed (e.g., funders may need PII data to do a follow-up survey), Child Trends will inform the	NCES restricted data should remain in the Child Trends NCES secure data room and should not be transported. NCES data cannot be transmitted electronically. Data users are required to send publications based on NCES licensed data to the IES data security office prior to dissemination to non-licensed individuals, cc'ing Jen Manlove. Publications can only be disseminated to people that are not on Child Trends' NCES license once IES approval is obtained. NCES will check that all unweighted sample size numbers are rounded to the nearest ten (nearest 50 for ECLS-B) in all information products (i.e.: proposals, presentations, papers or other

	Level 1: Minimum Standard Public, Non-Restricted Data OR Other non-PII	Level 2: Strict Standard PII, Restricted Use Data (non-NCES) Administrative Data with PII De-identified data that could include PII through triangulation (see pg. 5 for definitions)	Level 3: NCES Standard NCES Restricted Data
		recipient of the data of the importance and need to maintain individual study participants' confidentiality and will request that data recipients adhere to data security procedures that provide for a level of security similar to that of Child Trends' policy. Where possible, Child Trends will review recipients' data security policies for this purpose. Data on individual study participants collected by entities other than Child Trends and provided as secondary data to Child Trends (e.g., administrative data provided by state or local governments) may not be shared with a third party without a formal agreement with the data provider. PII data should never be shared or transferred on Basecamp. Child Trends has a secure FTP site for sending and receiving data. Please contact IT for additional information.	documents that are based on or use restricted use data). For all other datasets, including administrative datasets produced by other agencies within the Department of Education (e.g. EDFacts, CRDC, etc.), disclosure avoidance standards will vary. The required disclosure avoidance measures for these non-IES datasets will be listed in a readme.txt file included with that specific dataset. The product cannot be disseminated to non-licensed individuals until formally notified by IES that no potential disclosures were found (the review process usually takes 3 to 5 business days). Note that IES review is required even when sharing preliminary tables/output with Child Trends colleagues who are not on the NCES license.
Accessing Data Remotely	Remote access is permitted. All Child Trends employees must use the NetExtender software when accessing the remote work server.	Same requirements as column 1; in addition: Data users may have remote access to level 2 data unless the Project Director restricts such access.	Not applicable. No analyses of NCES restricted data may be conducted outside the secure data room.
Backing Up Data	Child Trends regularly backs up all data in the server room, which includes all drives. Backups of most servers occur incrementally 6 times per day (only files that have changed that day are backed up). One full backup is done each day. Backups are stored locally and in the cloud. No user action is required.	Same as column 1. No backup copies of data should be stored on individual workstations or on home computers. If you have data that should not be backed up, please contact IT and they will put it on a server that is not backed up.	Licensees are permitted to make 1 copy of each NCES restricted data set. Only 1 copy of the entire data set is allowed, no additional or partial copies are permitted. This copy must be kept in the data safe. No routine backups should be made of NCES restricted data.
Removing Data	Upon employee departure, administration and the IT provider will immediately disable all access and privileges to departmental systems, networks, and facilities. All retired work station hard drives get removed. They are demagnetized and the data is cleaned. The hard drives are then discarded.	Same requirements as column 1; in addition: Where required by project funders/owners of the data, users must work with IT to destroy electronic data when the project is completed or when data are no longer needed. If not defined in other documents, data should be destroyed within three years of study completion. Electronic data should be permanently deleted. For data stored on the Child Trends server this can be done by right clicking and selecting delete or pressing shift + delete. For data not stored on the Child Trends server (hard drive, flash drive, or other external media) you must use File Shredder, a free tool (http://www.fileshredder.org/), to securely delete the file. Destroy other media by physically shredding (e.g., shred paper copies or cut up CDs or DVDs). *Note: Where appropriate, every effort should be made to allow Child Trends to retain data for potential future use. When data are retained beyond the conclusion of a project, they should be de-identified (unless longitudinal follow-up is planned with study participants) to minimize risk of the disclosure of participants' identities.*	Return all original data to NCES at the end of the project or when the license expires. When an employee who is listed on the NCES license leaves Child Trends, they should be removed from the license immediately.

	Level 1: Minimum Standard Public, Non-Restricted Data OR Other non-PII	Level 2: Strict Standard PII, Restricted Use Data (non-NCES) Administrative Data with PII De-identified data that could include PII through triangulation (see pg. 5 for definitions)	Level 3: NCES Standard NCES Restricted Data
Using Subcontractors/ Consultants	No requirements.	Subcontractors are required to follow the same data security provisions as Child Trends. If subcontractors have access to PII, they must undergo training on Child Trends' Human Subjects Research Protection Policy or provide evidence of comparable training. Prime contractors are responsible for ensuring compliance by subcontractors. See the 'Sharing Data' row.	Subcontractors who wish to use NCES data at their sites must obtain their own authorization for use of NCES data. Consultants may access NCES data from Child Trends if the subcontractor is listed on our license and meets the other requirements.
Training	Staff shall receive an orientation to Child Trends' data security policy and be trained about how to implement all aspects of the policy. In addition, users will ensure that they receive any supplemental training required by a specific data provider, as dictated by data licensing agreements or other communications with data providers.	Same requirements as column 1.	Same requirements as column 1; in addition Users will receive training on NCES data security when signing their affidavit.