DaSy The Center for IDEA Early Childhood Data Systems

Data Governance and Management Toolkit

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Contents

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

INTRODUCTION

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Introduction to the DaSy Data Governance and Management Toolkit

Data Governance is the overall **management** of the availability, usability, **integrity**, quality, and security of data. **Data governance** is both an organizational process and a structure. It establishes responsibility for data, organizing program area/agency staff to collaboratively and continuously improve **data quality** through the systematic creation and enforcement of policies, roles, responsibilities, and procedures (from the **DaSy Glossary**).

What is the DaSy Data Governance and Management Toolkit?

The DaSy **Data Governance** and **Management** Toolkit is a resource containing information, guidance, and templates to assist Part C and Part B 619 program staff with creating or enhancing their **data governance** policies and procedures. The toolkit complements and addresses quality indicators within the **DaSy Data System Framework**.

Why is data governance important to Part C and Part B 619 Programs?

As state agencies increasingly use data for multiple purposes (e.g., administrative operations, reporting, monitoring, continuous **program improvement**, informing state policy issues) it is essential that they have clear policies and procedures about the availability, usability, **integrity**, quality, and security of the data. Clear **data governance** policies and procedures are needed at the state level to manage the Part C and Part B 619 data and how the data are used. Of particular importance, stewardship of personally identifiable information requires comprehensive Part C and Part B 619 **data governance**.

Will the toolkit be useful for different state structures?

The toolkit in intended to assist Part C and Part B 619 programs with different types of existing or proposed governance structures:

- In some states, the Part C or Part B 619 programs may have stand-alone **data governance**.
- In some states, the Part C or Part B 619 programs are contained within a larger **data governance** structure (e.g., Part B 619 program within a general education governance structure or a Part C program embedded within a health or other lead agency **data governance** structure).

What types of information are included in the toolkit?

The toolkit is organized into the following sections:

- **Purpose, Structure, Process**
- **Data Breach Response**
- **Data Security and Access**
- **Data System Changes**
- **Data Quality**

- Data Requests
- Electronic Communications
- Public Reporting
- Resources

What do the toolkit sections contain?

Each section contains:

- **Overview:** A short description of the data governance topic covered in the section and how it applies to Part C and Part B 619 programs;
- **Considerations:** Questions that will help programs draft policies and procedures for that data governance and management topic;
- **Template:** A downloadable template (in Microsoft Word) for creating policies and procedures related to that topic.
- (Planned) **State Examples:** As state examples are found relevant to each data governance topic, and states agree to share them, they will be included.

How should the toolkit be used?

Sections of the toolkit are logically sequenced, although it is not necessary to complete them sequentially. Furthermore, because sections are independent of each other, states can use any section as needed and work on sections in any order. Starting with Section 1 (Purpose, Structure, Process) is recommended to ensure the state has the necessary infrastructure in place to support Part C and Part B 619 data governance.

It is essential that staff first review the data governance structure and policies of their larger state agency. Part C and Part B 619 programs do not operate independently of the state agency in which they are housed. Thus, the structure of any data governance *already within an agency* is of particular importance. To find out whether your state has a data governance body whose scope includes Part C or Part B 619 data please refer to the DaSy State of the States map.

This toolkit accommodates Part C and Part B 619 programs anywhere along a data governance continuum from "no existing data governance" to "one of many programs in, and governed by, an agency with functioning data governance policies and procedures."

How can the toolkit be used in a state with no or limited data governance?

Where no, or nearly no, functioning data governance exists—related to Part C or Part B 619—the toolkit contains comprehensive resources for Part C or Part B 619 programs to establish a full set of policies. Such users are encouraged to review and use all sections of the toolkit.

- Read each part of each section (overview, considerations, and template).
- The overview establishes importance.
- Considerations provides suggestions to help states determine how data governance should work in their program.
- The template is fully editable and prepopulated with language to expedite writing policies. We recommend that you consult with relevant staff and stakeholders when

developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

How can the toolkit be used in a state that already has many existing data governance policies and procedures?

Where **data governance** policies are in place, Part C or Part B 619 programs might need only to review them.

- Use the consideration questions within applicable toolkit sections to ensure that they cover Part C or Part B 619 **data governance** needs.
- Policies might need to be updated with specific references or provisions related to Part C or Part B 619.
- In such cases where policies may need updating, the template in each section may be helpful in proposing language.

What if I need assistance completing the toolkit?

DaSy Center staff are available to provide states with assistance in using the toolkit and supporting states to develop or improve **data governance** policies and procedures.

Note: *Updates to this toolkit will be posted as they become available. If you wish to be contacted when a new version is released,* ***enter your email address in the "Keep Me Updated" form.***

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Purpose, Structure, Process Charter

Overview

Formal **data governance** for Part C or Part B 619 programs provides both program oversight functions organized into a decision-making structure and a process for **management** to develop, review, and implement **data governance** policies. A purpose, structure, and process charter outlines the approach to Part C or Part B program **data governance** and details basic information about the Part C or Part B 619 program and data system.

It is important to create clear purpose statements for both the Part C or Part B 619 data system and **data governance** structure.

- The data system purpose statement articulates the intended use of the data and informs decision-making, priorities, and communication with **stakeholders** throughout data **system development** and enhancement. It is often aspirational, describing how the data system will support the state's goal of improving outcomes for young children with disabilities and their families.
- The data governance structure purpose statement articulates the purpose of the data governance structure and outlines the scope of decision-making authority.

Detailing the structure and process provides the framework for who is involved in data governance decisions, how **data governance** policies are developed and support **management** of the data system. Through the development of a charter, this section of the toolkit provides the foundation to formalize and sustain **data governance** for Part C or Part B 619 programs. It provides a basis for understanding the context for decisions and a template for developing goals and strategies to support data **management** functions.

The Individuals with Disabilities Act (IDEA) does not require states to state a purpose, implement a **data governance** structure, or design a **data governance** process, but it does specify data collection requirements (relevant IDEA federal regulations are referenced in the template in this section). Formalizing the purpose, structure, and process guides states' development of clear policies and procedures, clarifies decision making authority, and outlines expectations for **management** of IDEA-related data.

A formalized **data governance** structure is charged with establishing policy and procedures for the overall **management** of the data and the data system. The **data governance** structure may be organized differently for Part C and Part B 619 programs depending on where the program is housed, where the data are located, and the extent to which the program is included in an overall agency **data governance** structure and processes. The **data governance** structure could be a state agency committee with designated representatives from each unit/division/section/program. The agency committee could be charged with overseeing **data governance** for all agency data-related efforts. In contrast, the **data governance** structure could be as simple as one or two key program staff members designated to oversee Part C or Part B 619 **data governance**. Regardless of the size or location of the Part C or Part B 619 program, the **data governance** structure must

be well defined to support a clear understanding of the hierarchy of roles and responsibilities, including decision-making authority.

Because Part C and Part B 619 programs do not operate independently of the state agency where they are housed, it is essential that program staff first review the state agency's **data governance** structure and policies. Part C or Part B 619 may fall within the purview of a **data governance** structure that already exists. In the absence of a state agency **data governance** structure, a program-level **data governance** structure should be created specific to Part C or Part B 619.

The DaSy Data System Framework emphasizes the importance of articulating the **purpose and vision** and establishing authority and scope of the data system(s) in the **Purpose and Vision** section, Quality Indicators **PV1** and **PV2**, and the **Data Governance** section, Quality Indicators **DG1**, **DG2**, and **DG3**.

Considerations

Use the considerations below to support discussion on how to:

- develop a comprehensive purpose statement for Part C or Part B 619;
- develop a **data governance** structure purpose statement;
- document the organization of the larger **data governance** structure that the Part C or Part B 619 program belongs to and how the program interacts with it or establish a program-level **data governance** structure; and
- outline the new program-level **data governance** process or how Part C or Part B 619 will interact with the larger **data governance** process.

These considerations should be discussed with appropriate state and local program staff, parents, and stakeholders. Additionally, if Part C or Part B 619 is part of a larger governance structure, the results of these discussions should be shared with members of that structure to increase awareness about the Part C and Part B 619 programs and to support future work on program data governance issues. Development of purpose, structure, and process does not require responses to all the considerations below to be effective. However, review of each applicable consideration will help ensure that Part C or Part B 619 programs draft a comprehensive and clear purpose, adequately describe the existing structure or establish a new program-level structure, and detail the data governance structure process.

Supporting documentation should be referenced as needed. Where appropriate, organizational charts and procedures and operations manuals detailing specific structures or actions supporting implementation should be created.

Addressing these considerations will support completion of the template following the considerations. The policy can be updated or amended later as needed.

Note: Some consideration questions are coded. "N" supports the development of a new program-based data governance structure. "E" supports issues related to an existing larger data governance structure. Questions without either code are general, to be addressed by all structures. Of course, states with existing data governance structures may also want to review the "N" considerations as best practice.

1. **Purpose, Structure, and Process Charter: Purpose**
   a. What federal legislation or executive actions allow or require Part C or Part B 619 programs to collect and manage early intervention or preschool special education data?
   b. What state legislation or executive actions allow or require Part C or Part B 619 programs to collect and manage early intervention preschool special education data?
   c. Where within the state departments/agencies is the Part C or Part B 619 program housed?
   d. What data system(s) is the Part C or Part B 619 program using?
   e. What is the funding source for the data system(s)?
   f. What is the purpose(s) of the data system(s) supporting your Part C or Part B 619 program relative to **accountability**, **program operations**, public reporting, and **program improvement**?
   g. Whom does the data system support? What audiences are informed by the outputs of the data system(s) (e.g., parents, program staff, state agency leaders, state legislators)?
   h. How does each **user group** use the data system?
   i. What is the purpose of the **data governance** structure?

2. **Purpose, Structure, and Process Charter: Structure**
   a. What committee, office, or individual(s) is charged with Part C or Part B 619 program **data governance**?
   b. What is the function of the **data governance** structure? (N)
      1. How does it establish policy and procedures for the overall **management** of the data and data system?
      2. How does it support decision-making authority?
      3. How does it inform policy determinations?
      4. How does it establish criteria for approving development and implementation plans?
      5. How does it support the review of system designs or changes?
   c. What is the extent of the **data governance** structure's authority?
   d. How does the **data governance** structure support oversight decisions or recommendations to higher levels that make decisions?
   e. Who (what roles) serves on the **data governance** structure?
   f. How many members does the structure include?
   g. How are the members determined (e.g., selected, appointed)? (N)
   h. Who (what role) is designated to represent Part C or Part B 619 on the larger **data governance** structure? (E)
   i. How does the existing **data governance** structure meet Part C or Part B 619 needs?
   j. Who (what role) has authority to make decisions about data systems/data collection?
   k. What is the role of participating agencies in Part C or Part B 619 in the **data governance** structure?
   l. Who (what role) has authority to make decisions (e.g., changes, enhancements, integration) about data systems/data collection?

3. **Purpose, Structure, and Process Charter: Process**
   a. What are the frequency, dates, location, and duration of **data governance** structure meetings that address Part C or Part B 619 data? (N)
   b. Where are meetings held?

c. How do the Part C or Part B 619 program staff members interface with their designated representative for the larger data governance structure to address program-level **data governance** needs? (E)
d. Which role(s) are involved in the decision-making process? (N)
e. What is the process for approvals or major decisions? (N)
f. How do interested parties submit issues for the **data governance** structure to address?
    1. What entity (role) are they addressed to?
    2. How are decisions regarding submissions communicated?
g. How is **data governance** information, including current and updated policies, made available to program staff, participating agencies, and **stakeholders**? (N)
h. What entity or role(s) is responsible for implementing the **data governance** policies created by the **data governance** structure?
i. What entity or role(s) is responsible for training and technical assistance on the data governance policies created by the **data governance** structure?
j. What entity or role(s) is responsible for monitoring the implementation of the **data governance** policies created by the data governance structure?
k. What entity (or role) is responsible for responding to **data governance** policy violations?

Use and modify this template as needed to develop a **data governance** purpose, structure, and process. Select the highlighted text and replace it with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Purpose and Structure Policy (Word document)

DaSy The Center for IDEA Early Childhood Data Systems

Data Governance Purpose and Structure Template

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Governance Purpose and Structure Charter for NAME OF PART C or PART B 619 PROGRAM

PURPOSE

The intent of this charter is to clearly define the purpose of the data system and the data governance structure. Additionally, it is intended to document the data governance structure and process.

AUTHORITY

The NAME OF PART C or PART B 619 PROGRAM is located within NAME OF STATE AGENCY. The NAME OF PART C or PART B 619 PROGRAM is authorized to collect and maintain EARLY INTERVENTION or PRESCHOOL SPECIAL EDUCATION data as part of the following federal and state statute and state executive orders.

Federal Statute

Part C: These Part C federal regulations authorize each state to have a system for compiling and reporting timely and accurate data.

- Each statewide system must include a system for compiling and reporting timely and accurate data that meets the requirements in §§303.700 through 303.702 and 303.720 through 303.724 regarding state monitoring, enforcement, state performance plans, data collection, use of targets, and annual reporting of children served. *[34 CFR 303.124(a)]*
- The data system required must also include a description of the process that the state uses or will use to compile data on infants or toddlers with disabilities receiving early intervention services under Part C, including a description of the state's sampling methods, if sampling is used, for reporting the data required by the U.S Secretary of Education under §§ 616 and 618 of the IDEA and §§303.700 through 303.707 and 303.720 through 303.724. *[34 CFR 303.124(b)]*
- In addition, the Part C regulations require each state to collect valid and reliable information as needed to report annually to the U.S Secretary of Education on the indicators established by the secretary for the State Performance Plans. *[34 CFR 303.701 (c)(1)]*

Part B 619: These Part B 619 federal regulations require each state to have a system for compiling and reporting timely and accurate data.

- Each state is to collect valid and reliable information as needed to report annually to the U.S Secretary of Education on the indicators established by the Secretary for the State Performance Plans. If the U.S. Secretary of Education permits sates to collect data on specific indicators through state monitoring or sampling, and if the state collects the data through state monitoring or sampling, the state must collect data on those indicators for

each local educational agency (LEA) at least once during the period of the State Performance Plan. *(34 CFR 300. 601 (b))*

- In addition, each state education agency(SEA) must

  (a) establish procedures to be used by LEAs and other educational institutions in counting the number of children with disabilities receiving special education and related services;

  (b) set dates by which those agencies and institutions must report to the SEA to ensure that the state complies with federal child count requirements;

  (c) obtain certification from each agency and institution that an unduplicated and accurate count has been made;

  (d) aggregate the data from the count obtained from each agency and institution and prepare the federal reports required; and

  (e) ensure that documentation is maintained that enables the state and the secretary to audit the accuracy of the count. *(34 CFR 300.645)*

State Statute

INSERT STATE STATUTE

State Executive Order

INSERT STATE EXECUTIVE ORDER

The NAME OF PART C OR PART B 619 PROGRAM implemented the NAME OF DATA SYSTEM INSERT INFORMATION ON HISTORY, INCLUDING KEY DATES . *[OPTIONAL]* The NAME OF DATA SYSTEM is supported by PROGRAM FUNDING SOURCE.

4. PURPOSE of DATA SYSTEM

The NAME OF DATA SYSTEM will allow for collection and maintenance of IDEA-related data, including (INSERT TYPES OF DATA). These data will be to INSERT USES OF THE SYSTEM. The NAME OF DATA SYSTEM is intended to be used by the following groups for the stated purpose:

User Group	*Purpose*

STRUCTURE

5. PURPOSE of DATA GOVERNANCE STRUCTURE

The NAME OF STATE/PROGRAM DATA GOVERNANCE STRUCTURE is granted authority and responsibility for the formal oversight and governance of the NAME OF DATA SYSTEM. The duties of the NAME OF STATE/PROGRAM DATA GOVERNANCE STRUCTURE are to MAKE POLICY DETERMINATIONS, APPROVE DEVELOPMENT AND IMPLEMENTATION PLANS, REVIEW SYSTEM DESIGNS OR CHANGES, ESTABLISH PROCEDURES FOR DATA RELEASE, [OTHER DUTIES]. *[OPTIONAL]* The NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE will report to NAME OF LEGISLATIVE GROUP OR INDIVIDUAL REQUIRING REPORTING as required.

The NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE is composed of XX members from the roles listed in the table below. Members are INSERT HOW SELECTED OR APPOINTED.

Role	*Definition*
ROLE	
ROLE	
ROLE	

Part C OR Part B 619 is represented on the larger data governance structure by INSERT ROLE. The following table includes critical information about each data collection to support basic understanding about the data system and to designate who (what role) has decisionmaking authority related to certain data governance functions. Each column represents specific data collections or data systems.

