



Avoid the Pitfalls: Benefits of Formal Part C Data System Governance

Denise Mauzy, Bruce Bull, & Tate Gould

Since the initial authorizing legislation for Part C of the Individuals with Disabilities Education Act (IDEA) in 1986, the scope and complexity of data collected by Part C programs have significantly increased.

These data about children with disabilities and their families, collected and stored at the child level, are used for multiple purposes including administrative operations, reporting, monitoring, continuous program improvement, and informing state policy issues. Therefore, clear policies and procedures related to accountability are essential for managing the data system, improving data quality, and increasing data security and access. Additionally, ongoing public concern about the security of information of all types calls for increased scrutiny of Part C systems data governance.

Formal governance establishes responsibility for Part C data and enables program staff to improve the effectiveness of data processes and support greater use of data through the systematic creation and enforcement of data policies, roles, responsibilities, and procedures. The 2013 DaSy Needs Assessment (2013) found that only 17% of Part C programs reported having formal data governance systems in place. This brief promotes formal data governance by

- * describing the lessons learned from other industries that supports the need for formal Part C data governance;
- * outlining the risks of informal data governance and the benefits of formal data governance; and
- * providing action steps to support state Part C systems' in establishing or improving formal data governance.

What evidence do you have to answer these questions?

- * How do data elements relate to each another?
- * How are data elements and business rules formally defined?
- * Who understands what the data mean and how these data can be used?
- * How are the data protected?
- * What are all the sources of Part C data?
- * Where are all the Part C data housed?
- * What operational policies and procedures are in place to support improved data quality?
- * What role does each Part C staff member play in data security?
- * How is data quality ensured?
- * Under what circumstances can Part C data be shared? With whom? By whom?
- * When should a data sharing agreement be developed, and what safeguards and components should it include?

If you cannot produce the evidence, your Part C system will benefit from formal data governance.

Data Governance Lessons Learned from Other Industries: Keep Data Secure

The growing reliance on data necessitates reflection about how to appropriately protect, manage, and use data. The risks of increased data usage are apparent in all business sectors: risks related to data security, privacy, and consumer confidence. Yet organizations can bolster consumer trust, minimize risks, and protect against breaches through more formalized data governance.

Data governance is the overall management of the availability, usability, integrity, quality, and security of data. It is both an organizational process and structure. A data governance function sets up an environment in which program staff are assigned roles and responsibilities to work together to establish order and organization for overseeing the data. Formal data governance includes recording and sharing

processes and procedures, which pave the way for responsible data use and continuous data quality improvement. Recent survey research on data risks has shown that across a broad spectrum of companies, 43% experienced a data breach during 2013, a 10% increase from the prior year (Madden & Rainie, 2015).

Data breaches take various forms, ranging from inadvertent personal disclosure to intentional hacking or physical loss; Figure 1 gives an example for the U.S. healthcare industry. Regardless of the type of breach, the ultimate effect is the same: reduced institutional confidence and increased risk of malicious data use, which ultimately negate the positive effects that data can have on organizational goals and long-term positive results.

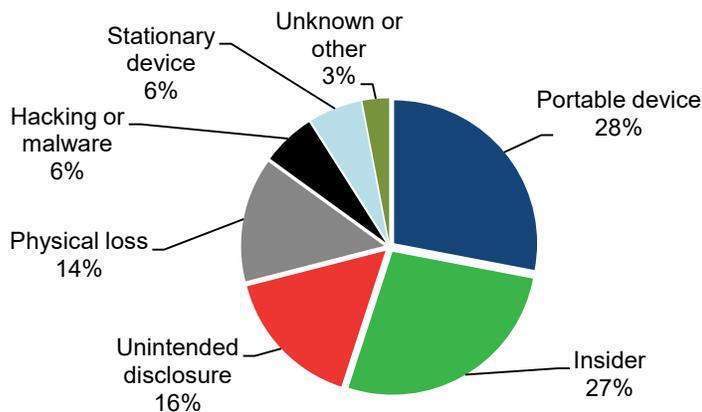
Recent data breaches in various industries have increased awareness of data security and privacy. Data breaches can take various forms.

Data breaches are not just the concern of information technology staff. A data breach can occur whether data are housed internally, in the cloud, or with a third party vendor. For Part C, data responsibility translates to all agencies and individuals participating in the system, including program staff: administrators, service coordinators, data managers, vendors, service providers, etc.

Further, Part C data have specific legal protections under IDEA and the Family Educational Rights and Privacy Act (FERPA),¹ in some instances under the Health Insurance Portability and Accountability Act (HIPAA),² as well as under state regulations, which may be more stringent than federal. Thus, there are legal and political ramifications if these data are not governed and protected appropriately. Formal data governance establishes policies and procedures to minimize risks, and establish management practices for responsible data use.

