

# Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration

Actionable Intelligence for Social Policy,  
Expert Panel Report

Authors

Amy Hawn Nelson, Deja Kemp, Della Jenkins,  
Jessie Rios Benitez, Emily Berkowitz, TC Burnett,  
Kristen Smith, Sharon Zanti, Dennis Culhane

JUNE 2022



## Acknowledgments

*Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration* was created by Actionable Intelligence for Social Policy (AISP) based upon more than a decade of working with and learning alongside our Network and Learning Community Sites, with generous support from the Annie E. Casey Foundation.

This resource builds upon AISP's [Introduction to Data Sharing and Integration](#) (2020), by Amy Hawn Nelson, Della Jenkins, Sharon Zanti, Matthew Katz, TC Burnett, Dennis Culhane, and Katie Barghaus, and AISP's [Quality Framework for Integrated Data Systems](#) (2021), by Della Jenkins, Emily Berkowitz, TC Burnett, Dennis Culhane, Amy Hawn Nelson, Kristen Smith, and Sharon Zanti. It also draws from [Legal Issues for IDS Use: Finding a Way Forward](#) (2017), an AISP expert panel report by John Petrila, Barbara Cohn, Wendell Pritchett, Paul Stiles, Victoria Stodden, Jeffrey Vagle, and Mark Humowiecki.

We also recognize members of our AISP Legal Advisory Workgroup, who provided invaluable review of this resource, including Karen Barber, Richard Gold, Paul Hogle, Samuel Kohn, Elliot Regenstein, Joy Royes, and Paul Stiles. We are particularly indebted to Richard Gold, who crafted the original legal agreement templates we include in the appendices, and John Petrila, the lead author of the previous iteration of this guidance (2017). Both have patiently and substantively guided AISP's approach to supporting legal frameworks for successful cross-sector data integration over the years.

### Suggested Citation

Hawn Nelson, A., Kemp, D., Jenkins, D., Rios Benitez, R., Berkowitz, E., Burnett, TC, Smith, K., Zanti, S., Culhane, D. (2022). *Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration*. Actionable Intelligence for Social Policy. University of Pennsylvania.

### Disclaimer

Finally, this resource is not intended to constitute legal advice, nor is it a substitute for consulting with legal counsel. All information and content are for general informational purposes only. Readers should always consult with their attorney for specific legal advice.

# Table of Contents

<b>Introduction</b> .....	3
▶ <b>How to use this document</b> .....	4
▶ <b>Quality Framework for IDS</b> .....	4
<b>Why: The Four Questions</b> .....	5
▶ <b>Is this legal?</b> .....	6
Authority.....	6
Access.....	7
Practice: Defining Access and Use to Determine Legality.....	9
▶ <b>Is this ethical?</b> .....	10
Social License.....	11
Weighing Legal Risks of Data Integration.....	12
Practice: Considering Risks and Benefits to Determine Ethical Use.....	13
▶ <b>Is this a good idea?</b> .....	13
Practice: This is legal and ethical. Is it a good idea?.....	14
▶ <b>How do we know? Who decides?</b> .....	14
Data Governance.....	14
Practice: Considering the Four Questions.....	20
<b>How: Drafting the Legal Agreements</b> .....	23
▶ <b>Memorandum of Understanding (MOU)</b> .....	25
▶ <b>Data Sharing Agreement (DSA)</b> .....	26
▶ <b>Data Use License (DUL)</b> .....	26
▶ <b>Consent</b> .....	27
▶ <b>Practice: Evaluating Your Legal Agreements</b> .....	27
<b>How: Site Examples</b> .....	29
<b>Tribal Data Sovereignty</b> .....	38

