disc
Data Integration Support Center
WestEd

2023
Issue 3

Using a Legal Framework Approach for Integrated Data Systems

INTEGRATED DATA SYSTEMS connect data over time and across sectors to provide data insights that support leaders in answering policy questions, directing resources, and better supporting individuals.

Having access to cross-sector data can be powerful. By linking data across various public agencies, states can create a more holistic picture of outcomes for people in education, health care, the workforce, and beyond. This clearer picture enables a better understanding of the complex needs of individuals and communities, which can inform the design of new strategies and interventions to address those needs and the evaluation of the effectiveness of programs and policies on desired outcomes. The systems that cohesively bring together data from various agencies are known as *integrated data systems*.

While there are significant benefits to integrated data systems (IDSs), one of the main challenges to combining data sets from disparate sources is complying with the requirements imposed by the different federal, state, and local laws that may govern each of the data contributors and their particular data types. Additional layers of complexity are created by state laws pertaining to linked data sets and broader obstacles relating to issues such as governance, funding, and legal risks.

This document provides information for states, public agencies, and other parties interested in facilitating data sharing and implementing IDSs. Specifically, the document explores how a legal framework approach

can inform the use, sharing, and protection of data in an IDS, including

- the complexity of linking information across state agencies given the regulatory frameworks in the United States,
- the value of a legal framework approach,
- tips and key questions to guide the development of legal frameworks, and
- case studies from two states.

The Complexity of Linking Data Across Sectors in the United States

In the United States, linking data across sectors is complicated by several factors. Federal data privacy regulations take a piecemeal approach that is based on the type of entity that initially collects data. For example, there are different laws for federally funded education institutions compared to covered health care entities. There are also rules that govern specific types of data collected, such as protected health information, student loan information, social security numbers, and federal assistance data. In addition to federal laws, state privacy and security laws apply additional restrictions to data use. By contrast, laws such as the European Union's GDPR (General Data Protection Regulation) or Brazil's LGPD (in English: Brazilian General Data Protection Law) focus on comprehensive human privacy protections and are more cohesive. Further, the privacy landscape in the United States is in constant flux, often in response to issues that emerge at both the state and federal levels.

The legal framework approach to linking data

There are many isolated legal requirements for combining data across sectors, sometimes even in conflict with one another, that make it difficult to create an IDS. Rather than attempt to resolve each legal requirement as a stand-alone concern, it can be helpful to adopt a legal framework approach. An initial step using this approach can be to map out the nontechnical processes for data connection and data use, then evaluate what should be included in legal agreements in the context of relevant laws, regulations, and contracts. Understanding the legal framework in its totality helps to determine what is mandatory, permissible, and prohibited within the IDS.

Specifically, a legal framework delineates privacy and security requirements when linking data and establishes access and use restrictions for the data in the IDS related to the IDS's overarching purpose. The legal framework may vary based on the IDS content and uses. For example, a legal framework may clarify that only aggregated data may be used for studies and evaluations, or it may allow staff at data-contributor agencies to access individual-level integrated data to inform services to clients whom they serve.

The legal framework informs written agreements relating to the system. It also creates a common understanding of what default conditions apply if a provision is not expressly covered by a written agreement. The legal framework and written agreements, in turn, help set parameters for the technical process by which information will be linked.

Tips and Key Questions to Guide the Development of Legal Frameworks

Identify the key contributors and governance structures

The agencies participating in an IDS will need to disclose personally identifiable information to the entity that will host and operate the IDS. Therefore, an IDS requires a governance framework that accommodates the federal and state legal restrictions of each contributor.

Data contributors and users are critical to the success of IDS efforts. Effectively engaging contributors is a key component of ensuring that an IDS is sustainable and that it continues to meet the needs of contributors, policymakers, families, program staff, and the public. Successful governance includes identifying and engaging the appropriate collaborators. For example, it is helpful to address the following questions:

- Who are the key collaborators needed for prioritizing, defining, developing, and rolling out the IDS initiatives?
- Which entities will contribute data to the IDS? Will it just be state agencies, or will other parties be included (such as private entities that can provide supplementary information)?
- How are the data contributors structured, governed, and/or funded? Are there potential issues that need to be addressed based on the contributors' different organizational structures (such as Executive Branch agencies versus separate legal entities)?
- How will the entity that implements the IDS be structured, governed, and funded?