Public trust about the collection and use of data is an issue. The term “data trust deficit” describes the public’s relatively lower level of trust in an institution’s use of data than in that institution in general (Royal Statistical Society, 2014). In a recent study, the Pew Research Center found that most people are concerned about maintaining privacy of their personal data, with 90% of the respondents indicating that they want control over what personal information institutions collect about them (Madden & Rainie, 2015). Additionally, only 31% indicated confidence that government agencies can keep their records private and secure.

Figure 1. Source of U.S. Healthcare Data Breaches, January–October 2013



In 2013, a staggering 43% of companies experienced a data breach, up 10% from the prior year.

Source: http://www.americanbar.org/content/dam/aba/publications/books/healthcare_data_breaches.authcheckdam.pdf

¹ For more information, visit <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

² For more information, visit <http://www.hhs.gov/ocr/privacy/hipaa/understanding/>

Formalize Data Governance to Minimize Risk and Increase Public Confidence

Data governance structures exist along a continuum of informal to formal. Informal data governance is characterized by loosely or poorly established data policies and practices, lack of written procedures, and/or failure to clearly assign data responsibilities. Because informal structures lack established guidelines and authority for conducting data governance, risks are higher and data problems occur more frequently and are not always addressed effectively, offering no assurance of data integrity, quality, security, or confidentiality of personally identified information.

Conversely, formal data governance structures are characterized by established policies, guidelines, and practices and defined data roles for specific staff. Formal data governance

- * establishes policies and procedures that are reviewed and adjusted periodically to ensure high-quality and trustworthy data;
- * creates checks and balances to minimize risks, address risks if they emerge, and maintain data integrity;
- * provides direction and increases transparency of data to those who handle it (collect, enter, process, transfer, report) and to those who use the data for continuous improvement;
- * maintains data confidentiality and contributes to confidence in the data with internal staff members, clients, and those externally connected to the organization; and
- * outlines processes and responsibilities to ensure that all data issues are addressed.

Table 1 contrasts informal and formal data governance on selected Part C data topics. The formal governance in the right column would have policies in place supporting those processes and structures.

Table 1. Differences Between Informal and Formal Data Governance

Data Topic	Informal Data Governance	Formal Data Governance
Storage and access	Data are not encrypted and exist on an agency's network for any staff member to access.	Data are encrypted and accessible only by staff with assigned permissions based on position and training.
Stability	Data collection schedule, element definitions, and/or data processes change frequently with minimal regard to alignment with other agency data efforts. These changes make consistent reporting and data use difficult.	Collection schedule, definitions, and/or processes change only after considering impact on internal and external constituents and only in ways consistent with the purpose and vision of the broader data system.
Staff roles	Data roles and responsibilities of internal and external agency staff are fluid, frequently changed, and/or known to only a select few staff.	Data roles and responsibilities are clearly defined and written in policy, and adherence is monitored. New staff are trained on data policies and their particular role.
Sharing	Unregulated child-level data sharing is allowed among internal and external agency staff and across external agencies.	Data sharing among internal staff and external agencies is regulated by policy and is consistent with federal and state requirements. Necessary parent consent and/or formal agreements are signed, are on file, and address acceptable data storage, use, and destruction (if applicable).
Stakeholders	Stakeholders have little or no opportunity to provide input on data systems and data issues.	Stakeholder input is an ongoing part of the Part C system's data oversight, and stakeholder input is considered by the agency.

Two scenarios illustrate the potential risks of informal data governance compared with benefits of formal data governance.

Scenario 1: A data manager makes changes to the statewide Part C data system.

Type of Governance	Action	Potential Outcome
Informal governance	Part C data manager requires changes be made with minimal lead time and without any input from program staff or stakeholders. Because of the compressed time frame, staff do not document changes to the data dictionary or update policies and procedures. Little or no agency communication occurs with other associated agency data staff or with local agencies that provide data.	Local Part C agencies do not have adequate lead time to modify (where applicable) local data systems to align with the changes. Changes may not align with other state agency data. Since limited, or no, business rules were developed during the system change, there is potential for poor or inconsistent data. Local providers and other end users are not adequately trained in a timely manner, resulting in a lack of understanding between state and local program staff.
Formal governance	Part C data manager seeks stakeholder recommendations for changes. Formal recommendations are submitted to an internal governance committee within the state agency and adhere to established lead-time policies for data changes. The governance committee documents and disseminates updated policies and procedures, including data business rules, to all interested and affected parties in a timely manner. Adequate plans are developed for training to address these changes.	Local Part C agencies have adequate lead time to modify (where applicable) local data systems to align with the changes. Clear policies exist to align Part C data collections with other agency data. Business rules are developed to support state and local entry of the data, resulting in improved data quality. Necessary training and technical assistance are available in a timely manner. The reason for changes, timelines, and ramifications are understood by all.

Scenario 2: A parent contacts the Part C program and requests that his child’s initial evaluation information be deleted from the data system. Although the child was evaluated and found eligible for services, the family declined Part C services and sought services privately.