	Insert Name of Collection/Data #1	*Insert Name of Collection/Data #2*
Primary purpose	*(insert purpose)*	*(insert purpose)*
Time and frequency	*(insert time and frequency)*	*(insert time and frequency)*
Data collected (Child, family, program/services, workforce, finance, accountability, etc.)	*(insert type of data collected)*	*(insert type of data collected)*
Level of source data received by state (Individual record, aggregate)	*(insert level of collection)*	*(insert level of collection)*
Location of state data	*(insert location of data)*	*(insert location of data)*
Name of data system where located (if regular collection)	*(insert name of system where located)*	*(insert name of system where located)*

	Insert Name of Collection/Data #1	*Insert Name of Collection/Data #2*
Who (what role) is responsible for the data at the state level (data steward or owner)?	*(insert role)*	*(insert role)*
Who (what role) decides what data are collected?	*(insert role)*	*(insert role)*
Who (what role) decides how data collected?	*(insert role)*	*(insert role)*
Who (what role) decides when a report is complete?	*(insert role)*	*(insert role)*
Who (what role) approves internal agency data requests?	*(insert role)*	*(insert role)*
Who (what role) approves third-party (external) data requests, including LEAs?	*(insert role)*	*(insert role)*
Who (what role) approves data sharing agreements?	*(insert role)*	*(insert role)*

PROCESS

1. *Meeting Information*
   The NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE will meet INSERT FREQUENCY STANDING DATE, LOCATION, AND TIME OF MEETING.

2. *Coordination with Assigned Part C OR Part B 619 Representative for Larger Governance Structure*
   Part C OR Part B 619 interact with the NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE through assigned representative by INSERT STRATEGIES, MEETINGS, PROCESS.

3. *Responsibilities and Decision Making Authority and Process Within Governance Structure*
   The table above outlines the roles at each decision making level of the NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE. The responsibilities of each INDIVIDUAL, GROUP, COMMITTEE, ETC., are outlined below, including expectations for reporting and approvals.

   - ROLE: RESPONSIBILITIES (FUNCTIONS, DUTIES, REPORTING STRUCTURE)
   - ROLE: RESPONSIBILITIES (FUNCTIONS, DUTIES, REPORTING STRUCTURE)
   - ROLE: RESPONSIBILITIES (FUNCTIONS, DUTIES, REPORTING STRUCTURE)
   - ROLE: RESPONSIBILITIES (FUNCTIONS, DUTIES, REPORTING STRUCTURE)

The process for decision making is INSERT DECISIONMAKING PROCESS.

4. *Responding to Issues Raised by Interested Parties*

Interested parties may submit data governance issues to the NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE by INSERT METHOD. All submissions should be addressed to INDIVIDUAL, GROUP, COMMITTEE, ETC. Responses will be INSERT PROCESS.

5. *Communicating Data Governance Policy Changes*

Part C and/or Part B 619 staff, participating agency staff, and stakeholders are informed about data governance policies (current and revisions) through INSERT PROCESS OR MECHANISM.

6. *Implementation of, Training About and Compliance with Data Governance Policies*

INDIVIDUAL, GROUP, COMMITTEE, ETC., is responsible for the implementation of data governance policies created by NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE.

INDIVIDUAL, GROUP, COMMITTEE, ETC., is responsible for training and technical assistance on the data governance policies created by NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE.

INDIVIDUAL, GROUP, COMMITTEE, ETC., is responsible for the monitoring implementation of the data governance policies created by NAME OF PART C OR PART B 619 DATA GOVERNANCE STRUCTURE.

INDIVIDUAL, GROUP, COMMITTEE, ETC., is responsible for responding to data governance policy violations.

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Data Breach Response

Overview

Data breaches are not the concern of just information technology staff; they are the concern of everyone who has access to and handles Part C/Part B 619 data. A **data breach** may take numerous forms, from inadvertent **disclosure** of **personally identifiable information (PII)** to intentional hacking. Even the physical loss of a laptop computer with **PII** through negligence or theft can constitute a breach. Regardless of the type or magnitude, the ultimate effect of a breach is the same: greater risk of malicious **data use** and reduced institutional confidence. Those whose **PII** is released risk having their information accessed and used for any number of nonauthorized and potentially negative purposes including but not limited to identify theft, undesired solicitations, or residence location found by those with adverse intentions. Not only can a breach have significant negative effects on children and families, it can also negatively affect program staff, program functions and the state agency as a whole. Specifically, public awareness of a **data breach** can hamper subsequent efforts to collect and use Part C/Part B 619 data that are important to the agency's goals and long-term positive results.

The *DaSy Data System Framework* emphasizes the importance of data security — including prevention of data breaches — in the **Data Governance** section, Quality Indicators **DG6**, **DG7**, and **DG8**.

Of course, like insurance, the best data breach response policy is the one never used. Establishing and maintaining high levels of data security and data authorization reduce the risk of data breach. However, even with robust security policies and procedures, data are vulnerable to theft, loss, and unauthorized use. A data breach can happen at any time to data stored at any level. Therefore, an agency must have a data breach response policy regardless of whether data are stored internally, in the cloud, or with a third-party vendor.

Data breach: Any instance in which there is an unauthorized release or access of **personally identifiable information (PII)** or other information not suitable for public release. (**Privacy Technical Assistance Center**)

A **data breach** response policy establishes a set of procedures to be followed in the event of a **data breach**: how and when the breach should be reported to authorities, how and when to inform the public—specifically those at risk because of the **data breach**, recommendations to the public to reduce the post-breach risk, sanctions the agency might consider if warranted, and strategies to minimize future risk of a breach.

Other federal non-educational requirements, including Medicaid and the **Health Insurance Portability and Accountability Act (HIPAA)**, may also apply with respect to data security and data breaches. Additionally, **almost every state has a data breach law** that should be included in a **data breach** policy for Part C/Part B 619 programs.

Part C and Part B 619 programs do not operate independently of the state agency in which they are housed. Thus, the structure of any **data governance** already within an agency is of particular importance. Before developing a **data breach** response policy, Part C and Part B 619 programs should review any policies regarding data breaches developed by the agency in which their program resides. Existing policies might need to be updated with specific references or

provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language.

Where no policy on **data breach** response exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new **data breach** response policies.

Considerations

Use the questions below to discuss, consider, and develop a comprehensive **data breach** response policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created. (See the **PTAC Data Breach Response Checklist**.) In developing the policy, it is important to consider responses proportional to the different types and magnitudes of data breaches. For example, if in the course of a workday a person without training and **authorization** viewed a computer screen with **PII**. A measured course of action could be to talk to the agency staff member who did not follow policy regarding locking the computer screen when away from his/her desk. A disproportional response might be to contact the individuals whose **PII** was exposed.

A **data breach** response policy need not address all the questions below to be effective. However, considering each question will help ensure that states/programs draft a comprehensive policy with detailed procedures. The policy should be updated or amended at a later date as additional breach scenarios or risks surface.

1. Data Breach Response Policy: Scope

a. How does this policy align with any existing state policy and/or broader state agency data breach response policies?
b. What Part C/619 data are included/covered by this data breach response policy?
c. What constitutes an unauthorized release or access of personally identifiable information (PII) (e.g., unauthorized copying of data, system hacking, unauthorized data viewing, loss of flash drive or laptop with data)?
d. Who must adhere to the data breach response policy (e.g., staff, participating agencies, vendors, contractors)?
e. Are there binding clauses in contracts with vendors regarding data breach responsibilities?
f. Do training/policies exist for agency staff?

2. Data Breach Response Policy: Responsibility

a. Who (what role) is responsible for informing Part C/619 staff and ensuring their compliance with the data breach response policy?
b. If a Part C/Part B 619 data breach is suspected, who (what role) is responsible for investigating and confirming it?
c. What team or individuals are responsible for authorizing and carrying out the actions of the data breach response?
d. What monitoring/tracking will occur to ensure policy compliance? What monitoring documentation is needed?

3. Data Breach Response Policy: Data Breach Immediate Actions

a. Who (what role) reports a Part C/619 data breach to administration?
b. When shall a data breach be reported internally?
c. Under what circumstances shall a data breach be reported to individuals potentially at risk?
d. Under what circumstances shall a data breach be publicly reported?
e. How should a data breach be reported to those at risk? To the public?
f. When will individuals and/or public be notified?
g. Who (what role) will notify individuals and/or public about the data breach?

4. Data Breach Response Policy: Post Breach Actions

Under what circumstances will sanctions/consequences be levied on those responsible for the Part C/Part B 619 **data breach**?

a. What procedures will be taken to prevent similar data breaches in the future (e.g., investigation, process review, training, security measures)?
b. What are the projected timeline and process for implementing these response procedures?

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

See *Toolkit:* **Data Security and Access** for policies and procedures that may be reviewed in the event of a **data breach**.

Data Breach Policy Template

Use, and modify as needed, the template linked below for developing a **data breach** response policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Data Breach Response Policy

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Breach Response Policy Template

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Breach Response Policy for NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this data breach policy is to establish authority and a framework for responding to any data breach that may occur, notwithstanding the reasonable efforts to prevent such a breach.

BUSINESS CASE

Federal (AND POTENTIALLY NAME OF STATE) laws require reasonable efforts to secure and protect certain information that the agency possesses, thereby protecting the integrity and confidentiality of any such maintained information.

DEFINITIONS

For purposes of this policy, a data breach is "any instance of an unauthorized release of or access to personally identifiable information (PII) or other information not suitable for public release" that the PART C/PART B 619 PROGRAM NAME collects, maintains, manages, operates control over, and/or otherwise oversees.[1]

A data breach may occur from but is not limited to unauthorized data copying, unauthorized dissemination, system hacking, unauthorized data viewing, loss of physical data (e.g., loss of laptop computer, flash drive), accidental release of data, and accidental (unsecured) access to data.

SCOPE

Various federal (AND POTENTIALLY NAME OF STATE) laws (statutes/regulations/rules/ policies) apply to security and breach situations depending on the data to be protected. The NAME OF STATE statutes that address a breach of information security are

- RELEVANT STATUTE 1
- RELEVANT STATUTE 2
- RELEVANT STATUTE 3

This data breach response policy applies to NAME OF DATA TYPE(S), which are collected, maintained, managed, operated, or otherwise controlled by PART C/PART B 619 PROGRAM NAME, WITHIN AGENCY NAME(S). This data breach response policy specifically excludes

- NAME OF DATA TYPE 1
- NAME OF DATA TYPE 2
- NAME OF DATA TYPE 3
- NAME OF DATA TYPE 4

[1] http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf

This data breach response policy applies to WHO IS COVERED BY POLICY – STAFF, PARTICIPATING AGENCIES, VENDORS, CONTRACTORS, ETC., that collect, maintain, manage, operate, or are otherwise active in the control of NAME OF DATA TYPE(S) that if breached would trigger notification. This may include staff from NAME OF LOCAL PROGRAMS directly associated with NAME OF PARTICIPATING AGENCY(IES). If such local programs are named, all such programs must adhere to this policy including actions listed below in response to a data breach.

RESPONSIBILITY

Anyone observing what appears to be a data breach, including a breach of security designed to protect such data, potential or actual violation of other federal or state data law/statute/regulation/rule/policy, theft of hardware and/or software designed to house and protect data, unauthorized duplication of data, or any action placing the state or state resources at risk pursuant to this data breach policy, must immediately report the incident to an appropriate-level supervisor, manager, or security officer within their organization.

ROLE, GROUP, COMMITTEE, ETC is responsible for informing and ensuring that staff follow the intent of this policy and adhere to all related procedures including the provision of training and technical assistance. ROLE, GROUP, COMMITTEE, ETC is responsible for investigating and confirming any data breach. ROLE, GROUP, COMMITTEE, ETC are charged with carrying out the actions within this data breach response policy. ROLE, GROUP, COMMITTEE, ETC is responsible for monitoring adherence to this policy and will document such monitoring by INSERT MONITORING PROCEDURE.

IMMEDIATE ACTIONS

In the event of a data breach, all the following actions shall be considered and those deemed applicable by ROLE, GROUP, COMMITTEE, ETC shall be implemented:

1. As it is the responsibility of anyone COVERED BY THIS POLICY: STAFF, PARTICIPATING AGENCIES, VENDORS, CONTRACTORS, ETC., to report a data breach or potential data breach, and when such breach has been confirmed, ROLE, GROUP, COMMITTEE, ETC shall report such breach to ROLE, GROUP, COMMITTEE, ETC, including all appropriate agency heads and the AGENCY DIRECTOR.
2. Any confirmed breach shall be reported immediately.
3. GROUP, COMMITTEE, ETC shall convene as soon as possible to consider all options of informing both individuals potentially at risk based on the breached data and, if warranted, the public at large.
4. When individuals potentially at risk based on the breached data and/or the public at large are to be informed, ROLE, GROUP, COMMITTEE, ETC and AGENCY DIRECTOR shall determine when and how such notification shall occur.

POST BREACH ACTIONS

After any notifications have occurred, ROLE, GROUP, COMMITTEE, ETC shall consider and may implement any of the following post breach actions:

1. ROLE, GROUP, COMMITTEE, ETC and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for the data breach including but not limited to discussing the circumstances, formal reprimand, administrative leave, dismissal, criminal charges.
2. ROLE, GROUP, COMMITTEE, ETC shall review the data breach and determine what and when procedures shall be taken to prevent or minimize risk of similar data breaches in the future.
3. An agency that has a security policy in place and maintains a breach response policy and procedures consistent with the requirements of NAME OF RELEVANT STATUTE(S) shall be in compliance with the requirements of this policy.

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Data Quality

Overview

Part C and Part B 619 programs rely on data to inform decisions on **program improvement**, track child and family progress, and report performance to federal, state, and local policymakers and other **stakeholders**. Using inaccurate or poor quality data to report on program performance or make decisions will result in erroneous conclusions. Therefore, it is necessary to have comprehensive policies and procedures to ensure high-quality data—data that are accurate, consistent, timely, and complete.

The importance of **data quality** is addressed by the U.S. Department of Education's Implementing Regulations for Part C programs as follows: "Each statewide system must include a system for compiling and reporting timely and accurate data…" (34 CFR 303.124(a)). In addition, Part C regulations at 303.723 require the lead agency to submit a certification signed by an authorized official of the agency that the information provided, "is an accurate and unduplicated count of infants and toddlers with disabilities receiving early intervention services." These regulations require that **data quality** be a high priority for Part C and Part B 619 programs.

A comprehensive approach to **data quality** involves the intersection of people, processes and data system(s).

Definition
Data Quality: A multi-dimensional measurement of the adequacy of a particular datum or data sets based on a number of dimensions including, but not limited to **accuracy**, completeness, consistency, and timeliness.
Source: **BusinessIntelligence.com**.

People (roles/responsibilities): Individuals at the state or local level who collect, enter, prepare, analyze, report, and/or access data are responsible for ensuring that the data are and remain of high quality. Policies should communicate role expectations, outline **data quality** monitoring responsibilities, and prepare for staff transfer of knowledge when there is staff turnover. It is important that **data governance** policies for **data quality** include training and professional development opportunities for anyone who collects, maintains, or uses Part C or Part B 619 data.

Processes: Part C and Part B 619 programs need to have clearly documented and consistently applied processes and procedures to support **data quality** through summarizing, analyzing, and reporting of data. Included in **data quality** processes should be regularly updated documentation (data entry manuals, data dictionaries, tip sheets), continuous **data quality** monitoring and checks/audits, and procedures for correcting **data quality** issues when discovered.

Data system(s): Data systems used by Part C or Part B 619 programs should have the capability to perform automated edit checks to reduce data entry errors (e.g., such as having predefined option sets, acceptable response ranges, etc.). That is, when a person is entering data, the data system automatically identifies data entry values that are questionable so they can be confirmed or corrected as soon as possible. The system should generate reports at all levels (child record, provider, agency, etc.) to help identify potential data errors.

Data governance policies that address **data quality** must clearly communicate expectations for how data are to be collected, entered, prepared, analyzed, and reported. For effectiveness, **data quality** policies should specify responsibilities for specific **data quality** actions, the processes associated with these actions including timelines, and how the data system contributes to **data quality**.

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any **data governance** already within an agency is of particular importance. Before developing any **data quality** policy, Part C and Part B 619 programs should review policies regarding **data quality** developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose.
Where no policy on **data quality** exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new **data quality** policies.

The *DaSy Data System Framework* emphasizes the importance of **data quality** in the **Data Governance** section, Quality Indicator **DG4** & **DG5**, in the **System Design** and Development section, Quality Indicator **SD4**, and in the **Data Use** section, Quality Indicator **DU2**.

Considerations

Use the questions below to discuss, consider, and develop a comprehensive **data quality** policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created.

1. Data Quality Policy: General Provisions

a. Which federal laws/regulations (IDEA/**FERPA**) related to **data quality** apply to your Part C or Part B 619 program?
b. Are there additional state agency policies related to **data quality** that apply to the Part C or Part B 619 program? If yes, what are they?
c. What specific Part C or Part B 619 **data quality** policies or procedures, if any, exist and apply?
d. Which role, within what agency/program should be contacted with questions about this policy?
e. Which role, within what agency/program is responsible for ensuring adherence to this policy?
f. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
g. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
h. What consequences, if any, will apply when this policy is not followed?
i. How often will this policy be reviewed for necessary revisions?
j. How will the public be informed about this policy? Where will it be posted on the state's website?