## Table of Contents

<b>Federal and State Laws</b> .....	38
▶ <b>Health Insurance Portability and Accountability Act (HIPAA)</b> .....	40
▶ <b>Federal Education Rights and Privacy Act (FERPA)</b> .....	40
▶ <b>Federal Regulations Governing the Confidentiality of Alcohol and Substance Abuse Treatment Records (42 CFR Part 2)</b> .....	41
▶ <b>The Homeless Management Information System (HMIS)</b> .....	41
▶ <b>The Privacy Act</b> .....	42
<b>Conclusion</b> .....	42
<b>Common Definitions</b> .....	43
<b>References</b> .....	45
<b>Appendix A: Relevant Federal Law and Policy</b> .....	48
<b>Appendix B: Selected State &amp; Tribal Laws, Policies, and Rules</b> .....	50
<b>Appendix C: Sample Executive Orders and Legislation to Facilitate Data Integration</b> .....	52
<b>Appendix D: Definitions for Legal Framework for StateIDS</b> .....	53
<b>Appendix E: EMOU Checklist</b> .....	65
<b>Appendix F: Annotated EMOU Template</b> .....	56
<b>Appendix G: DSA Checklist</b> .....	64
<b>Appendix H: Annotated DSA Template Between IDS Lead and Data Provider</b> .....	66
<b>Appendix I: DUL Checklist</b> .....	73
<b>Appendix J: Annotated DUL Template Between IDS Lead Agency and Data Licensee (or Recipient)</b> .....	75

# ❖ Introduction

*Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration* was created by Actionable Intelligence for Social Policy (AISP) to support the essential and challenging work of exchanging, linking, and using data across government agencies. Cross-sector data sharing and integration has become more routine and commonplace, and for good reason. When governments and their partners bring together data safely and responsibly, policymakers and practitioners are better equipped to:

- Understand the complex needs of individuals and families
- Allocate resources where they're needed most to improve services
- Measure impacts of policies and programs holistically
- Engage in transparent, shared decision-making about how data should (and should not) be used
- Institutionalize regulatory compliance

Data sharing and integration is also not without risks, and clear legal frameworks are essential to mitigate those risks, protect privacy, and guide responsible data use. Designing the appropriate legal framework for the context can be a complex task and a test of endurance. This resource was created to frame out key considerations and provide effective practices for agencies working to “find a way forward” to share and integrate data.

**Administrative data** are data collected during the routine process of administering programs, and are used to support evaluation, analysis, and research. Reusing administrative data is essential to support audit, evaluation, research, and evidence-based practice in public policy and programs.

We generally refer to cross-sector infrastructure and data governance efforts that facilitate the reuse of administrative data as integrated data systems (IDS), but they have other names, including data hubs, data collaboratives, and data intermediaries. Whatever they are called, all efforts that seek to leverage integrated data to improve individual and population outcomes will likely face common ethical, relational, legal, and technical considerations.

**While data sharing is often a precursor to data integration, this resource specifically addresses legal considerations to establishing cross-sector data integration, which, for purposes of this report, means the inclusion of identifiers.** It is designed for legal counsel and agency leaders who are tasked with establishing routine data integration across government agencies, and is based on the following assumptions:

- There are risks and benefits to sharing and integrating data that must be carefully considered
- The legality of data integration depends on the specifics of data access and use
- Not only must data integration be legal, it must be ethical and a good idea
- Ethical use is context specific and requires strong data governance and legal frameworks (see our [Integrated Data Systems Quality Framework](#) for more on key components of data integration)
- Data integration is iterative, and as relational as it is technical. Collaboration among partners should be prioritized throughout the process to ensure continuous improvement

- “Finding a way forward” can be a heavy lift, but it can be worth the time, energy, and resources to collaboratively craft and use a legal framework that facilitates routine and sustainable integration

If you are new to this work, we encourage you to start with our [Introduction to Data Sharing & Integration](#)<sup>1</sup> as a primer on the basics of using, sharing, and integrating administrative data.

### ► How to use this document

This resource is based on the experience of practitioners who, collectively, have decades of experience developing strong data governance and legal frameworks to support cross-sector data integration. Each section frames out key concepts and then provides prompts for discussion to move toward action.