Type of Governance	Action	Potential Outcome
Informal governance	The Part C data manager accesses the back end of the data system and deletes all data associated with the record. There is no method to track this action or to indicate an “expunged” status. There is no communication with the local Part C agency informing it of this request or subsequent actions.	The child’s record is totally deleted. No transaction record in the state data system or notes in the file (at the local level) explain that data were deleted. Therefore, local and state data and reports will differ. Consistent information will not be available for reports (e.g., dispute resolution).
Formal governance	The Part C data manager reviews the standing governance policies related to deletion of data on parent request. Finding no policy, the Part C data manager requests a review by the agency procedural safeguards staff and data governance committee. The committee reviews the request and, after consulting with the agency legal staff and data system staff, establishes a policy for conditions allowing for the removal of potentially identifiable information from the record using a newly established process vetted by agency attorneys.	The record maintains necessary data elements so that reporting remains accurate and complies with the policies and legal requirements of the program or agency.

Action Steps: How to Establish or Improve Formal Data Governance

DaSy has identified three steps for Part C programs to establish or improve formal data system governance: (1) clarify who will be involved; (2) assess the status of the current data governance system; and (3) develop a plan that considers timelines, resources, and stakeholder input. The DaSy Data System Framework (2014a), available on the DaSy website, is a resource available to Part C coordinators, data managers, and other state staff that will assist in establishing or improving formal data governance and management for Part C programs.

Step 1: Clarify Who Will Be Involved

The first step is for Part C programs to clarify who should be involved and their roles with formalizing the governance of Part C data. The Part C lead agency is responsible for ensuring the quality, integrity, reliability, and confidentiality of Part C data. Therefore, formal governance should be established either through dedicated Part C data governance or as a part of a larger data governance body representing all data within the broad lead agency structure. The lead agency should designate someone (e.g., Part C data manager) to be specifically responsible for compiling, synthesizing, and organizing Part C data. The designee should also understand how Part C state data are associated with other agency data (internal agency data, external agency data). The lead agency administration should support data managers’ work by connecting and enhancing data governance, providing the time that formalized data governance requires, understanding and communicating about Part C data with interested constituencies, and using Part C data for program improvement efforts.

Step 2: Assess the Status of the Current Data Governance System

Part C programs should look critically at the current data governance and management structures to determine areas where improvement is necessary. The [Data Governance and Management subcomponent](#) of the DaSy Data System Framework (2014b) provides a means to assess the status of Part C data governance. DaSy recommends completing the data governance and management subcomponent self-assessment that accompanies the framework. The end result will be a snapshot of agency current data governance status with areas for potential improvement. The self-assessment scores will inform actions, including DaSy technical assistance, going forward.

Step 3: Develop a Plan That Considers Priorities, Timelines, Resources, and Stakeholder Input

After completing the self-assessment, it is recommended that the Part C program create a plan to develop or improve data governance structures. DaSy is available to assist in the development and implementation of the plan, which may include the following actions:

- * Identify and recruit administrative support to champion this effort
- * Consider the political environment and administrative structures
- * Generate support from the broad Part C community
- * Develop a strategy for engaging key stakeholders and leadership and garnering their support
- * Identify key steps for formalizing and improving governance, using information from the self-assessment
- * Develop a list of data governance policies needed
- * Develop a timeline for formalizing and improving data governance
- * Identify resources needed.



For assistance in completing the DaSy Framework and developing a plan for formal data governance, contact DaSy.
Phone: 650-859-3881
Email: dasycenter@sri.com

References

- DaSy Center. (2013). *IDEA Part C and Part B 619 state data systems: Current status and future priorities*. Retrieved from <http://dasycenter.org/idea-part-c-and-part-b-619-state-data-systems-current-status-and-future-priorities/>
- DaSy Center. (2014a). *The DaSy data system framework*. Retrieved from <http://dasycenter.org/resources/dasy-framework/>
- DaSy Center. (2014b). *DaSy framework subcomponent: Data governance and management*. Retrieved from <http://dasycenter.org/resources/dasy-framework/data-management/>
- Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. Retrieved from www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/
- Royal Statistical Society. (2014). *New RSS research finds 'data trust deficit', with lessons for policymakers*. Retrieved from www.statslife.org.uk/news/1672-new-rss-research-finds-data-trust-deficit-with-lessons-for-policymakers

Suggested Citation

Mauzy, D., Bull, B., & Gould, T. (2016). *Avoid the pitfalls: Benefits of formal Part C data system governance*. Menlo Park, CA: SRI International.

About Us

The contents of this brief were developed under a grant from the U.S. Department of Education, #H373Z120002. However, those contents do not necessarily represent the policy of the U.S. Department of Education, and you should not assume endorsement by the Federal Government. Project Officers, Meredith Miceli and Richelle Davis.

The DaSy Center is a national technical assistance center funded by the U.S. Department of Education, Office of Special Education Programs. The DaSy Center works with states to support IDEA early intervention and early childhood special education state programs in the development or enhancement of coordinated early childhood longitudinal data systems.

To learn more about the DaSy Center, visit the DaSy Center website at <http://www.dasycenter.org/>.