2. Data Quality Policy: Responsibility

a. Which role, within what agency/program is responsible for overseeing and monitoring **data quality** for the overall data system and for particular data collections?
b. What participating agencies, if any, will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?
c. Which role, within what agency/program develops and revises **data quality** policies and procedures/manuals?
d. Which role, within what agency/program is responsible for creating and reviewing Part C or Part B 619 data reports to determine whether data are of acceptable quality?
e. Which role, within what agency/program is responsible for responding to end **users' data quality** questions?
f. Which role, within what agency/program is responsible for correcting **data quality** issues once **data quality** problems/issues have been identified or reported?
g. Which role, within what agency/program is responsible for communicating about **data quality** issues/problems to **data governance** group(s), local programs and **stakeholders**?
h. Which role, within what agency/program is responsible for ensuring adherence to **data quality** procedures when data are exchanged or transferred?
i. Which role, within what agency/program is responsible for training/retraining staff on the importance of **data quality** and how to identify **data quality** issues/problems? What content is delivered at trainings and how are they conducted?

3. Data Quality Policy: Processes

a. What processes/procedures are in place to ensure that data are accurate, consistent, timely, and complete?
b. What documentation exists that details how data are collected and entered into the data system (e.g., data entry manuals, data dictionaries, tip sheets)?
c. What kinds of regular **data quality** checks/audits are completed by Part C and/or Part B 619 staff? How often is each check completed?
d. What mechanism is in place for end **users** to report **data quality** issues/problems?
e. How are **data quality** issues resolved/corrected?
f. If **data quality** issues/problems are identified, what process is in place to prevent future **data quality** issues/problems (e.g., training/retraining of staff, changes to the data system, document updates)?
g. How are **data quality** issues communicated to local programs and **stakeholders**?
h. How often are **data quality** policies reviewed and updated?
i. What process is used to obtain input from **users** and other **stakeholders** when reviewing and revising **data quality** policies?

4. Data Quality Policy: Data System(s)

a. What automatic edit checks are built into the data system(s) to help ensure data are entered accurately (e.g., predefined option sets, field definitions, out-of-range checks, error messages)?
b. What reports in the data system(s) are used and/or needed to help identify outliers, data anomalies, errors, or inconsistencies?
c. How is input (reviews, testing, feedback) obtained from **users** as revisions are considered in system edit checks or reports that detect **data quality** issues?

Data Quality Policy Template

Use, and modify as needed, the template linked below for developing a **data quality** policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Data Quality Policy

DaSy The Center for IDEA Early Childhood Data Systems

Data Quality Policy Template

This page intentionally left blank

Data Quality Policy

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this data quality policy is to establish authority and a process for ensuring PART C OR PART B 619 are accurate, consistent, timely, and complete within the data system supporting the PART C/PART B 619 PROGRAM NAME.

DEFINITIONS

Data quality refers to a multi-dimensional measurement of the adequacy of a particular datum or data sets based on a number of dimensions including, but not limited to accuracy, completeness, consistency, and timeliness.

AUTHORITY

NAME OF STATE is federally required to collect and report PART C OR PART B 619 data and collects such data through data systems noted in the table below. The following federal (AND POTENTIALLY NAME OF STATE) requirements (statutes/regulations/rules/policies) apply to data quality:

Federal regulations are IDEA regulations for Part C at 34 CFR 303.124(a) and 34 CFR 303.723 and Part B at 34 CFR 300.643.

The NAME OF STATE/PROGRAM statute, regulations, and current policies that address data quality are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. to oversee the data for the PART C/PART B 619 PROGRAM NAME and carry out or oversee required data quality processes to help ensure that the individuals involved with the data (e.g., internal staff, external staff, vendors) are equipped to support and maintain high data quality. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this data quality policy.

PART C/PART B 619 PROGRAM NAME Data System(s)

1. ***(insert program name)***
2. ***(insert program name)***
3. ***(insert program name)***
4. ***(insert program name)***
5. ***(insert program name)***
6. ***(insert program name)***

AGENCY, PROGRAM, ROLE, ETC. is responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM data systems. AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to this policy through REVIEW OF DATA QUALITY

REPORTS, REVIEW OF DATA QUALITY ISSUES REPORTED, ETC.. Data quality policy questions will be addressed by AGENCY, PROGRAM, ROLE, ETC.. AGENCY, PROGRAM, ROLE, ETC. who will also secure or provide training and technical assistance on data quality when requested. This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

The public will be informed about this policy through AGENCY WEBSITE, MANUAL, ETC..

The table below outlines specific roles and responsibilities related to data quality:

Data Quality Responsibility	Responsible Entity
Overseeing, developing and/or revising data procedures, manuals, and support documentation for those involved with processing and reporting the data	*(insert agency, program role, etc.)*
Creating and reviewing data quality reports including identifying data quality issues during regular and ad hoc data reviews	*(insert agency, program role, etc.)*
Reviewing and responding to reports of data quality questions/issues	*(insert agency, program role, etc.)*
Correcting data quality issues once problems/issues have been identified or reported	*(insert agency, program role, etc.)*
Reporting the findings to data governance group, local program directors, IT staff, etc.	*(insert agency, program role, etc.)*
Ensuring adherence to data quality procedures when data are exchanged or transferred	*(insert agency, program role, etc.)*
Training/Re-training of all staff that routinely access, process, and/or use the data and data systems.	*(insert agency, program role, etc.)*

(add other responsibilities as needed)

Training should include orientation for new staff on the content and use of: DATA DICTIONARY, DATA ENTRY REQUIREMENTS, IMPORTANCE OF ACCURACY AND CONSISTANCY OF DATA ENTRY, ETC. Trainings are conducted via ONSITE, FACE-TO-FACE, DISTANCE TECHNOLOGY, PRE-RECORDED WEBINAR, ETC..

APPLICABILITY

This policy applies to those who collect, maintain, use, manage, operate, report or are otherwise active in the control of data regardless of format. This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING

AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. These entities and the mechanism (regulation/contract/interagency agreement) that make this policy applicable to each program/agency are listed in the table below.

Entities Covered by Policy	Mechanism
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*

PROCESSES

Data Dictionaries/Business Rules Manuals

All users have access to NAME OF DATA SYSTEM 's NAME OF DATA DICTIONARY/MANUAL/TRAINING RESOURCE which explains all associated data processes and timelines including:

- ENTERING/UPLOADING DATA INTO THE SYSTEM, ENSURING ACCURACY OF DATA BEING ENTERED/UPLOADED, CONDUCTING STEP BY STEP DATA ANALYSIS FOR STANDARD REPORTS (THAT ARE NOT SYSTEM GENERATED), ETC.

Data dictionaries will include DEFINITIONS OF EACH DATA FIELD INCLUDING THE TYPES OF DATA THAT CAN BE ENTERED, OPTION SETS, DATA FORMATS, ETC.. These resources can be found WEB-BASED, EMAILED, LOCAL INTRANET, DATA SYSTEMS, HELPDESK, ETC.

Data Quality Reviews

Data quality reviews/checks will be conducted by AGENCY, PROGRAM, ROLE, ETC. on a REGULAR/MONTHLY/VARIED schedule. The table below outlines the types of data reviewed, the responsible group or individual, and how often the data are reviewed:

Type of Data	Responsible Entity for This Data Quality Review	Method*	How Often?
EXAMPLE: Child Outcomes Data	*Data Manager*	*System-generated report*	*Monthly*

**Methods used to review the data to ensure quality can include:*

- *Matching data across sources (e.g. matching paper form data with data entered in data system)*
- *Analyzing data over time to look for trends*
- *Running frequencies to identify incorrect or missing data*
- *Generating reports to review with leadership and staff*

Data Quality Problems/Issues

System users can report data quality issues via EMAIL, PHONE CALL, STANDARD FORM, ETC.. to AGENCY, PROGRAM, ROLE, ETC..

When the AGENCY, PROGRAM, ROLE, ETC. has been alerted to or identifies potential data quality problems/issues, they will report those to AGENCY, PROGRAM, ROLE, ETC.. It will then be the responsibility of AGENCY, PROGRAM, ROLE, ETC. to determine the best methods for correction. The methods for correction can include:

- MAKING CHANGES/CORRECTING DATA/COMPLETING INCOMPLETE DATA AT THE DATA SYSTEM LEVEL, REQUESTING THAT LOCAL PROGRAMS MAKE THE NECESSARY CHANGES, ETC.

It will be the responsibility of AGENCY, PROGRAM, ROLE, ETC. to communicate data quality issues to local programs and stakeholders via EMAIL, NEWSLETTER, MEETING, ETC.. They will also follow-up on any reports of data quality issues, and ascertain that the corrections have been made once identified.

Data quality processes, including data dictionaries, manuals, and business rules, will be reviewed and/or updated at ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM,

ROLE, ETC.. Changes will be communicated to users and stakeholders via NEWSLETTERS, MEETINGS, ETC..

DATA SYSTEM

NAME OF DATA SYSTEM has several automated mechanisms in place to identify possible data quality issues/problems. These include:

- EDIT CHECKS, PRE-DEFINED OPTION SETS, FIELD DEFINITIONS, ERROR MESSAGES .

Additionally, the NAME OF DATA SYSTEM is capable of generating reports that summarize data. The table below describes the name of each report, the purpose of each report, responsible parties for running each report, and the expected frequency that each report should be run to help identify data issues/problems:

NAME OF REPORT	PURPOSE OF REPORT	ROLE/GROUP RESPONSIBLE FOR RUNNING REPORT *	HOW OFTEN TO RUN REPORT?
EXAMPLE: *Children with no COS entrance rating*	*To determine if there are children in the data system without an entrance COS rating*	*Part C Data Manager*	*Monthly*

**This can be broad ("STATE AGENCY" or "LOCAL PROGRAMS"), or specific (ROLE or GROUP) or both*

End users can provide input on potential changes or additions to automatic EDIT CHECKS, PRE-DEFINED OPTION SETS, FIELD DEFINITIONS, ERROR MESSAGES or data quality reports through REVIEWS, TESTING, FEEDBACK as determined by AGENCY, PROGRAM, ROLE, ETC..

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Data Security and Access

Overview

Part C and Part B 619 programs collect and maintain large amounts of data, including **personally identifiable information (PII)**, on the children and families they serve. To protect and safeguard Part C and Part B 619 **PII** and other important data, programs should develop and implement policies that address how these data are secured (i.e., making sure that data are protected from unauthorized access) and who may access the data. Securing data and limiting access guard data from loss, corruption, breach, and other compromises such as unintended access.

Policies supporting *data security* outline the purpose and requirements of data protection and the roles and responsibilities needed to maintain secure Part C and Part B 619 data. Data security encompasses the technical processes and actions associated with preserving data existence and **integrity**.

Policies supporting *data access* establish processes for managing access to Part C and Part B 619 data. These are the technical approaches to limiting data access, including differentiated access, to all those with a legitimate need for the data—in some cases other data systems—based on agency, role, established agreements, and the like. Policies should describe procedures in detail and, where applicable, refer to federal and state laws and regulations.

Whether Part C and Part B 619 programs are considering developing new data security and access policies or are revisiting existing policies, it is important to review **relevant federal and state agency regulations** related to data security and access.

Definition

Data Security: Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and type.

Access: Access, in the context of security, is the privilege or assigned permission to use computer data or resources in some manner. Access may restrict the use and distribution of **Information***, settings, and the general use of a data system.

Source: **Techopedia**

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any **data governance** *already within an agency* is of particular importance. Before developing a data security and access policy, Part C and Part B 619 programs should review any policies regarding data security and access developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose.

Where no policy on data security and access exist or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new data security and access policies.

The *DaSy Data System Framework* defines both data security and access and emphasizes the importance of both in the **Data Governance** and **Management** section, Quality Indicator **DG6**, **DG7**, and **DG8**.

Considerations

Use the questions below to discuss, consider, and develop a comprehensive data security and access policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created.

1. Data Security and Access Policy: General Provisions

a. What federal laws/regulations (e.g., IDEA/**FERPA**) related to data security and access apply to the Part C or Part B 619 program?
b. Are there additional state agency policies related to security and data access that apply to your Part C or Part B 619 program? If yes, what are they?
c. What specific Part C or Part B 619 data security and access policies or procedures, if any, exist and apply?
d. What established data sharing agreements, if any, pertain to support data access and data security?
e. Which participating agencies, if any, will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?
f. Which role, within what agency/program should be contacted with questions about this policy?
g. Which role, within what agency/program is responsible for ensuring adherence to this policy?
h. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
i. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
j. What consequences, if any, will apply when this policy is not followed?
k. How often will this policy be reviewed for necessary revisions?
l. How will the public be informed about this policy? Where will it be posted on the state's website?

2. Data Security and Access Policy: Security

a. What technical security measures (e.g., firewalls, secure laptops, password, **management**, etc.) will be used to secure the Part C or Part B 619 data?
b. What nontechnical security measures will be used to increase data security? For example:
    i. Data access and sharing restrictions
    ii. Regular staff trainings
    iii. Ensuring correct access and administrative rights are granted for staff and authorized data **users**
c. Under what circumstances should a security assessment or audit be conducted and security risks be evaluated? Which role, within what agency/program conducts the security assessment?
d. Does the organization maintain a current inventory of all computer equipment, **software**, and data files associated with Part C or Part B 619 data? Where is this located?

e. Have data records been classified in accordance with the level of risk for **disclosure** of **PII**?

3. Data Security and Access Policy: Access

a. How are **users** approved for and assigned access? How and when is this access terminated?
b. What methods are used to restrict authorized **users'** access to the minimum amount of data needed to complete their job duties?
c. Which role, within what agency/program is responsible for maintaining system access controls in coordination with the **IT team**?
d. What privacy, confidentiality, and data protection trainings exist for individuals with access to data?
e. What policies are in place to guide decisions about data exchanges and reporting, including sharing data (either in the form of individual records containing **PII** or as de-identified aggregate reports) with educational institutions, researchers, policymakers, parents, third-party contractors, and the like?
f. What sharing agreements or other appropriate procedures are in place to ensure that protected data are guarded from unauthorized **disclosure**, once the **users** are provided access?
g. Where are the records maintained that document the access and denial requests for data? Which role, within what agency/program oversees the maintenance of these records?

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

Data Security and Access Policy Template

Use, and modify as needed, the template linked below for developing a data security and access policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Data Security and Access Policy

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Security and Access Policy Template

This page intentionally left blank

Data Security and Access Policy

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this data security and access policy is to establish authority and a process for protecting and safeguarding PART C OR PART B 619 PII and other important data within the data system supporting the PART C/PART B 619 PROGRAM NAME.

DEFINITIONS

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases, and websites. Data security also protects data from corruption occurring during the writing, reading, transmission, or processing of data resulting in unintended changes to the original data. Data security is the main priority for organizations of every size and type.

Access, in the context of security, is the privilege or assigned permission to use computer data or resources in some manner. Access may restrict the use and distribution of information, settings, and the general use of a data system

AUTHORITY

NAME OF STATE is federally required to collect and report PART C OR PART B 619 data and collects such data through data systems noted in the table below. The following federal (AND POTENTIALLY NAME OF STATE) requirements (statutes/regulations/rules/policies) apply to data security and access:

Federal regulations are IDEA regulations for Part C at 34 CFR 303.414(a) and (b) and Part B at 34 CFR 300.622(a)

The NAME OF STATE statute, regulations, and current policies that address data security and access are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and carry out those processes associated with data security and access to PART C/PART B 619 PROGRAM data systems. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this data security and access policy.

PART C/PART B 619 PROGRAM NAME Data System(s)

7. *(insert name of data system)*
8. *(insert name of data system)*
9. *(insert name of data system)*
10. *(insert name of data system)*
11. *(insert name of data system)*
12. *(insert name of data system)*

AGENCY, PROGRAM, ROLE, ETC. is responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM data systems. Further, AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to these processes, identifying the timing and method for such monitoring to occur.

This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to this policy through REVIEW OF DATA QUALITY REPORTS, REVIEW OF DATA QUALITY ISSUES REPORTED, ETC. Any questions data quality will be addressed by AGENCY, PROGRAM, ROLE, ETC. AGENCY, PROGRAM, ROLE, ETC. who will also secure or provide training and technical assistance on data quality when requested. This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

The public will be informed about this policy through AGENCY WEBSITE, MANUAL, ETC..

APPLICABILITY

This policy applies to those who collect, maintain, use, manage, operate, or are otherwise active in the control of data regardless of format. This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. These entities and the mechanism (regulation/contract/interagency agreement) that make this policy applicable to each program/agency are listed in the table below.

Entities Covered by Policy	Mechanism
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*

Entities Covered by Policy	Mechanism
(insert name of program/agency)	*(insert regulation/contract/interagency agreement)*

SECURITY OF DATA

The table below describes the technical security measures used by the PART C/PART B 619 PROGRAM DATA SYSTEM to ensure protection and security of PART C/PART B 619 PROGRAM data including the type of security measure, the entity responsible for implementing the security measure, how often the measure is revised or updated, and how often the measure is tested.

