DaSy The Center for IDEA Early Childhood Data Systems

This page intentionally left blank

DaSy The Center for IDEA Early Childhood Data Systems

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.

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?

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?

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?

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

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

This data breach response policy applies to WHO IS COVERED BY POLICY – STAFF, PARTICIPATING AGENCIES, VENDORS, CONTRACTORS, ETC., that collect, maintain,

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

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.