Map the legal landscape

Once the collaborators have been identified, relevant laws and regulations can be documented. Because each of the entities that are contributing data to an IDS and the entity that implements the IDS may have different regulatory constraints on appropriate use cases, protection requirements, and allowable disclosure of protected information, entities that are participating in an IDS should map out what laws or restrictions apply to which data and when. For example, key federal laws that may apply to an IDS that combines early childhood, primary school, secondary school, and workforce data are the Family Educational Rights and Privacy Act (FERPA), Higher Education Act (HEA), Health Insurance Portability and Accountability Act (HIPAA), Workforce Innovation and Opportunity Act (WIOA), and Department of Labor (DOL) regulations.

It is also important to analyze relevant laws to understand the rights and liabilities that exist for each of the participating entities on topics that are not explicitly addressed in the legal agreements for the IDS. It is critical for the IDS leaders to consult with legal counsel in the early planning stages of the IDS because legal counsel's role is to protect and promote their client's interests. If other parties are not familiar with constraints that are specific to a particular data

With a legal framework in place, states can identify the specific content that needs to be covered in memoranda of understanding and ensure that these requirements are consistently included in all agreements.

contributor, it can create challenges for reaching a compromise in how to organize, develop, and select data for the IDS. This compromise generally involves a more restrictive approach to how the contributors' data are used and shared in the IDS. Adopting a more restrictive context can help to build trust among data contributors. Leveraging data contributors' current agreements and practices can also provide common ground and early successes in drafting legal agreements.

When mapping out the legal landscape of the IDS, it may be helpful to address the following questions:

- Are state agencies permitted to contribute data to another entity under state law?
- If private entities are included in the data system, are there any legal barriers regarding sharing data or allocating risk between public- and private-sector entities?
- Are there existing model agreements or templates at the state level or used by the data contributors that are either required or already in place that can be leveraged?

Determine how data may be accessed

After identifying the governance framework and establishing a common understanding of applicable laws permitting data sharing among the relevant partners, the next step is to consider how requests to use the linked data will be approved and what requirements will be established for those accessing the information. Any structure for decision-making about data access must be grounded in laws and regulatory frameworks, like rule-making authority, administrative procedures requirements, public meeting laws, and public records requirements. Many states now impose far stricter release restrictions for disclosing information at the level of a specific individual. These restrictions include requiring that data only be released for groups of people above a minimum threshold number or requiring that disclosure-avoidance methods be applied prior to the release of data analyses based on individual-level information. For example, Nevada has laws that attempt to address the disclosure of individual-level data. In contrast, Colorado has run into reporting issues due to the small numbers of students at rural schools and schools with small populations.

When determining how data in the IDS can be accessed, issues to decide on include the following:

- When is it appropriate for linked data to be shared?
- Who should have access to this information?
- How should the legal framework vary for cases where access is provided to individual-level records versus aggregate, properly de-identified information?
- How should the legal framework vary based on who is accessing the information?

Determine issues related to security and data breaches

With the increasing challenge of maintaining security due to cyberattacks, many state agencies are seeking to establish clearer legal guidelines for handling data breaches and their associated costs. As with other legal regulations, state agencies may be responsible for both federal security standards and state rules that have been developed piecemeal to address discrete events. The data contributors may also want legal agreements to expressly address the risk created by merging data sets.

Issues to explore include the following:

- Are there statewide standards about data breaches or data-breach notification that public agencies contributing data must follow? Are all data contributors subject to the same provisions?
- Are all contributing agencies similarly situated regarding liability and possible immunity and funding? If the legal agreements are silent on indemnification, who would be responsible for the costs of a data security incident?
- What level of controls needs to be in place for each contributing entity and the entity that implements the IDS, including provisioning, frequency of contribution, permissions, and security requirements?