Security Measure	Responsible Entity for This Security Measure	How Often Reviewed/Updated?	How Often Tested (if applicable)
EXAMPLE: Anti-virus Software	*Information Technology*	• *Updates pushed out weekly* • *Yearly License*	*Monthly*

In addition to the above measures, several nontechnical security measures are used to increase data security, including:

- Equipment inventories – a list of all computer equipment and devices which access or store PII can be found INSERT LOCATION. This inventory is updated TIMEFRAME by AGENCY, PROGRAM, ROLE, ETC.. Any loss or theft of equipment should be reported immediately to AGENCY, PROGRAM, ROLE, ETC. and data breach response actions shall be instituted, if applicable (see Data Breach Response policy).
- Security assessments – assessments and audits need to be conducted by AGENCY, PROGRAM, ROLE, ETC. on a TIMEFRAME in order to identify any potential security risks to the system.
- Trainings on confidentiality, data access, and data sharing restrictions for both new staff and refresher trainings conducted by AGENCY, PROGRAM, ROLE, ETC..
- OTHER MEASURES (LEVEL OF RISK CLASSIFICATION FOR DATA, ETC.)

DATA ACCESS

Permissions and restrictions for access to PART C/PART B 619 PROGRAM DATA are managed by AGENCY, PROGRAM, ROLE, ETC.. AGENCY, PROGRAM, ROLE, ETC. will be responsible for:

- Responding to requests for data system access (see below)
- Responding to access requests within TIMEFRAME from receiving the EMAIL, REQUEST FORM, ETC..

- Ensuring that staff have access to the minimum amount of data needed to complete his/her job duties through user roles or other mechanism
- Identifying various levels of access to restrict authorized users' access

Identified sharing agreements or other appropriate procedures for all PART C/PART B 619 PROGRAM DATA are in place to ensure that protected data is are guarded from unauthorized disclosure.

- LIST OTHER RESPONSIBILITIES
- Staff Training for privacy, confidentiality, and data protection issues are the responsibility of AGENCY, PROGRAM, ROLE, ETC. and are offered INSERT TIMEFRAME.

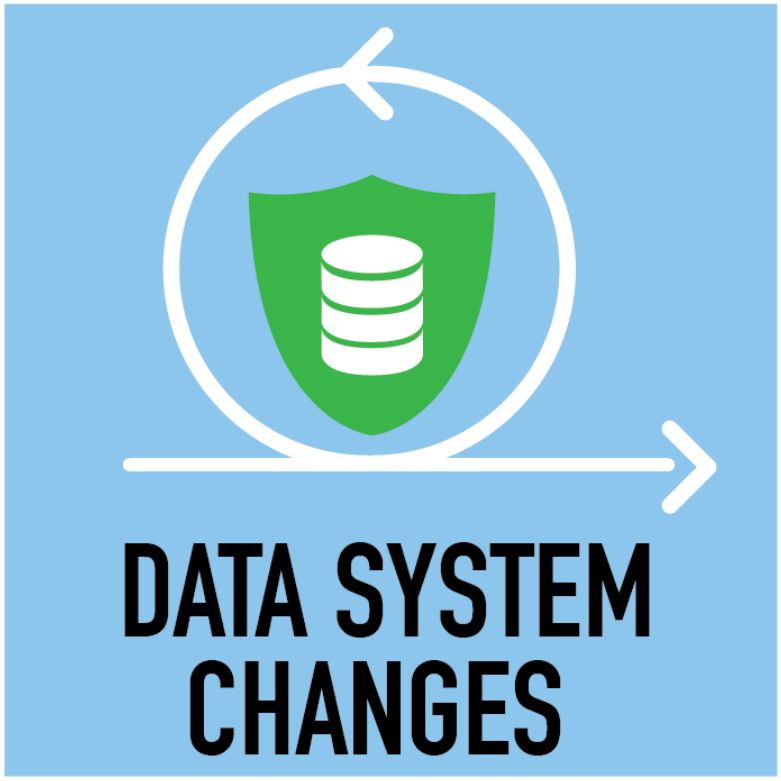
Steps To Request Data System Access

The following steps are required to request access to the PART C/PART B 619 PROGRAM DATA SYSTEM:

1. Access requests are made to AGENCY, PROGRAM, ROLE, ETC. via EMAIL, REQUEST FORM, ETC. and are to contain the following information, NAME, TITLE/ROLE, EMAIL, PHONE NUMBER, SUPERVISOR NAME, SUPERVISOR CONTACT INFORMATION, SUPERVISOR APPROVAL, REASON FOR ACCESS, ETC..
2. AGENCY, PROGRAM, ROLE, ETC. confirms supervisor approval via EMAIL, REQUEST FORM, ETC..
3. AGENCY, PROGRAM, ROLE, ETC. determines the level of access/permission needed based on staff role and data access needs as outlined in EMAIL, REQUEST FORM, ETC..
4. Notification of approval or denial will be sent by AGENCY, PROGRAM, ROLE, ETC. via EMAIL, REQUEST FORM, ETC.. Denials of access should be accompanied by the reason(s) for denial. Access requests and resulting permissions/denials are located LOCATION WHERE ACCESS REQUESTS ARE STORED and are maintained by AGENCY, PROGRAM, ROLE, ETC..

NOTE: Requests for access to PART C/PART B 619 PROGRAM DATA by others not covered by this data security and access policy are addressed in the PART C/PART B 619 PROGRAM data request policy.

DaSy The Center for IDEA Early Childhood Data Systems



This page intentionally left blank

Data System Changes

Overview

State Part C and Part B 619 programs will encounter the need for changes in their data system(s). Many changes to an existing data system can affect work conducted at the state, local/district, and/or provider levels. Even the addition of a single response option to just one established data element could have significant and far- reaching implications to business rules, data collection screens, supported forms, post-collection analysis, reports, data dictionary, trainings, and the like.

Therefore, while Part C and Part B 619 staff may not be directly involved in the technical changes made to data systems that directly affect their work, the state should establish a process for Part C and Part B 619 program staff to be actively involved in partnering with information technology (IT) staff when considering data system changes that will affect their data and work. This section of the toolkit aids in the development of comprehensive data governance policies to support Part C or Part B 619 consideration of potential data system changes and when and how to make such changes.

Recommendations or requirements to make changes to a Part C or Part B 619 data system(s) may emanate from many different sources. New or modified federal and/or state data collection or reporting requirements, changes to internal program data needs (e.g., monitoring, new reports),recommendations from stakeholders in the field, agency or cross-agency data integration efforts, technical architecture changes, updates to security, new requirements from information technology—many sources can trigger a request to change the content, functionality, technical aspects, or reports associated with an existing data system. Regardless of where the recommendations for change come from, data governance policies should reflect the involvement of Part C or Part B 619 program representatives in considering and deciding data system changes affecting their programs. In many cases considering a data system change will require Part C or Part B 619 program staff work closely with agency information

Considering a New Data System?

This section of the Data Governance Toolkit focuses exclusively on policies for change(s) to existing data systems, not new data systems. Adding a new Part C or Part B 619 data system or replacing an old system is a decision predicated on factors external to established Part C and Part B 619 data governance.

Records that have a re-identification code and have enough personally identifiable information (PII) removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. The re-identification code may allow the recipient to match information received from the same source.

A decision that a new system is decidedly better than enhancing an existing system is based on many considerations. Such a conclusion is supported by: availability of funds (immediate and sustaining), political climate supportive of both state agency and local-level changes required with a new data system, technology alignment, internal and external agency data integration efforts, etcetera.

technology (IT) staff so all will understand the overall impact of the requested change.

It is important to consider the scope and identify the potential impact(s) of any proposed system change. A proposed system change can be small and quick to implement such as addressing a minor bug or spelling error. It can be scheduled and routine, such as an annual update to a list of active agencies. Or it can be complex and long term, such as a multiphase enhancement over an extended period to collect more data and develop more complex reports. While a *request to change* should detail what is desired to be changed and why, *a decision to change* focuses on the impact the change will have. It is important that Part C and Part B 619 staff with content knowledge, as well as IT staff with data system knowledge, share perspectives on the change impact. Logically, not all change requests necessitate the same level of consideration. For example, correcting a misspelled word might require no additional input and has little (or no) system impact. In contrast, significant consideration would be required to decide on proposing a data system change to add a new data element such as medical diagnosis or updating service delivery codes.

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any data governance *already within an agency* is of particular importance. Before developing a data system change policy, Part C and Part B 619 programs should review policies regarding data system changes developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language.

Where no policy on data system change exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new data system change policies for this purpose.

The *DaSy Data System Framework* describes all major aspects of developing a new and enhancing an existing data system in the System Design and Development section, Quality Indicators SD1 through SD9, in the **Data Governance** section, Quality Indicator DG3, and in the Sustainability section, Quality Indicator SU1.

Considerations

Use the questions below to discuss, consider, and develop a data system change policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created.

1. Data System Change: General Provisions

a. Are there state agency policies related to data system changes that apply to the Part C or Part B 619 program? If yes, what are they?
b. What specific Part C or Part B 619 data system change policies or procedures, if any, exist and apply?
c. Which role, within what agency/program should be contacted with questions about this policy?
d. Which role, within what agency/program is responsible for ensuring adherence to this policy?

e. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
f. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
g. What consequences, if any, will apply when this policy is not followed?
h. How often will this policy be reviewed for necessary revisions?
i. How will the public be informed about this policy? Where will it be posted on the state's website?

2. Data System Change: Initiation of Request

a. What is the standardized request process for suggesting changes (e.g., a paper/online form to complete, an individual to contact)?
b. Which role, within what agency/program, should receive data system change requests, and how are these requests communicated to the Part C or Part B 619 program?
c. What is the process for acknowledging receipt and responding to a data system change requester?
d. How are data system users informed of the process for suggesting data system changes?

3. Data System Change: Request Required Information[1]

a. What information is required to request a change? Shall a requestor (internal or external to an agency) specify exactly what they would like changed with respect to Part C and Part B 619 data system(s)? For example, requested change details might be associated with:
    i. New (or removed) item/field
    ii. Item response options
    iii. Descriptive text (e.g., item, response option, element definition, application instructions, documentation)
    iv. Business logic (validations)
    v. User interface
    vi. Dashboards
    vii. User permissions
    viii. Data exports
    ix. Embedded reports, system reports, tools
    x. System speed/capacity/scalability
b. Shall a requestor (internal or external) provide a rationale for the change request? That is, shall the requestor justify why the change is being requested?
c. What additional information on the impact of the requested change on affected items will be gathered? (Much of this information will be provided by IT staff with Part C and Part B 619 staff providing content knowledge.) For example, what will be the change impact on:
    i. Business logic (validations)
    ii. User interface
    iii. Dashboards
    iv. User permissions
    v. Data exports
    vi. Embedded reports, system reports, tools

vii. Data analysis
viii. Continuity of pre-change data with post-change data
ix. Technology (hardware, software, hosting, security, performance, system speed/capacity/scalability)
x. Agency staffing needs to design, develop, test, deploy, support
xi. Internal agency functionality and processes
xii. Budgets (short term, mid-term, long term, maintenance)
xiii. Local agency: systems, processes, staffing, etc.
xiv. Training (internal and external) to inform stakeholders of the change and ramifications of the change
xv. Timeline to support and implement the change (communicating with stakeholders about upcoming change, scheduling change, implementing change)

d. In what circumstances will Part C or Part B 619 collect information from stakeholders to inform the decision(s)? What stakeholders, (e.g. local IT staff, content staff)? How will stakeholder information be collected and processed (e.g., surveys, focus groups, rank order priority changes)?
e. In what circumstances will a cost/benefit analysis be needed to address issues related to costs (local and state agency impact, vendor, technology, etc.)? Which role, within what agency/program, will decide if a cost/benefit analysis is required?

4. Data System Change: Evaluation of Request

a. Which role, within what agency/program, is familiar with the data system targeted for change and therefore shall review the request for completeness, benefits, and redundancy?
b. Which role, within what agency/program, is familiar with relevant technical aspects of the request and therefore shall review the request and determine the technical feasibility?
c. Which role, within what agency/program, shall review the impact of the request on costs, expected time to implement, training, etc.?
d. Which role(s), within what agency/program, will review the request and all associated information and approve or deny the request? What role do Part C and Part B 619 programs play in this process?
e. What is the process for communicating a content decision or recommendation to all interested parties (e.g. requestor, administration, IT)?
f. Within what time frame shall the decision regarding the change request be communicated to the requestor?
g. What role do Part C and Part B 619 programs play in processes supporting the evaluation of the change request?

5. Data System Change: Planning for Change

a. What is the process for implementing an approved data system change? For example, is a project manager assigned to large enhancement efforts (that may contain many changes)? Are smaller changes overseen by content or technical staff? Will there be a plan and schedule to support proposed changes? If so, how will plans and schedules accommodate stakeholder input and support local agency lead time to accommodate changes?
b. How will stakeholders be kept apprised of upcoming planned system changes (e.g., newsletter, webinar, newsletter, trainings)?

c. Which role, within what agency/program, will make changes, and how, to program and technical documentation based on the data system change (e.g., collection forms, data dictionaries, report titles, support manuals, system service documentation)?
d. What role do Part C and Part B 619 programs play in supporting the plan to change?

6. **Data System Change: Implementation, Management, Confirmation, and Communication**
   a. Which role, within what agency/program, will oversee the design, development, testing, and deployment of the data system change?
   b. Which role, within what agency/program, will test and review that implemented system changes work as designed? How will tests be conducted? Will it include local stakeholders?
   c. Which role, within what agency/program, will distribute change details to all relevant parties (e.g., programs, participating agencies, vendors)? How?
   d. Which role, within what agency/program, will determine that no further actions are needed relevant to the change (close out the request)?
   e. What role will determine if, and if so when, any follow up review shall be scheduled?
   f. Which role, within what agency/program, will confirm (if warranted) that the data system change is supported (e.g., maintenance budget)?
   g. What role do Part C and Part B 619 programs play in implementation, management, confirmation, and communication processes?

Footnotes

1. Many possible data system change areas are listed. Though content may be helpful for classifying and reviewing data change requests, each specific area does not need to be included within a Part C or Part B 619 data system change policy.

Data System Change Policy Template

Use, and modify as needed, the template linked below for developing a data system change policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and stakeholders when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Data System Change Policy

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Systems Change Policy Template

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Systems Change Policy Template

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this data systems change policy is to establish authority and processes for considering requests to make changes to data systems and managing any approved changes to those data systems that support the PART C/PART B 619 PROGRAM NAME.

DEFINITIONS

A *data system change* is any change to an existing data system. A data system change includes any change including but not limited to: data items, response options, business rules/logic, system analysis of data, system generated reports, user interface, support documentation, technology, etc.

AUTHORITY

NAME OF STATE is federally required to collect and report Part C/Part B 619 data and collects such data through the data systems noted in the table below. Ramifications of any proposed data system change must be thoughtfully considered by weighing the local and state effort, impact and cost of the proposed change against the state and local benefits of the proposed change.

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and carry out processes associated with considering and overseeing any approved changes to PART C/PART B 619 PROGRAM data systems. It is understood that agency IT staff will be instrumental partners in considering and overseeing any approved changes. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this data system change policy.

PART C/PART B 619 PROGRAM NAME Data Systems

13. ***(insert name of data system)***
14. ***(insert name of data system)***
15. ***(insert name of data system)***
16. ***(insert name of data system)***
17. ***(insert name of data system)***
18. ***(insert name of data system)***

AGENCY, PROGRAM, ROLE, ETC. is responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM data systems. AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to this policy. Any questions regarding the data system change policy will be addressed by AGENCY, PROGRAM, ROLE, ETC.. AGENCY, PROGRAM, ROLE, ETC. who will also secure or provide training and technical assistance on data system changes when requested. This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED by AGENCY, PROGRAM, ROLE, ETC. and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy.

The public will be informed about this policy through AGENCY WEBSITE, MANUAL, ETC..

INITIATION OF REQUEST

Requests to change an above listed Part C/Part B 619 data system shall be submitted on a completed *Data System Change Request Form*. (See sample *Data System Change Request Form*.) The *Data System Change Request Form* is to be publicly available at INSERT URL. In addition, each data system used by PART C/PART B 619 PROGRAM NAME shall inform users of the process for requesting a data system change. (Users may be informed about requesting data system changes through: SOURCE OF COMMUNICATION ABOUT CHANGES (E.g., DATA SYSTEM MANUAL, APPLICATION HOME PAGE, SUPPORT DOCUMENTATION, MEMOS, CORRESPONDENCE TO DATA SYSTEM USERS, ETC.).

Completed *Data System Change Request Forms* must be submitted to NAME OF OFFICE/ROLE <Alternatively: to any member of the AGENCY, PROGRAM, ROLE, ETC>. The recipient of the completed form shall acknowledge receipt by EMAIL OR OTHER WRITTEN MEDIUM within TIME PERIOD. Written acknowledgement shall include when a decision about the requested change can made and expected date of communication about the decision back to the requester.

REQUEST REQUIRED INFORMATION

A *Data System Change Request Form* shall be completed to initiate a change request. Sample form content areas include:

1. Requester contact information *(Required of requester)*
2. Name of data system *(Required of requester)*
3. Rationale for the requested change including description of the foreseen value of the proposed change and impact of change on local and state work. *(Required of requester)*
4. Details of the specific change desired associated with one or more areas below. All requested additions, deletions, modifications must be described. (R*equired of requester*)
    1. New (or removed) item/field
    2. Item response options
    3. Descriptive text change (e.g., item, response option, element definition, application instructions, documentation)
    4. Business logic (validations)
    5. User interface
    6. Dashboards
    7. User permissions
    8. System reports
    9. Data exports
    10. Embedded report tools and/or tools
    11. System speed/capacity/scalability
    12. Other
5. Form shall include addressee for submitting completed *Data System Change Request Forms*. (Incomplete requests shall be returned to requester for completion.)

GROUP, COMMITTEE, PART C/PART B 619 PROGRAM STAFF WITH SYSTEM AND/OR CONTENT KNOWLEDGE, AND/OR IT STAFF shall review a data system change request for new information to determine if the requested elements are already being collected.

Requested changes that have no impact; (e.g., spelling, grammar, minor user interface updates) can be made without additional information at the direction of the AGENCY, PROGRAM, ROLE, by PART C/PART B 619 PROGRAM STAFF WITH SYSTEM AND/OR CONTENT KNOWLEDGE.

Changes that will have impact require information from sources outside the requester. One or more members of SELECTED MEMBER(S) OF THE AGENCY, PROGRAM, ROLE, ETC. shall review the request and provide an informed estimate of the impact of conducting the requested data system change. The areas below are *examples of areas that should be considered*. All impact shall be written for further review and evaluation by the AGENCY, PROGRAM, ROLE.

1. Business logic (validations)
2. User interface
3. Dashboards
4. User permissions
5. Data exports
6. Embedded reports, system reports, tools
7. Data analysis
8. Continuity of pre-change data with post-change data
9. Technology (hardware, software, hosting, security, performance, system speed/capacity/scalability)
10. Agency staffing needs to design, develop, test, deploy, support
11. Internal agency functionality and processes
12. Budgets (short term, mid-term, long term, maintenance)
13. Local agency: systems, processes, staffing, etc.
14. Training (internal and external) to inform stakeholders of the change and ramifications of the change
15. Timeline to support and implement the change (communicating with stakeholders about upcoming change, scheduling change, implementing change)

As needed, upon the direction of the AGENCY, PROGRAM, ROLE, ETC., additional perceived impact information may be collected from local representatives (stakeholders) including both local content and local IT staff. Local perceived impact shall be written for further review and evaluation.

As needed, upon the direction of the AGENCY, PROGRAM, ROLE, ETC., a cost-benefit analysis may be conducted regarding the change request. Local, state agency, vendor, technology, and all other costs associated with the proposed change shall be investigated as part of a cost-benefit analysis. Cost-benefit analysis information shall be written for further review and evaluation.

EVALUATION OF REQUEST

The team evaluating the request for a data system change shall be made up primarily of those in the agency or program responsible for funding, overseeing, and supporting and processing the data (IT) based on the change. AGENCY, PROGRAM, ROLE, ETC. shall review the request and all additional information (e.g., impact, stakeholder input, costs) for completeness, benefits, and redundancy (with available data). The evaluation team shall decide to accept the request, deny the request, or table the request (e.g., pending more information) for future consideration.

The decision of the evaluation team shall be communicated back to the requester in a reasonable time depending on the significance of the request (e.g., 4-12 weeks). The response shall be in writing and include the decision made. If the data system change request was accepted the response back shall include the expected time for implementing the change. For all other decisions, a brief explanation shall be provided as to why the request was denied, tabled, or delayed.

PLANNING FOR CHANGE

AGENCY, PROGRAM, ROLE, ETC. shall establish a process for implementing an approved data system change commensurate with the magnitude of the approved change. PART C/PART B 619 PROGRAM STAFF WITH SYSTEM AND/OR CONTENT KNOWLEDGE shall have an established role in that plan to determine successful changes affecting Part C/Part B 619 data. A plan and schedule to support the approved changes will include input from PART C/PART B 619 PROGRAM STAFF WITH SYSTEM AND/OR CONTENT KNOWLEDGE. On large approved changes, Part C/Part B 619 stakeholder input may be sought and included in the plan. Plans that support ll substantial changes must establish and accommodate adequate local agency lead time to accommodate local changes to databases, where applicable. On substantially large approved changes, plans shall detail frequency and process for informing all interested stakeholders of upcoming planned system changes (e.g., newsletter, webinar, newsletter, trainings).

IMPLEMENTATION, MANAGEMENT, CONFIRMATION AND COMMUNICATION

AGENCY, PROGRAM, ROLE, ETC. shall devise a data system change plan commensurate with the approved data system change. Simple rudimentary changes shall be assigned to TECHNICAL STAFF, VENDOR, ETC. and designed, developed, tested and deployed as part of standard work under existing administration oversight or contractual obligations. Substantial data system changes may require a detailed plan, project manager, schedule, budget, etc. In some cases, additional or ongoing stakeholder input from local agencies may be required and sought by the project manager. At a minimum, AGENCY, PROGRAM, ROLE, ETC. or designee, shall inform stakeholders (e.g., newsletter, webinar, newsletter, trainings, etc.) of upcoming planned system changes. Where any state data system change requires local agencies to change their data systems, local agencies shall be provided ample time to make such changes. Such timelines will be determined and communicated to local agencies by AGENCY, PROGRAM, ROLE, ETC..

Once the data system change has occurred, supporting documentation (e.g., collection forms, data dictionaries, report titles, support manuals, system service documentation) shall be reviewed and updated as required to reflect the approved data system change. AGENCY, PROGRAM, ROLE, ETC. shall confirm that documentation changes have been made.


PUBLIC
REPORTING

This page intentionally left blank

Public Reporting

Overview

An important part of each state's Part C and Part B 619 **accountability** system is the regular reporting of data related to the implementation of IDEA. Part C and Part B 619 state staff or representatives analyze and publicly report data for a variety of reasons. Public reporting is the publishing of information that has no restricted access (i.e., information or data that contains personally identifying information cannot be released in public reports). Public reports are generated to a) meet federal reporting requirements; b) meet state reporting requirements, c) address local and state program **accountability** and improvement needs; and d) provide information to the general public. State and local reports are made available through public means, including posting on lead agency Websites, distribution to the media, and distribution to local programs. Part C and Part B 619 public reporting policies should be consistent with applicable data system(s) **purpose and vision** statements.

Reports should be tailored to specific stakeholder groups (e.g. local programs, policy-makers, parents, service providers) and include their input in decisions about what reports should be developed. For example, the legislature might request annual reports on the monthly referrals as compared to enrollment into the program. The state advisory council might request regular reporting on frequency of specific services based on local programs and age of children enrolled. The state agency overseeing the program may want to provide annual media releases about child outcomes. Data reports should be prepared to promote understanding of the data and inform state and local decision-making.

Under IDEA Section 618, Part C and Part B must annually report data to the U.S. Secretary of Education and the public at the times specified by the Secretary *(34 CFR 303.720 and 34 CFR 300.640. (34 CFR 303.722 and 34 CFR 300.642).* Additionally, states are required to report the state's performance on its annual performance plan for Part B and for Part C *[34 CFR 303.702(b)(2)* and *34 CFR 300.602(b)(2)]*. States must also publicly report on the annual performance of local education agencies (LEAs) and early intervention service (EIS) programs on state set targets for specific priority indicators. These reports on LEA's and EIS programs must be published no later than 120 days after the state submits its statewide Annual Performance Report (APR) *[(34 CFR 303.702(b)(1)* and *34 CFR 300.602(b)(1)]*.

While IDEA requires states to publicly report state and local performance data, IDEA does not require local agencies to publicly report data. Regardless, many local agencies or programs do report IDEA data regularly. State **data governance** policies on IDEA public reporting would apply to reports that are developed and disseminated at the local level.

Both IDEA and ESSA[1] are clear that data publicly reported by each state must not result in **disclosure** of data identifiable to an individual child. States must not report to the public any data or information on performance that would result in the **disclosure** of personally identifiable information about individual children. *(34 CFR 303.702(b)(3), 34 CFR 722(a), 34 CFR 300.602(b)(3)),* and *34 CFR 300.642(a).* Therefore data containing **personally identifiable information (PII)** in public reports must be reported and displayed in ways that ensure no **PII** is

identifiable directly or through the combination of attributes (e.g., program, agency, disability category, race/ethnicity).

The U.S. Department of Education does not mandate a particular method of data protection techniques. Nor does it establish a threshold for what constitutes sufficient **disclosure avoidance** (so that no personally identifiable information is reported). These decisions are left up to the individual agencies and programs at the state and local level to determine what works best within their specific contexts.

Establishing and adhering to clear public reporting policies and procedures will ensure the protection and the privacy of information about all children and families served under IDEA. Policies should also address protection of the privacy of information about staff working in Part C and Part B 619 programs. The IDEA regulations listed above specify that data must be publicly reported by each State in a manner that does not result in **disclosure** of data identifiable to individual children. A public reporting policy should describe processes used to ensure that data meet privacy and reporting requirements prior to becoming publicly available. The policy should describe methods for aggregating and de-identification of data to maintain child and family privacy as well as a process for the review of public reports to ensure compliance with these policy requirements.

Definition

De-Identification of Data: The process of removing or obscuring any personally identifiable information from children's education and early intervention records in a way that minimizes the risk of unintended **disclosure** of the identity of individuals and information about them.

De-Identified Data:

Records that have a re-identification code and have enough **personally identifiable information (PII)** removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. The re-identification code may allow the recipient to match information received from the same source.

Source: **DaSy/Privacy Technical Assistance Center (PTAC)**

Policies should describe data de-identification methods in detail, referring or linking to relevant federal and state requirements, particularly those related to the Individuals with Disabilities Education Act (IDEA) and the **Family Educational Rights and Privacy Act (FERPA)2**. These federal statutes and their implementing regulations generally require parental consent be obtained prior to the **disclosure** of any **PII**. However, if data are properly de-identified, then that information may be shared publicly. To ensure successful data protection, it is essential that data de-identification methods are appropriate for the intended purpose and that their **application** follows best practices and established **data governance** policy[3].

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any **data governance** *already within an agency* is of particular importance. Before developing any public reporting policy, Part C and Part B 619 programs should review policies regarding public reporting developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose. Part C and B 619 may find their

State Education Agency's (SEA's) ESSA plan for its statewide **accountability** system is helpful for identifying the techniques for de-identification of data, establishing minimum sample size, and addressing extremes in cell size for public reporting.

Where no policy on public reporting exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new public reporting policies.

The DaSy Data System Framework focuses on the importance of public reporting in the **Purpose and Vision**, **Data Governance**, **Data Use** and **Sustainability** sections at PV2, DG3, DU1, DU2, DU3 and SU1.

Considerations

Use the questions below to discuss, consider, and develop a comprehensive public reporting policy. Where appropriate, procedures and operational manuals that detail specific actions supporting implementation of this policy should be created.

1. Public Reporting: General Provisions

a. Which federal laws/regulations (e.g., IDEA/**FERPA**) related to public reporting apply to your Part C or Part B 619 program?
b. Are there additional state agency policies related to public reporting of data that apply to your Part C or Part B 619 program? If yes, what are they?
c. What specific Part C or Part B 619 public reporting policies or procedures, if any, exist and apply?
d. What participating agencies, if any, will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?
e. What program or state longitudinal public reporting efforts are considered under this policy (e.g., **SLDS** and/or **ECIDS**)?
f. Which role, within what agency/program should be contacted with questions about this policy?
g. Which role, within what agency/program is responsible for ensuring adherence to this policy?
h. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
i. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
j. What consequences, if any, will apply when this policy is not followed?
k. Which role, within what agency/program is responsible for procedures to be used to resolve any disputes or disagreements about what data are to be released and how or when?
l. How often will this policy be reviewed for necessary revisions?
m. How will the public be informed about this policy? How is this policy included in your agency's privacy statement? Where will it be posted on the state's website?

2. **Public Reporting: Planning and Management of Data Reports**
   a. What types of data (e.g., child count, race/ethnicity, gender, programmatic, fiscal, monitoring results) will be reported publically and therefore covered under this policy?
   b. What subtypes or crosstabs of data (e.g., numbers of children by primary disability and by race/ethnicity) will be reported publically and therefore covered under this policy?
   c. What process is used to plan for periodic public reporting of data tailored to specific stakeholder groups? How can **stakeholders** use the data being reported?
   d. What process is used to evaluate current public reports and revise plans as necessary?
   e. What procedures are in place to ensure that data, as queried and reported, are accurate and include, when appropriate, checks with the authoritative or original source of the data? (See **Data Quality** section of this toolkit for additional information.)
   f. What supporting documentation and processes (e.g., videos, webinars, data dictionaries, key finding summaries) will be used to assist consumers with understanding the publically reported data?
   g. How long will public reports be made available (for example, how many years' worth of data will remain accessible on a website)?
   h. If/when changes happen from one year to the next that might affect the data, how will the public be informed of those changes and potential impact? (E.g., use of different data collection instruments, changes to summary statistics based on sampling vs population measurements.)
   i. If errors in publically reported data are found, what processes) address how the reported errors are to be corrected?
   j. What are the steps in the public reporting process and associated timeline or schedule? (E.g., full release only after local agency data reviews and finalization, tentative release of restricted data not to be shared further than appropriate, full release of data.)
   k. Where will data be publically available?

3. **Public Reporting: Data De-Identification/Disclosure Avoidance**
   a. What procedures are used to guide decisions about reporting **de-identified data** in aggregate reports with educational institutions, researchers, IDEA and other policy-makers, parents and third party contractors?
   b. What procedures are in place to ensure that **PII** is not inadvertently disclosed in public aggregate reports?
   c. Which office or individuals are responsible for ensuring that only **de-identified data** are made publicly available?

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

Footnotes

1. Like IDEA, the Every Student Succeeds Act (Public Law 114-95) also supports the protection of student data. ESSA requires each state to create a plan for its statewide accountability system. State plans must specify a single value as the minimum number of students to report

statistically sound data for students within a subgroup, while also protecting personally identifiable information of each student. **Section 1111(c)(3)(A)(i-iii)**

2. **Data De-identification: An Overview of Basic Terms** (Updated in October 2012)
3. **Best Practices for Determining Subgroup Size in Accountability Systems While Protecting Personally Identifiable Student Information**

Public Reporting Policy Template

Use, and modify as needed, the template linked below for developing a public reporting policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and stakeholders when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Governance Public Reporting Policy

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Public Reporting Template

This page intentionally left blank

Public Reporting Policy Template

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this public reporting policy is to establish authority and a process for ensuring protection of PART C OR PART B 619 personally identifiable information (PII) and other important data when publicly reporting data/information from the PART C/PART B 619 PROGRAM NAME.

DEFINITIONS

Public reporting is the publishing of information that has no restricted access (i.e., information or data that contains personally identifying information cannot be released in public reports).

AUTHORITY

NAME OF STATE is federally required to collect and report PART C OR PART B 619 data and collects such data through data systems noted in the table below. The following federal AND POTENTIALLY NAME OF STATE requirements (statutes/regulations/rules/policies) apply to public reporting of data/information:

34 CFR Part 303 – Part C Regulations

- 34 CFR 303.702(b)(1)
- 34 CFR 303.702(b)(2)
- 34 CFR 303.702(b)(3)
- 34 CFR 303.720
- 34 CFR 303.722

34 CFR Part 300 – Part B Regulations

- 34 CFR 300.602(b)(1))
- 34 CFR 300.602(b)(2)
- 34 CFR 300.602(b)(3).
- 34 CFR 300.640
- 34 CFR 300.642

The NAME OF STATE statute, regulations, and current policies that address public reporting are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and carry out those processes associated

with public reporting. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this public reporting policy.

PART C/PART B 619 PROGRAM NAME Data System(s)

19. ***(insert program name)***
20. ***(insert program name)***
21. ***(insert program name)***
22. ***(insert program name)***
23. ***(insert program name)***
24. ***(insert program name)***

AGENCY, PROGRAM, ROLE, ETC responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM NAME data systems. AGENCY, PROGRAM, ROLE, ETC is responsible for monitoring adherence to this policy through REVIEW OF REPORTS PRIOR TO PUBLICATION, REVIEW OF EXISTING REPORTS ON PUBLIC WEBPAGES, ETC. Any questions regarding the content of any publicly reported data/information will be addressed by AGENCY, PROGRAM, ROLE, ETC who will also secure or provide training and technical assistance on public reporting when requested. This policy will be reviewed Choose an item. By AGENCY, PROGRAM, ROLE, ETC and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy. AGENCY, PROGRAM, ROLE, ETC and AGENCY DIRECTOR will address any disagreements regarding what data are to be released, as well as how and when these data are to be released.

The public will be informed about this policy through AGENCY, WEBSITE, MANUAL, ETC and is included in the agency's privacy statement (IF APPLICABLE).

APPLICABILITY

This policy applies to those who collect, maintain, use, manage, operate, report or are otherwise active in the control of data regardless of format. This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. These entities and the mechanism (regulation/contract/interagency agreement) that make this policy applicable to each program/agency are listed in the table below.