Create templates when possible

One of the challenges of data sharing is the time spent creating custom legal agreements every time data will be linked or accessed. With a legal framework in place, states can identify the specific content that needs to be covered in memoranda of understanding and ensure that these requirements are consistently included in all agreements. They can also identify whether different templates are required for different contexts. For example, a different template may be used when data contributors are sharing information among themselves, as opposed to external parties that may access data for research or program implementation.

When determining aspects of legal templates to use, consider the following questions:

- Given federal and state requirements, what information needs to be consistently represented in legal agreements (such as allowable use or relationship of the entity accessing the data to the data contributor)?
- What components of a legal agreement (such as definitions, controlling laws, data security requirements, nondisclosure rules, liability, and termination) could be inserted as boilerplate, particularly among data contributors and the entity hosting the data?
- Is it preferable to have third parties that will be accessing data sign individual data-use agreements with each data contributor? Or is it feasible to create a master template that includes the requirements of all data contributors?

Identify whether laws need to be changed

In instances in which states have adopted data-use regulations that are stricter than federal privacy laws, changes may be needed to state laws, in addition to crafting legal agreements. For example, California has regulations that are considered stricter than the federal regulations. States may also elect to pass laws that specifically permit or restrict data sharing for an IDS, address conflicts among related state regulations, or establish the authority of data contributors, particularly as a mechanism for establishing transparency regarding which data will be included and how they will be used.

Questions to consider include the following:

- What current state laws are hampering data exchanges and access?
- How could state law be amended in ways that help to clarify the content and uses of the IDS?
- When establishing a rationale for new laws, what models for allowable use could be referenced that enable data exchanges and access under federal frameworks or other agency protocols?

Determine which issues can be resolved outside of contractual agreements

As with most complex projects, some elements governing data linkage and use will be unknown at the time that the legal framework is created. For example, some systems are created with only a few initial data contributors—with additional data contributors included later as the IDS evolves. Because data security standards are continuously evolving, some details are best left undefined in the legal written agreements. Rather than waiting to clarify all these elements, legal agreements can make reference to documented policies that may need to be added or amended over time. Unknowns may provide opportunities to maintain purposeful flexibility. The legal framework should be used to identify the areas of flexibility.

Questions to consider include the following:

- What types of requirements are likely to evolve rapidly and thus be better documented through policies rather than legal agreements?
- What mechanisms could be used to finalize and ensure compliance with those requirements, outside of a legal agreement?
- What general processes or principles are appropriate to include in a legal agreement that would provide sufficient criteria for decisions that will be made later?

Examples

The following examples summarize some of the ways that Connecticut and Kentucky are using the legal frameworks approach to facilitate data sharing.

Connecticut

Developing templates for data sharing

Connecticut is developing a set of flexible and durable data-sharing agreements as part of an internal review on how to improve interagency data sharing, particularly as education and workforce data are augmented with social service information. Connecticut's approach includes creating four types of legal agreements:

- **Letter of Intent:** a document that does not obligate state agencies to share specific data but that states each respective agency's arrangement to help develop a formal process for sharing data
- **Enterprise Memorandum of Understanding:** a legal document that outlines how data may be shared in accordance with the IDS's governance process, such as roles and responsibilities, privacy and security requirements, and data-matching specifications

- **Data Sharing Agreement:** a legal document for sharing information using the state's data-linking hub under the terms established in the Memorandum of Understanding, including how data are transferred, the specific data points being shared, and the legal basis for data sharing
- **Data Use License:** a legal document signed by the receiver of a data set establishing permitted data use; indicating that ownership remains with the data provider; documenting institutional review board approval; and providing terms for authorized use, disclosure, and destruction

More information about the work in Connecticut can be found in the Connecticut General Assembly Report, Legal Issues in Interagency Data Sharing.