Entities Covered by Policy	Mechanism
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*

Entities Covered by Policy	Mechanism
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*
(insert agency name)	*(insert regulation/contract/interagency agreement)*

PLANNING AND MANAGEMENT OF DATA REPORTS

The table below summarizes information about the current public reports that are released by PART C/PART B 619 PROGRAM NAME, including the name of the report, the responsible entity for preparing the report, how often the report is produced, the type of data contained in the report, where the report is posted, and for how long the report is posted.

Name of Report/Use	Responsible Entity for This Report	How Often Reported/ Posted?	Type of Data Reported	Where Posted?	Length of Posting
EXAMPLE: Annual Performance Report	***Part C Coordinator/ Part C Data Manager***	***Annually*** ***Due February 1st***	***Child Find Child Outcomes Transition General Supervision Compliance Dispute Resolution***	***Reports section of program website, found at www.example.com***	***5 most recent years of reports only***

Name of Report/Use	Responsible Entity for This Report	How Often Reported/ Posted?	Type of Data Reported	Where Posted?	Length of Posting

Any substantial changes to the reports listed in the table above, or if errors are found in any public reports, these changes and updates must be reported to AGENCY, PROGRAM, ROLE, ETC.

When a new public report is posted, the public will be informed via ANNOUNCEMENT ON HOMEPAGE, EMAIL, ETC. Further information about the data contained in public reports, including supporting documentation, can be found on the program homepage, located at NAME OF WEBPAGE SECTION OR PART.

In addition to the public reports above, the PART C/PART B 619 PROGRAM NAME produces ad hoc and as needed reports throughout the year. These ad hoc reports are produced by AGENCY, PROGRAM, ROLE, ETC, and reviewed by AGENCY, PROGRAM, ROLE, ETC to ensure compliance with federal and state public reporting requirements.

DATA DE-IDENTIFICATION/DISCLOSURE AVOIDENCE

Prior to release, all public reports must be reviewed by AGENCY, PROGRAM, ROLE, ETC to ensure that only de-identified data are reported and that the report user cannot identify individual children or families. The PART C/PART B 619 PROGRAM requires minimum cell or n-size for data with INSERT PARAMETERS FOR MINIMUM CELL OR N-SIZE. Any violation of this public reporting policy, including accidental release of PII or violating minimum cell or n-size rules must be reported to AGENCY, PROGRAM, ROLE, ETC and as specified in the agency's Data Breach Response procedures (if applicable).

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Electronic Communications

Overview

Given the continuing increase in the use of electronic communications (e.g., texting, email, instant messaging, video chatting, Instagram, Facebook, Twitter), it is not surprising that families and Part C and Part B 619 providers use these technologies to communicate and share program information. However, use of these forms of communication introduces the risk of unintended **disclosure** of **personally identifiable information (PII)**. State **data governance** policies can minimize this risk by addressing the use of electronic communications. State policies can require implementation statewide, require local programs/agencies to develop and implement consistent policies and procedures, or require a combination of these two options.

The Privacy and Technical Assistance Center (PTAC) of the U.S. Department of Education lists use of mobile devices as one of the top threats to data protection.

> Use of mobile devices, such as laptops or handheld devices, including smartphones, is exploding. However, the ability to secure them is lagging behind. The situation is complicated by the fact that these devices are often used to conduct work outside the organization's regular network security boundaries. Data breaches can occur in a number of ways: devices can be lost, stolen, or their security can be compromised by malicious code and/or downloaded applications invading the operating system and other applications. — **Privacy Technical Assistance Center, Data Security: Top Threats to Data Protection (2011)**

Some federal policy clarification already exists about the use of electronic mail (email). The Individuals with Disabilities Education Act (IDEA) Part B regulations at 34 CFR 300.505 permit the use of email to provide procedural safeguard notices to parents under certain circumstances as long as the parent and the agency agree. The use of email is further clarified in the policy guidance from the Office of Special Education Programs (OSEP) related to Part B of IDEA, which indicates that parents may elect to receive written notices, procedural safeguards notices, and due process complaint notices by email if a school district makes that option available. This guidance is located in the **"Frequently Asked Questions on Confidentiality Requirements"** issued in October 2016.

Additionally, according to this OSEP guidance,

> email communications are permitted for providing parents copies of their child's IEP and progress reports if a public agency has implemented the following security procedures when delivering such information via electronic mail: the district obtains prior signed permission from the parents; the parents provide the address of their confidential email account; a secure password is used to access documents; and the parents may request hard copies at any time and/or refuse the electronic mail option.

These security measures should be addressed through the development and implementation of **data governance** policies. PTAC developed a helpful **video** about sharing **PII** via email.

The OSEP guidance above specifically relates to Part B of IDEA. A reasonable best practice would be to apply these principles to Part C because the relevant procedural safeguards and confidentiality requirements are consistent across Part B and Part C of IDEA.

PTAC recommends additional security processes to protect all electronic **PII** data. They recommend **PII** data be encrypted on all mobile devices storing sensitive information. Further, PTAC states the best protection is to implement a strict mobile device usage policy and monitor networks for malicious activity. Encryption, usage policy and network monitoring should be included in **data governance** policies on electronic communications. In addition, it is important to remember that the use of personal devices increases risk as policies and monitoring of personally-owned devices may not apply or will be difficult to enforce. Note that the most substantial risk to mobile devices occurs with downloaded applications. Many of those applications have terms that you must agree to that "allow the **application** to read, share, or modify any contents of your mobile device without your knowledge."

A key consideration in developing policies related to electronic communication is to be sure parent identity is authenticated. The **Family Educational Rights and Privacy Act (FERPA)** regulations require Part C and Part B 619 programs to use reasonable methods to identify and authenticate the identity of parents, children, school officials, providers, and other parties before disclosing or permitting access to **PII** (34 CFR 99.31(c)). These requirements must be addressed in **data governance** policies. As technology and data security standards change, policies and procedures should be reviewed and updated to ensure reasonable governance for and methods to authenticate the identity of all parties before disclosing **PII**.

Definition
"Authentication of identity" means ensuring that the recipient of education records or the party who receives or transmits students' records is in fact the authorized or intended recipient or sender. Authentication is the process by which an **educational agency** or institution establishes the appropriate level of identity authentication assurance or confidence in the identity of the person or entity requesting access to the records. This assurance is established through the use of a variety of vetting methodologies, which employ so-called "authentication factors," individually or in concert, to raise the level of confidence that the party being granted access is the person or entity it claims to be.

Data Governance policies must also support procedures that address what information is included as part of the child's early intervention or education record. Such information will then be subject to other **data governance** policies. In general, electronic **PII** on an individual child and their family collected, maintained, or used to meet requirements under Part C or Part B of IDEA would be considered part of an education or early intervention record. Although Part C and Part B regulations do not specifically reference electronic files, the **FERPA** regulations at 34 CFR 99.3 that apply to IDEA define a "record" as "any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche." This definition would include digital photos, videos, text messages and emails as long as it meets the definition of a **record under FERPA**.

Further, Part C and Part B 619 programs do not operate independently of the state agency in which they are housed. Thus, the structure of any **data governance** already within an agency is of particular importance. After first taking into consideration all relevant federal requirements, Part C and Part B 619 programs should review any policies regarding electronic communications

developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose.

Where no policy on electronic communications exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new electronic communication policies.

The DaSy Data System Framework focuses on the importance of electronic communications in the ***Data Governance and Management*** section at DG6, DG7, and DG8.

Considerations for an Electronic Communication Policy

Use the questions below to discuss the components of a comprehensive electronic communications policy. Where appropriate, procedures and operational guidance that detail specific actions for implementing this policy should be created.

1. Electronic Communications: General Provisions

a. What federal laws/regulations related to electronic communications apply to the Part C or Part B 619 program?
b. Are there additional state agency policies related to electronic communication that apply to your Part C or Part B 619 program? If yes, what are they?
c. What specific Part C or Part B 619 electronic communication policies or procedures, if any, exist in your state agency's **data governance** policies?
d. What communication methods will be covered by the term "electronic communications" (e.g., text, email, video chatting, Facebook, Instagram, Twitter)?
e. How will parents elect or choose these forms of communication?
f. What participating agencies will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?
g. Will the policy be specified at the state level or will local programs/agencies be required to develop and implement their own policies and procedures?
h. Which role within what agency/program should be contacted with questions about this policy?
i. Which role within what agency/program is responsible for ensuring adherence to this policy?
j. Which role within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
k. Which role within what agency/program is responsible for managing the implementation of this policy, including provision of training and technical assistance?
l. What consequences, if any, will apply when this policy is not followed? If the policy is not followed, what procedures are in place to report this occurrence within the agency?
m. How often will this policy be reviewed for necessary revisions?
n. How will the public be informed about this policy? How is this policy included in your agency's privacy statement? Where will it be posted on the state's website?

2. Electronic Communications: Specific Provisions

a. Under what circumstances can **PII** information be communicated electronically by agency/program/vendor staff?
b. What procedures are required to authenticate the recipient's identity?
c. What policies govern the use of personally owned devices (e.g., mobile, computers) for electronic communication and transference of **PII**?
d. What policies govern the use of personally owned devices (e.g., mobile, computers) for electronic communication when **PII** is not being transmitted?
e. What policies govern virus protection?
f. Under what circumstances is encryption of electronic communication required?
g. What procedures are required when a device is lost or damaged?
h. Under what circumstances is the information that is communicated electronically included in the child's early intervention or educational record?

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

See also: Related sections of Data Governance and Management Toolkit: Data Breach Response, Data Security and Access, and Record Retention and Data Destruction.

Resources

- **Privacy Technical Assistance Center, Data Security Top Threats to Data Protection** (Updated June 2015)
- **Identity Authentication Best Practices** (Updated July 2015)
- **Understanding the Confidentiality Requirements Applicable to IDEA Early Childhood Programs Frequently Asked Questions** (2016)

Electronic Communication Policy Template

Use, and modify as needed, the template linked below for developing an electronic communications policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and stakeholders when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Electronic Communications

DaSy The Center for IDEA Early Childhood Data Systems

Electronic Communications Policy Template

This page intentionally left blank

Electronic Communications Policy Template

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this policy regarding electronic communications is to establish authority and a process for ensuring protection of PART C OR PART B 619 personally identifiable information (PII) and other important data when sharing these data/this information from the PART C/PART B 619 PROGRAM NAME through electronic communications (e.g., texting, email, instant messaging, video chatting, Instagram, Facebook, Twitter).

DEFINITIONS

"Authentication of identity" means ensuring that the recipient of education records or the party who receives or transmits students' records is in fact the authorized or intended recipient or sender. Authentication is the process by which an education agency or institution establishes the appropriate level of identity authentication assurance or confidence in the identity of the person or entity requesting access to the records. This assurance is established through the use of a variety of vetting methodologies, which employ so-called "authentication factors" individually or in concert, to raise the level of confidence that the party being granted access is the person or entity it claims to be.

"Record" as defined by FERPA regulations at 34 CFR 99.3 is, "any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche."

AUTHORITY

NAME OF STATE is federally required to protect personally identifiable PART C OR PART B 619 data during electronic communication. The following federal AND POTENTIALLY NAME OF STATE requirements (statutes/regulations/rules/policies) apply to electronic communication:

34 CFR Part 300 – Part B Regulations

- 34 CFR 300.505

34 CFR Part 99 – FERPA Regulations

- 34 CFR 99.3
- 34 CFR 99.31(c)

The NAME OF STATE statute, regulations, and current policies that address electronic communication are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and implement policies related to electronic communication. The policy is specified at the STATE LEVEL/LOCAL PROGRAMS'/AGENCIES' LEVEL.

AGENCY, PROGRAM, ROLE, ETC is responsible for ensuring adherence to this policy in PART C/PART B 619 PROGRAM NAME. AGENCY, PROGRAM, ROLE, ETC is responsible for monitoring adherence to this policy. AGENCY, PROGRAM, ROLE, ETC will answer any questions regarding the use of electronic communication. AGENCY, PROGRAM, ROLE, ETC will provide training and technical assistance on electronic communication when requested. This policy will be reviewed INSERT TIMELINE by AGENCY, PROGRAM, ROLE, ETC , and it will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy and what procedures are in place to report this occurrence within the agency.

The public will be informed about this policy through AGENCY, WEBSITE, MANUAL, ETC and the policy is included in the agency's privacy statement (IF APPLICABLE).

APPLICABILITY

This policy applies to NAME OF PARTICIPATING AGENCY(IES) under TYPE OF MECHANISMS (e.g., contracts, subgrants, or interagency agreements). This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy.

Communication methods covered by this policy include TEXTING, EMAIL, INSTANT MESSAGING, VIDEO CHATTING, FACEBOOK, INSTAGRAM, TWITTER.

Parents will elect or choose these forms of communication through PROCESS/MECHANISM [COMPLETION OF FORM]

SPECIFIC PROVISIONS

PII can be communicated electronically by agency/program/vendor staff through INSERT CIRCUMSTANCES. Procedures required to authenticate the recipient's identity include INSERT PROCEDURES.

Policies governing the use of personally owned devices (e.g., mobile, computers) for electronic communication and *transference of PII* include INSERT POLICIES.

Policies governing the use of personally owned devices (e.g., mobile, computers) for electronic communication *when PII is not being transmitted* include INSERT POLICIES.

Virus protection policies include INSERT POLICIES.

Circumstances under which encryption of electronic communication is required include INSERT CIRCUMSTANCES.

Procedures required when a device is lost or damaged include INSERT PROCEDURES.

Circumstances under which the information that is communicated electronically is included in the child's early intervention or educational record are INSERT CIRCUMSTANCES.

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

Data Requests

Overview

State agencies for Part C and Part B 619 regularly receive requests for data from internal and external parties. While protection of **personally identifiable information (PII)** is paramount, appropriately sharing data can lead to innovations in research, policies, and practices – innovations that benefit children, families, and practitioners/teachers. Data requested may be for a summary about a subpopulation of children, such as trends in the number of children with autism over the last 15 years, or the number of referrals received from neonatal intensive care units. An external researcher or a member of another state agency might request trend data for development of grant applications, or a state legislator may request data about the entire program population of children. Part C and Part B 619 programs must balance being responsive to data requests with ensuring data confidentiality and privacy to prevent violation of state and federal requirements. Therefore, a data request policy is a necessary part of comprehensive Part C and Part B 619 **data governance**.

Part C and Part B 619 programs should develop a data request policy to establish what data are available, to whom, in what formats, for what purposes, and how data requests are to be handled. In many cases, Part C or Part B 619 staff members can help the requestor better understand the strengths and limitations of the data and increase the likelihood that agency efforts are spent on fulfilling viable requests.

A data request policy should outline the requirements for the release and use of requested data that are consistent with federal and state requirements. Part C and Part B 619 programs need to understand relevant federal and state agency regulations whether they are considering developing a new data request policy or are reviewing an existing policy.

A number of regulations apply when a data request involves releasing **PII**. Per federal Part C IDEA regulations, parents of referred children have the right to confidentiality of **PII**, including receiving written notice of, and providing consent to, the exchange of **PII** among agencies [34 CFR 303.401(a)]. Further, IDEA regulations for Part C [34 CFR 303.414(a) and (b)] and Part B [34 CFR 300.622(a) and (b)] address the circumstances in which parental consent must be obtained and when information **disclosure** is authorized without consent by **FERPA** [34 CFR 99. 31]. Finally, the Uninterrupted Scholars Act (USA) amended **FERPA** in January 2013 to permit education agencies to disclose **PII** from the education records of children in foster care placement, without parental consent, to an agency caseworker or other

What About a Record Request?
IDEA guarantees parents the right to inspect and review any education record the school system or any other participating agency collects, maintains, or uses. Additionally, parents may provide consent to service providers (e.g., pediatrician) to request their child's record to support planning and provision of services.

Part C and Part B 619 programs are required to provide this information and the request does not need to be reviewed formally to determine whether it is appropriate before approval. Therefore, this section concerns exclusively other parties requesting data not covered under record requests.

representative of a state or local child welfare agency or tribal organization authorized to access a child's case plan when the agency is legally responsible for the care and protection of the child (20 U.S.C. § 1232g(b)(1)(L)). **FERPA** has additional exceptions to the release of **PII** without parental consent including the audit and evaluation exception that requires a **data sharing agreement**. These regulations at 34 CFR 99.31 describe permissive exceptions and apply to Part B and Part C as well as to **FERPA**.

Part C and Part B 619 programs operate within the state agency in which they are housed. Thus, the structure and content of any **data governance** already within an agency is of particular importance. Before developing a data request policy, Part C and Part B 619 programs should review any policies regarding data requests developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language for this purpose.

Where no policy on data requests exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new data security and access policies.

The DaSy Data System Framework emphasizes the importance of appropriately responding to data requests in its **Data Use** section, Quality Indicators DU1 and DU2, and it **Data Governance** section, Quality Indicators DG5 and DG7.

Considerations for a Data Request Policy

Use the questions below to discuss the components of a comprehensive data request policy. Where appropriate, procedures and operational guidance that detail specific actions for implementing this policy should be created.

1. Data Request Policy: General Provisions

a. Which federal laws/regulations (IDEA/**FERPA**) related to data requests apply to your Part C or Part B 619 program?
b. Are there additional state agency policies related to data requests that apply to the Part C or Part B 619 program? If yes, what are they?
c. What specific Part C or Part B 619 data request policies or procedures, if any, exist and apply?
d. Which role, within what agency/program should be contacted with questions about this policy?
e. Which role, within what agency/program is responsible for ensuring adherence to this policy?
f. Which role, within what agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
g. Which role, within what agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
h. How is this policy shared with all participating agencies and how is the implementation of this policy monitored?
i. What role do **stakeholders** play in the development/review of this policy?
j. What consequences, if any, will apply when this policy is not followed?
k. How often will this policy be reviewed for necessary revisions?

l. How will the public be informed about this policy? Where will it be posted on the state's website?

2. Data Request Policy: Legal Considerations and Response Parameters

a. Under what circumstances can data be released and for what purposes?
b. What data and/or subsets of data are available for answering data requests and for what purposes? What level of aggregation (e.g., sample size) can be reported and for what purposes? (See **Public Reporting** section for additional information)
c. What data are classified as personally identifiable data (**PII**) or protected data? Are **PII** available for release, and if so, under what circumstances? Who (what role) can authorize release of **PII** data in response to a request?
d. How shall research data requests be handled?
    - What constitutes research?
    - What data may be requested for research?
    - What level of authority (e.g., institutional review board) must be in place to oversee the research?
    - What requirements, if any, will the state agency put in place for the researcher to report on, publish, and share data or findings back with the agency?
e. Under what circumstances will a Part C or Part B 619 program notify parents when their data are shared?
f. What provisions are in place to ensure that the data request is reasonable and consistent with the types of research questions being asked by the requestor (data minimization)?
g. Under what circumstances are agreements (e.g., memorandums of understanding/MOUs, data sharing/use agreements) needed to respond to data requests?
h. What mechanisms does the **data governance** structure have in place to ensure compliance with the requirements of the data request policy?

3. Data Request Policy: Required Information

a. Who (e.g., Part C or Part B 619 program staff, researchers, an agent of a participating agency, service providers) are eligible to potentially receive data, and under what conditions?
b. What information is required to respond to a request for data (e.g., requestor contact information, purpose of request, years of data requested, field [elements] requested, requested format [e.g., .xls, .pdf, .csv], proposed **analysis**)?
c. What requirements will be made of participating agencies to ensure continued protection of shared data?

4. Data Request Policy: Process

a. What is the method (e.g., written request, online form) for requesting data?
b. What forms, if any, will be required for completing a request?
c. How will a request be prioritized (including denied, modified, or accepted) given agency capacity and the perceived effort to provide necessary data to answer the request?
d. Which role, within what agency/program has the authority to approve/deny the data requests?
e. What is the process for approving, denying, mediating, or suggesting modifications (e.g., request could be addressed with **de-identified data**) to data requests?

f. What is the timeframe for evaluating and responding to data requests?
g. What system is in place to track requests from start to finish?
h. Which role, within what agency/program will oversee the data request process?
i. How are request determinations (approving, denying, mediating, or suggesting modifications) to be communicated to requestors?
j. Which role, within what agency/program is responsible for fulfilling the request (preparing and validating the data)?
k. Are fees associated with data requests? If so, under what circumstances and what is the fee structure?
l. How are data requests tracked and processes documented to inform a systemic approach to similar future data requests (e.g., web postings of frequently requested reports)? What is the tracking and documenting process?
m. What specific guidance is in place about safeguarding data for those who receive requested data and/or data reports?
n. Which role, within what agency/program is assigned as a point of contact about this policy?

5. Data Request Policy: Access to/Use of Data/Recognition

a. What is the expectation for reviewing and approving requested data/reports prepared by requestors prior to release?
b. What length of time will data be made available for specific purposes? (For example, will archived data be used to respond to a data request? If yes, under what data request circumstances?)
c. In what secure format are data made available (e.g., encrypted MS Excel files, secure FTP downloads)?
d. What mechanisms will be used to ensure that data are properly destroyed once they have been used for the agreed upon/intended purpose?
e. What is the expected publication reference for provided data (e.g., acknowledgement of state agency, grant number, funding source for data, etc.)?

Note: See ***Data Security and Access*** section of the Toolkit for additional information related to data security and data transfer.

When analyzing the privacy and confidentiality requirements for children with disabilities, it is critical to begin by examining the IDEA requirements first. If you or members of your staff have questions, please contact your **State Lead** in OSERS Office of Special Education Program's (OSEP) Monitoring and State Improvement Planning Division.

Footnotes

1. ***FERPA Exceptions Summary*** is a 2014 publication from the U.S. Department of Education's Privacy Technical Assistance Center intended to be a handy visual aid to help identify at a glance what **FERPA** exception applies to the data sharing work you are trying to do.
2. ***Understanding the Confidentiality Requirements Applicable to IDEA Early Childhood Programs Frequently Asked Questions*** provides responses to frequently asked questions to facilitate and enhance states' implementation of IDEA privacy and confidentiality provisions

and can be used in conjunction with the 2014 side-by-side guide of the IDEA and **Family Educational Rights and Privacy Act (FERPA)** Confidentiality Provisions.

3. ***A Little Privacy Please? Safeguarding the Privacy of Young Children with Disabilities under IDEA and FERPA*** was a December 2016 webinar in which privacy and legal experts from the U.S. Department of Education discussing answers to frequently asked questions related to privacy and confidentiality for IDEA early childhood programs.

Data Request Policy Template

Use, and modify as needed, the template linked below for developing a data request policy. Select the highlighted text and replace with your state/program information. We recommend that you consult with relevant staff and **stakeholders** when developing these policies. Upon completing the template, be sure to follow your state's processes for finalizing and enacting policy.

Download Template for Data Request Policy

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Request Policy Template

This page intentionally left blank

Data Request Policy

NAME OF PART C/PART B 619 PROGRAM

PURPOSE

The purpose of this data request policy is to establish authority and processes for external and internal requests for PART C/PART B 619 PROGRAM NAME data.

AUTHORITY

NAME OF STATE is federally required to collect and report PART C OR PART B 619 data and collects such data through data systems noted in the table below. The following federal AND POTENTIALLY NAME OF STATE requirements (statutes/regulations/rules/policies) apply to requests for PART C/PART B 619 PROGRAM NAME data that include personally identifiable information (PII):

34 CFR Part 303 – Part C Regulations

- 34 CFR 303.401(a)
- 34 CFR 303.414(a) and (b)

34 CFR Part 300 – Part B Regulations

- 34 CFR 300.622(a) and (b)

FERPA

- 34 CFR 99.31

The NAME OF STATE statute, regulations, and current policies that address data request are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

RESPONSIBILITY

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. overseeing the data for the PART C/PART B 619 PROGRAM NAME to establish and carry out processes associated with considering and overseeing any requests for PART C/PART B 619 PROGRAM data. The following PART C/PART B 619 PROGRAM NAME data systems are covered by this data request policy.

PART C/PART B 619 PROGRAM NAME Data Systems

25. Click or tap here to enter text.
26. Click or tap here to enter text.
27. Click or tap here to enter text.
28. Click or tap here to enter text.
29. Click or tap here to enter text.
30. Click or tap here to enter text.

AGENCY, PROGRAM, ROLE, ETC. is responsible for ensuring adherence to this policy. AGENCY, PROGRAM, ROLE, ETC. is responsible for monitoring adherence to this policy. Any questions regarding the data request policy will be addressed by AGENCY, PROGRAM,

ROLE, ETC.. AGENCY, PROGRAM, ROLE, ETC. will also secure or provide training and technical assistance on data requests when asked. This policy will be reviewed ANNUALLY, BI-ANNUALLY, AS NEEDED, by AGENCY, PROGRAM, ROLE, ETC. , and they will address failures to adhere to this policy. AGENCY, PROGRAM, ROLE, ETC. and AGENCY DIRECTOR shall consider and determine what, if any, sanctions or consequences are to be levied on those responsible for violations of this policy, up to and including LIST ANY SANCTIONS OR CONSEQUENCES .

The public will be informed about this policy through AGENCY WEBSITE, MANUAL, ETC. This policy shall me reviewed ANNUALLY, QUARTERLY, ETC., and such reviews will include stakeholder input when possible.

PART C/PART B 619 PROGRAM NAME Data System(s)

1. *(insert program name)*
2. *(insert program name)*
3. *(insert program name)*
4. *(insert program name)*
5. *(insert program name)*
6. *(insert program name)*

DATA REQUEST RESPONSE PARAMETERS

The table above outlines the data systems used by the PART C/PART B 619 PROGRAM NAME for program operations. The table below outlines the data that are collected in each data system:

Data System Name	Data Available
(insert name) *Ex. State IFSP System*	*(list data available)* ***Evaluation Data, Assessment Data, Eligibility Determination, Services, IFSP dates***

Requests for PART C/PART B 619 PROGRAM NAME data must be reviewed by AGENCY, PROGRAM, ROLE, ETC to determine if the requestor is asking for aggregate and/or personally identifiable information (PII). The PART C/PART B 619 PROGRAM NAME WILL/WILL NOT respond to requests for PII (see INITIATION OF REQUEST SECTION BELOW FOR ADDITIONAL INFORMATION). [IF YES] All requests for release of PII will need to be approved by AGENCY, PROGRAM, ROLE, ETC. Notification of release of PII to parents will be determined on a case-by-case basis as determined by TYPE OF REQUEST, STATE/FEDERAL REGULATIONS AND RULES, ETC.

All data requests are reviewed by AGENCY, PROGRAM, ROLE, ETC. to determine if the request is reasonable and consistent with the types of research questions being asked by the requestor. Additional information may be requested of the data requestor if the purpose of the request is unclear. An MOU, DATA/USE SHARING AGREEMENT will be necessary for REQUESTS FOR RELEASE OF PII, REPEATED DATA REQUEST, ALL DATA REQUESTS.

All data requests will require the completion of a Data Request Form (outlined below in INITIATION OF REQUEST). Use of the data once made available is limited to the purpose outlined in the original request only. Data cannot be rereleased to another entity, and any publication of program data released by the requestor will need approval of AGENCY, PROGRAM, ROLE, ETC. All data released by PART C/PART B 619 PROGRAM NAME will need to be destroyed within X years as per NAME OF DATA DESTRUCTION POLICY. AGENCY, PROGRAM, ROLE, ETC. will ensure that the data are properly destroyed by MECHANISM TO DETERMINE DATA ARE PROPERLY DESTROYED.

REQUIRED INFORMATION

INITIATION OF REQUEST

Requests for PART C/PART B 619 PROGRAM NAME data shall be submitted on a completed *Data Request Form*. The *Data Request Form* is to be publicly available at INSERT URL.

Completed *Data Request Forms* must be submitted to NAME OF OFFICE/ROLE <Alternatively: to any member of the AGENCY, PROGRAM, ROLE, ETC>. The recipient of the completed form shall acknowledge receipt by EMAIL OR OTHER WRITTEN MEDIUM within TIME PERIOD. Written acknowledgment shall include when a decision about the requested data will be made and expected date of communication about the decision back to the requester.

REQUEST REQUIRED INFORMATION

A *Data Request Form* shall be completed to initiate a data request. Sample form content areas are:

6. Requester contact information *(Required of requester)*
7. Data requested – including data elements/fields *(Required of requester)*
8. Time frame of data requested *(Required of requester)*
9. Purpose for the data request including any use of the data requested. *(Required of requester)*
10. Format of data requested *(Required of requester)*
11. IRB Approval *(Required for research requests)*

THERE ARE/ARE NOT fees associated with the data request. [IF THERE ARE FEES] The cost to cover staff time and resources is $X PER REQUEST, $X PER HOUR, ETC.

PROCESS FOR EVALUATION/APPROVAL OF REQUESTS

AGENCY, PROGRAM, ROLE, ETC. shall review the submitted data request form to ensure that all required information is included. Any incomplete data requests will be sent back to the requestor for additional information by AGENCY, PROGRAM, ROLE, ETC.

AGENCY, PROGRAM, ROLE, ETC. will review all data request forms in a reasonable time depending on the significance of the request (e.g., 4-12 weeks). AGENCY, PROGRAM, ROLE, ETC. may accept, deny, modify, or request additional information. The response shall be in writing and include the decision made and will be communicated back to the requestor by AGENCY, PROGRAM, ROLE, ETC. If the data request was accepted, the response back shall include the expected time for completing the request. For all other decisions, a brief explanation shall be provided as to why the request was denied, tabled, or delayed.

It is the responsibility of AGENCY, PROGRAM, ROLE, ETC. to act as the point of contact and to fulfill all data requests approved by AGENCY, PROGRAM, ROLE, ETC. This INDIVIDUAL/GROUP will be responsible for conducting and documenting the steps for the data analysis, preparing the data in the requested format, and sending the completed data request to AGENCY, PROGRAM, ROLE, ETC. for final approval.

Prior to release, the data requested will be reviewed by AGENCY, PROGRAM, ROLE, ETC. to ensure that the data are in the proper secure format for release (e.g., encrypted MS Excel files, secure FTP downloads) and that they do not contain any information not requested.

It will be the responsibility of AGENCY, PROGRAM, ROLE, ETC. to send the requested data to the requestor, ensuring that state and federal requirements for security and protection of data are followed (de-identification, encryption, etc.). A record of all data requests will be maintained by AGENCY, PROGRAM, ROLE, ETC. for a period of X years.

DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Governance of Data Partnerships

Overview

A **data partnership** is an arrangement between two or more parties that agree to collaborate for the purpose of advancing their mutual data interests (e.g., Part C and Early Hearing Detection and Intervention or Part B 619 and State Longitudinal Data System). Such collaboration often involves matching, linking, and/or integrating record-level data. (A **data partnership** is not needed when publicly available aggregate data from one agency are being shared and used by another.)

Given the importance and sensitivity of the Individuals with Disabilities Education Act (IDEA) data, it is critical to establish **data governance** policies when Part C and/or Part B 619 are in any **data partnership**. This Governance of Data Partnerships section of the DaSy Governance Toolkit does not address "how to" data activities and processes. Instead, it focuses on the joint governance: the legal requirements and the **management** of the **data partnership**.

Navigating This Section of the Toolkit

This Governance of Data Partnerships section of the Toolkit is for Part C and Part B 619 programs that need to share record-level data with another program or agency. It provides foundational information to prepare partners as they jointly consider and build a **data sharing agreement** and/or **data partnership management plan**. Although DaSy suggests accessing the sections in the order shown below, it is more important to start where the partners are, where the need is greatest.

What if my agency or program does not have adequate data governance policies and/or a structure?

Agencies in a **data partnership** are responsible for their own **data governance** policies. If your agency does not have adequate program-level **data governance**, DaSy encourages you to use the **Data Governance Toolkit** to establish strong **data governance** policies *before* beginning a **data partnership** with another agency or program.

This page intentionally left blank


DATA
RETENTION
DATA
DESTRUCTION

This page intentionally left blank

Data Retention and Destruction

Data Destruction: Physical destruction of the record or ensuring that personal identifiers are removed from a record so that the record is no longer personally identifiable. — 34 CFR 300.611(a) and 303.403(a)

Overview

Part C and Part B 619 programs collect, maintain, and use significant amounts of **personally identifiable information (PII)** and non-personally identifiable information to meet federal and state requirements, to provide services to eligible children and families, and to support general administration. Examples of non-**PII** are fiscal information, local agency/program information, correspondence, federal and state applications, minutes of advisory groups, and monitoring results. These data are maintained in both paper and electronic format.

It is critical that Part C and Part B 619 governance policies address record retention and data destruction. In developing their own policies and procedures, it is essential to review relevant federal and state agency regulations regarding data retention and destruction.

According to federal IDEA regulations, some **PII** data may be kept indefinitely, such as child's name, parent contact information, and providers' names, as well as entry and exit dates, attendance records, grades, classes attended, and services provided [34 CFR 303.416(b) and 34 CFR 300.624(b)]. Other data are maintained for a preestablished period based on federal and state agency requirements. Some Part C and Part B 619 programs retain data longer for use in state **accountability** longitudinal data (**PII** and non-**PII**) initiatives.

Agencies that administer Part C and Part B 619 programs must follow federal record retention requirements. The U.S. Department of Education's General Administrative Regulations at 34 CFR Part 76 specify that a state and its subgrantee (local educational agencies) must keep records of compliance with program requirements and use of grant funds. Part 76 applies to Part B and Part C of IDEA. The Part C regulations at 34 CFR 303.414(b)(2) specify that references to state and local educational authorities mean the lead agency under Part C.

Uniform Guidance regulations that apply to Parts B and C of IDEA at 34 CFR 200.333 specify that applicable records related to the federal award be retained for a period of 3 years from the submission of the final expenditure report for that fiscal year. The regulation contains several extensions to this time frame. Of particular importance to the data retention and destruction policy is the following statement: "If any litigation, claim, or audit is started before the expiration of the 3-year period, the records must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action taken." The **Family Educational Rights and Privacy Act (FERPA)**, which also applies to Parts B and C of IDEA, contains a similar provision stating that educational agencies/institutions cannot destroy educational records if there is an outstanding request to inspect or review them.