Kentucky

Passing state laws to allow for data sharing and use

The Kentucky Center for Statistics (KYStats) has a legal framework that is based on five state laws. The legal framework provides transparency regarding what data will be used and why. The laws cover the following aspects of IDS implementation:

- identifying key definitions
- establishing KYStats as a statewide longitudinal data system
- describing overall duties of KYStats
- documenting duties and functions of the governing body
- establishing a formal guidance body

More information about the work in Kentucky can be found in these locations:

- KYStats Statutes included in the legal framework
- Summary of Select Statewide Longitudinal Data Systems (California Competes)

How the Data Integration Support Center Can Help

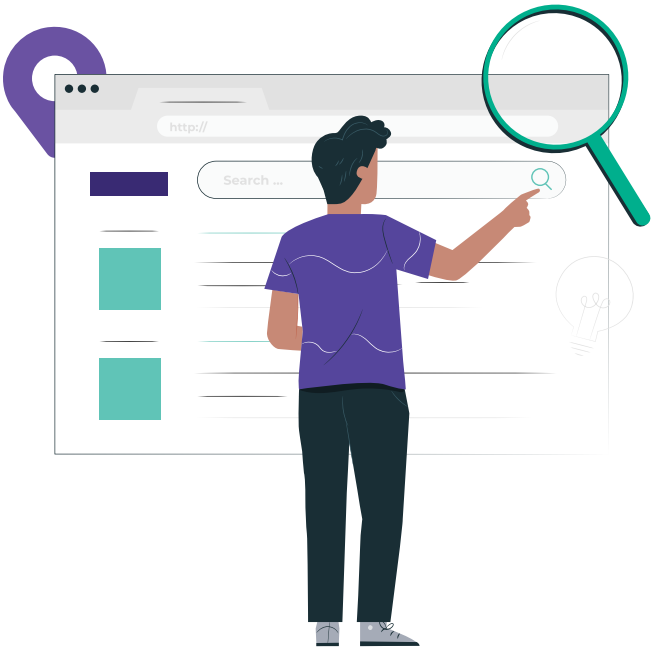
The Data Integration Support Center (DISC) at WestEd can serve a critical role and help alleviate the following potential gaps when creating a legal framework. DISC offers technical assistance to public agencies free of cost. Forms of technical assistance that can be provided by DISC include the following:

- mapping IDS data to applicable laws to expedite the development of legal frameworks
- providing legal assistance to develop a state-specific framework approach
- developing data-sharing agreement templates factoring in state, local, multisectoral-privacy, and security-regulatory requirements
- reviewing and curating privacy and security resources and tools online for public agencies
- reviewing applicable and/or required security frameworks and approaches needed to align with the required legal framework
- providing external security and privacy analysis of existing or developed legal or security frameworks by industry experts
- providing expert facilitation for legal, security, and technical architecture teams and other interested parties to address privacy, security, and legal challenges related to integrated data
- providing expert consultation and industry references to partner organizations specializing in policy, vendor, sectoral, or technical resources

Resources

The following are some readily accessible sites that provide informative and useful resources to consult as organizations consider building a legal framework to create or further develop an IDS:

- Statewide Longitudinal Data Systems (SLDS) Grant Program website: Developed by the National Center for Education Statistics, this site includes a variety of resources that complement a legal framework. These resources can be used to make sure an IDS has the essential building blocks for a successful data system in place and to benchmark progress in planning, implementing, and enhancing an IDS.
- SDLS Framework: This framework provides a helpful benchmark to understand an IDS.
- Integrated Data Systems and Student Privacy: This guidance document supports the development of a legal framework by explaining how FERPA must be considered in an IDS.
- Supporting the Use of Administrative Data in Early Care and Education Research: The Administration for Children & Families published this research series, which includes several resources that support the development of a legal framework for IDSs.



Suggested citation: McWilliams, M., Booth, K., & Rodriguez, B. (2022). *Using a legal framework approach for integrated data systems*. WestEd.