According to IDEA regulations, parents must be informed when **PII** — collected, maintained, or used — is no longer needed to provide the child with services. Further, parents may request that their child and family's personally identifiable data be destroyed consistent with these IDEA requirements. This applies to the destruction of any **PII** — collected, maintained, or used —

whether it is contained in the child's record or elsewhere (34 CFR 303.416 and 34 CFR 300.624).

Other federal noneducation requirements, including Medicaid and the **Health Insurance Portability and Accountability Act (HIPAA)**, may also apply to the timeline for retention of specific types of records. These additional federal provisions must be taken into account when developing a policy on records retention and destruction of data. Any federal requirements are minimal and state agencies may have longer required records retention time periods. It is important that any **data governance** policy in this area adhere to both federal and state timelines.

The **Privacy Technical Assistance Center (PTAC)** indicates that data destruction can include destroying, erasing, or **anonymizing** child and family data so that the data are unreadable (paper records), irretrievable (digital records), or purged of personal identifiers. State policies should address information contained in databases, server backups, file extracts, copies, and nonelectronic **PII** (e.g., paper, pictures).

PTAC identifies three categories of data destruction that may be helpful in the development of state policies (ordered from least to most aggressive):

- **Clear:** Uses programmatic **software**-based techniques, protects against simple data recovery, typically involves Read and Write commands (e.g., resetting a device to its factory state).
- **Purge:** Uses state-of-the-art lab techniques to make data recovery infeasible.
- **Destroy:** Uses state-of-the-art lab techniques to make data recovery infeasible and renders media unable to store data.

For additional information, refer to the PTAC **Best Practices for Data Destruction**.

Careful consideration should also be given to the state agency's current or planned efforts to use longitudinal data for **accountability** purposes. These data-linking and -sharing efforts could include State Longitudinal Data Systems (**SLDS**) or Early Childhood Integrated Data Systems (**ECIDs**).

Finally, state **data governance** policies on retention and destruction should specify required state timelines for the destruction of data when the data are no longer necessary or required to be maintained, consistent with any applicable federal requirements.

Part C and Part B 619 programs do not operate independently of the state agency in which they are housed. Thus, the structure of any **data governance** *already within an agency* is of particular importance. After first taking into consideration all relevant federal requirements, Part C and Part B 619 programs should review any data policies regarding record retention and data destruction developed by the agency in which their program resides. Existing policies might need to be updated with specific references or provisions related to Part C or Part B 619, in which case the considerations and the template below may be helpful in proposing language.

Where no policy on data retention and destruction exists or a separate policy related to Part C or Part B 619 is needed, the template following the Considerations section is fully editable and prepopulated with language to expedite writing new data retention and destruction policies.

The *DaSy Data System Framework* emphasizes the importance of **data governance** policies including record retention and destruction in its **Data Governance** section, Quality Indicator DG6.

Considerations

Use the questions below to discuss the components of a comprehensive data retention and destruction policy. Where appropriate, procedures and operational guidance that detail specific actions that implement this policy should be created.

1. Data Retention and Destruction Policy: General Provisions

a. Which federal requirements for record retention and destruction of data apply to your Part C or Part B 619 program?
b. Are there additional state agency policies related to record retention and destruction of data that apply to your Part C or Part B 619 program? If yes, which are they?
c. What specific Part C or Part B 619 data retention and destruction policies or procedures, if any, exist?
d. What types of data (e.g., **PII**, programmatic, fiscal, monitoring, applications) will be covered under this policy?
e. Which participating agencies will be required to follow this policy and under what mechanisms (e.g., contracts, subgrants, or interagency agreements)?
f. What program or state longitudinal data-sharing or -linking efforts are considered under this policy (e.g., **SLDs** and/or **ECIDS**)?
g. How will the public be informed about this policy? How is this policy included in your agency's privacy statement? Where will it be posted on the state's website?
h. Which agency/program should be contacted with questions about this policy?
i. Which agency/program is responsible for ensuring adherence to this policy?
j. Which agency/program is responsible for monitoring adherence to this policy, and how will the monitoring be conducted?
k. Which agency/program is responsible for managing the implementation of this policy including provision of training and technical assistance?
l. What sanctions will apply when this policy is not followed?
m. How often will this policy be reviewed for necessary revisions?

2. Data Retention and Destruction Policy: Record Retention

a. What is the retention timeline for each type of data included in this policy (e.g., **PII**, fiscal information, local agency/program information, correspondence, federal and state applications, minutes of advisory groups, and monitoring results)? Are the timelines different for state or local retention or for paper vs. electronic records?
b. What procedures and schedule will be required for data storage and archiving records, who is responsible for overseeing the process, and how it will be monitored)?

3. Data Retention and Destruction Policy: Destruction of Data

a. Which method and process of data destruction are appropriate for each type of data listed above based on the sensitivity of the data? (See PTAC **categories of data destruction** above.)
b. What timeline is required for the destruction of each type of data?

c. Who oversees that data destruction is executed on schedule and as required?
d. What procedures are followed if/when there is a request for data destruction (e.g., parent request to remove **PII** child information from paper records and the program **database**)?
e. What procedures are followed for informing parents about the agency's decision to destroy their **PII** data?

Template

Use, and modify as needed, this template for developing a data retention and destruction policy. Select the highlighted text and replace with your state/program information.

Download Template for Data Governance Data Retention and Destruction Policy (Word document)

DaSy The Center for IDEA Early Childhood Data Systems

Data Governance Data Retention and Destruction Policy Template

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Retention and Destruction Policy for NAME OF PART C OR PART B 619 PROGRAM

PURPOSE

The purpose of this policy is to establish the authority, responsibilities, and timelines for the retention and destruction of multiple types and formats of Part C or Part B 619 data consistent with federal and state requirements.

AUTHORITY

Various federal (AND POTENTIALLY NAME OF STATE) requirements (statutes/regulations/rules/policies) apply to this data retention and destruction policy.

Federal regulations are:

- IDEA Part B at 34 CFR 300
- IDEA Part C at 34 CFR 303
- EDGAR at 34 CFR 76
- Uniform Guidance at 34 CFR 200
- FERPA at 34 CFR 99

The NAME OF STATE statute, regulations, and current policies that address data retention and destruction are:

- RELEVANT STATE STATUTE
- RELEVANT STATE REGULATIONS/RULES
- RELEVANT STATE POLICIES

APPLICABILITY

This policy applies to those who collect, maintain, use, manage, operate, or are otherwise active in the control of data regardless of format. This includes staff from NAME OF LOCAL PROGRAMS/AGENCIES directly associated with NAME OF PARTICIPATING AGENCY(IES). All local programs, agencies, contractors, and staff identified in this policy must adhere to this policy. These entities and the mechanism (regulation/contract/interagency agreement) that make this policy applicable to each program/agency are listed in the table below.

Entities Covered by Policy	Mechanism

TYPES OF DATA

This data retention and destruction policy applies to PART C OR Part B 619 PROGRAM NAME data types as follows:

- Personally identifiable information (PII)
  - See definition at the end of this section.
- Non-personally identifiable information
  - Fiscal information
  - Local agency/program information
  - Correspondence
  - Federal and state applications
  - Minutes of advisory groups
  - Monitoring results
  - Other (Specify)

This policy covers data that are maintained in both paper and electronic format either at the state or local level. These data are collected, maintained, used, managed, organized or otherwise controlled by PART C OR PART B 619 PROGRAM NAME.

RESPONSIBILITY

NAME, ROLE, OF RESPONSIBLE PARTY(IES) is responsible for informing the public about this policy.

This policy will be disseminated to the public under the following mechanisms: NAME THE MECHANISMS. This policy is included in the agency's privacy statement located at LINK TO THE WEBSITE WHERE THE PRIVACY STATEMENT IS LOCATED.

NAME, ROLE, OF RESPONSIBLE PARTY(IES) should be contacted with questions about this policy.

NAME, ROLE, OF AGENCY/PROGRAM is responsible for ensuring adherence to this policy.

NAME, ROLE, OF AGENCY/PROGRAM is responsible for monitoring adherence to this policy, and the monitoring will be conducted as follows: INSERT MONITORING PROCEDURES.

NAME, ROLE, OF AGENCY/PROGRAM is responsible for managing the implementation of this policy, including the provision of training and technical assistance.

NAME, ROLE, OF PROGRAM/AGENCY/PARTY(IES) oversees that data destruction is executed as required.

Sanctions will be applied when this policy is not followed as indicated here.

NAME PROCESS FOR DETERMINING THE SANCTIONS TO BE APPLIED AND UNDER WHAT CIRCUMSTANCES AND/OR THE SANCTIONS.

NAME, ROLE, OF PROGRAM/AGENCY/PARTY(IES) receives requests for data destruction (e.g., parent request to remove PII child information from paper records and the program database). These requests are INSERT PROCEDURES FOR CONSIDERING SUCH REQUESTS AND FOR INFORMING PARENTS REGARDING THE DECISION TO DESTROY THEIR PII DATA.

TYPE OF DATA/RESPONSIBILITY/SCHEDULE/PROCEDURES/ DESTRUCTION

The table below provides information on responsibility, archiving schedule and procedures, retention, and destruction for each type of data as indicated.

NOTE: For each type of data, the duration of retention should consider all relevant federal and state requirements, as well as plans over time for the data to be used in a state longitudinal data sharing or linking effort such as State Longitudinal Data Systems (SLDS) and/or Early Childhood Integrated Data Systems (ECIDS). If necessary, create additional rows for a specific type of data to indicate state vs local and/or paper vs electronic.

Type of Data	Responsible Entity for This Type of Data	Schedule/Procedures for Archiving/Storage	Retention Duration Before Destruction	Type of Destruction Based on Data Sensitivity
TYPE OF DATA				
TYPE OF DATA				
TYPE OF DATA				
TYPE OF DATA				
TYPE OF DATA				
NAME OF DATA				
NAME OF DATA				
NAME OF DATA				

DEFINITIONS

For purposes of this policy, the following federal definitions are applicable. States may want to add additional state-specific definitions.

- Destruction - Part B of the IDEA defines the term "destruction" as the "physical destruction or removal of personal identifiers from information so that the information is no longer personally identifiable." *[34 CFR § 300.611(a)]*
- PII - As defined in FERPA, PII includes, but is not limited to:

  1) a student's name;
  2) the name of the student's parent or other family members;
  3) the address of the student or student's family;
  4) a personal identifier, such as the student's Social Security Number, student number, or biometric record;
  5) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
  6) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community,

who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and
7) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. *[34 CFR § 99.3]*

- Participating agency under Part B and Part C
  - Part B defines participating agency as "any agency or institution that collects, maintains, or uses personally identifiable information, or from which information is obtained, under Part B of the Act [IDEA]." *[34 CFR § 300.611(c)]*
  - Part C defines participating agency as "any individual, agency, entity, or institution that collects, maintains, or uses personally identifiable information to implement the requirements in part C of the Act and the regulations in this part with respect to a particular child. A participating agency includes the lead agency and EIS providers and any individual or entity that provides any part C services (including service coordination, evaluations and assessments, and other part C services), but does not include primary referral sources, or public agencies (such as the State Medicaid or CHIP program) or private entities (such as private insurance companies) that act solely as funding sources for part C services." *[34 CFR § 303.403(c)]*

ADDITIONAL STATE DEFINITIONS

This policy is effective as of INSERT DATE and will be reviewed for necessary revisions no later than INSERT DATE.

This page intentionally left blank


DATA GOVERNANCE

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

Data Governance Resources

This Special Collection displays the variety of resources we utilized when drafting and creating the DaSy **Data Governance** and **Management** toolkit. The resources are separated below into two categories:

- Overall Resources – these are general **Data Governance** and **Management** Resources.
- By Section Resources – these are the resources that were used to help draft the content in each section. Links to the resources can be found in each of the individual sections and have been compiled below for ease of access.

General Data Governance Resources

Center for IDEA Data System (DaSy) website When crafting **Data Governance** and **Management** policy, two DaSy topics are key: **Data Governance** Topic Collection, which offers 36 resources from DaSy and other TA providers. Data ... **Read more**

HHS Administration for Children and Families (ACF) This federal agency offers two resources specific to **Data Governance** and **Management**: Best Practices in **Data Governance** and **Management** for Early Care and Education: Supporting Effective ... **Read more**

Statewide Longitudinal Data Systems (SLDS) grant program This technical assistance project offers 3 helpful resources for **data governance**: Technical Brief 2. Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records (NCES ... **Read more**

Privacy Technical Assistance Center (PTAC) website The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) offers two very helpful **data governance** resources: **Data Governance** and Stewardship, a 7-page brief last updated ... **Read more**

Traveling Through Time: The Forum Guide to Longitudinal Data Systems (Book III: Effectively Managing LDS Data) This 2011 electronic book is the third in a four-part series about longitudinal data systems (LDS). It provides guidance on organizational issues, how to keep ... **Read more**

Resources by Section

With the exception of **Purpose, Structure, Process** and **Data Partnerships**, there are specific resources for each section of our **Data Governance and Management Toolkit**.

Data Breach and Response Policy

Data Breach Response Checklist This 14-page document from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) offers specific actions to be taken before a breach and in ... **Read more**

List of State Data Breach Laws This webpage from the National Conference of State Legislatures offers an interactive map listing each state's student data privacy laws, links to several individual state ... **Read more**

Data Quality

IDEA Data Center (IDC) The IDEA Data Center (IDC) offers a variety of resources related to **Data Quality** in their Resource Library. Link to website **Read more**

Building a Culture of High Quality Data This 2016 presentation from the IDEA Data Center's Interactive Institute featured a panel of staff from the **Data Quality** Campaign (DQC) and the Georgia Department ... **Read more**

Working Principles of High-Quality IDEA Data This IDEA Data Center (IDC) infographic provides definitions of key principles of high-quality IDEA data. Link to Infographic **Read more**

Data Security and Access

Privacy and Confidentiality The use of quality early intervention and education data enables policymakers, administrators, educators, service providers and parents to design and implement effective practices to improve ... **Read more**

Data System Changes

Why The Change Management Process Is Important For Disaster Recovery: This June 2014 article from the TechTarget Network addresses the importance of the change **management** process for disaster recovery. Specific roles and activities are ... **Read more**

Public Reporting

Interactive Public Reporting Engine The IDEA Data Center's Interactive Public Reporting Engine uses the IDEA Section 618 data states submit to OSEP to create easy-to-read charts and graphs. This ... **Read more**

Best Practices for Determining Subgroup Size in Accountability Systems While Protecting Personally Identifiable Student Information This 2017 report from the Institute of Education Sciences' National Center for Education Statistics was created to assist states as they develop **accountability** systems that ... **Read more**

Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting This 2010 Statewide Longitudinal Data Systems (SLDS) Technical Brief addresses the unintended **disclosure** of **personally identifiable information (PII)**, current **disclosure** prevention practices that retain some ... **Read more**

Data De-identification: An Overview of Basic Terms This 2014 document is intended to assist early intervention service programs and providers and preschool special education programs and agencies in maintaining compliance with privacy ... **Read more**

Frequently Asked Questions: IDEA Early Childhood – Disclosure Avoidance This 2014 document is an adaptation of the 2012 release of Frequently Asked Questions – **Disclosure Avoidance** intended for K-12 audiences. Presented here in the ... **Read more**

Electronic Communications

Email and Student Privacy This 2016 video from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) walks you through best practices on how to email student information. Link ... **Read more**

Understanding the Confidentiality Requirements Applicable to IDEA Early Childhood Programs FAQS The U.S. Department of Education's Office of Special Education Programs (OSEP) developed these Frequently Asked Questions (FAQs) to assist early childhood programs under the Individuals ... **Read more**

Identity Authentication Best Practices This 2012 brief offers best practice recommendations for developing and implementing effective authentication processes to help ensure that only appropriate individuals and entities have access ... **Read more**

Data Security: Top Threats to Data Protection This 2011 brief outlines critical threats to educational data and information systems. Threats are divided into two categories: technical and non-technical. A brief description of ... **Read more**

Data Requests

Forum Guide to Supporting Data Access for Researchers: A State Education Agency Perspective. This 2012 report from the National Center for Education Statistics (NCES) recommends a set of "core" practices, operations, and templates that can be adopted and ... **Read more**

A Little Privacy Please? Safeguarding the Privacy of Young Children with Disabilities under IDEA and FERPA This webinar featured privacy and legal experts from the U.S. Department of Education discussing answers to frequently asked questions related to privacy and confidentiality for ... **Read more**

Understanding the Confidentiality Requirements Applicable to IDEA Early Childhood Programs FAQS The U.S. Department of Education's Office of Special Education Programs (OSEP) developed these Frequently Asked Questions (FAQs) to assist early childhood programs under the Individuals ... **Read more**

FERPA Exceptions Summary A 2014 resource from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC), the **FERPA** Exceptions Summary is intended to be a handy visual ... **Read more**

Data Partnerships

Data Sharing Agreement Checklist for IDEA Part C and Part B 619 Agencies and Programs This 2014 document is an adaptation of the 2012 release of "**Data Sharing Agreement** Checklist" intended for K-12 audiences. Presented as a checklist, the document ... **Read more**

Data Retention and Destruction Policy

Best Practices for Data Destruction This 2014 document from the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) is a best practices guide on properly destroying sensitive student data ... **Read more**