First, we introduce the *Why* of this recommended approach. We guide the reader through key questions that will need to be answered through the legal framework to ensure integration is legal, ethical, and a good idea, and describe both how you will know and who decides whether these conditions are met, with examples to help guide the work. We then offer the *How*, and 1) walk through the essential components of each legal document, 2) provide explanations of the documents that should be included within a legal framework, and 3) discuss how they work together to operationalize interconnected pieces that lead to a high-quality IDS. Next, we present site examples that describe current legal frameworks that facilitate routine data integration, checklists, and annotated agreements. Finally, we examine the federal and state laws relevant to data integration. The goal is to give you the understanding and tools to avoid impasse and “find a way forward.”

### ► Quality Framework for IDS

While every data integration effort is different, we have identified five key components of quality that set successful data integration efforts apart. Please note that while these components are interrelated, this resource focuses on just the first two components—Governance and Legal—which set the foundation for success. The following table provides an overview of the five components that make up AISP’s [Quality Framework for IDS](#).<sup>2</sup>

<b>Governance</b>	Data governance is the people, policies, and procedures that support how data are used and protected.
<b>Legal</b>	Whether data can be shared legally depends on why you want to share, what type of information will be shared, who you want to share with, and how you will share the data. Legal agreements should reflect the purpose for sharing, document the legal authority to serve that purpose, and ensure that data sharing complies with all federal and state statutes.
<b>Technical</b>	Technical components are created to support analytics and insights that can help further improvements in policies, practice, and outcomes.
<b>Capacity</b>	Data sharing capacity refers to the staff, relationships, and resources that enable an effort to operate governance, establish legal authority, build technical infrastructure, and above all else, demonstrate impact.
<b>Impact</b>	All components of quality—governance, legal agreements, technical tools, and staff capacity—exist to drive impact.

1 See [Hawn Nelson, Jenkins, Zanti, Katz, Burnett, Culhane, Barghaus, et al. \(2020\)](#).

2 See [Jenkins, Berkowitz, Burnett, Culhane, Hawn Nelson, Smith, & Zanti \(2021\)](#).

# ❖ Why: The Four Questions

When working to establish data flow across public sector organizations, specifically government agencies, the initial question partners typically ask is, “Is this legal?” But while this is often the first question, we also acknowledge that it is the lowest bar. To ensure use is both legal and ethical, we strongly encourage you to grapple with broader considerations to help you decide, together with your stakeholders, whether and how to move forward with data integration.

We recommend asking the same four questions throughout all stages of this work:

 <b>1. IS IT LEGAL?</b>	 <b>2. IS IT ETHICAL?</b>	 <b>3. IS IT A GOOD IDEA?</b>
<p>What legal authority is in place to use these data?</p> <p>Are there federal or state statutes that prevent or constrain this data access or use?</p> <p>What are the particular state and federal law requirements enabling data sharing?</p>	<p>Do the benefits outweigh the risks, particularly for groups historically marginalized by discriminatory systems?</p>	<p>What action can be taken as a result of this data use?</p> <p>What can reasonably be changed or improved based upon this analysis?</p> <p>Is this a priority among marginalized populations and/or individuals included in the data system?</p>
 <b>4. HOW DO WE KNOW? WHO DECIDES?</b>		
<p>This is typically determined by agency-involved legal counsel.</p>	<p>This is typically determined by a data governance group, during the review process for data requests, that should include a variety of stakeholders, those “in” the data and users of the data.</p>	<p>This is typically determined by a data governance group, including data stewards who have deep expertise of the data, and data owners who will respond to insights that emerge from the analysis.</p>

## ▶ Is this legal?

There is no simple answer to whether data sharing and integration is legal.

It all depends on:

- The legal authority of the data owner, integrator, and user
- Why you want to share and integrate information
- What type of information will be shared and integrated
- Who you want to share it with and who conducts the integration
- How you will share the information once the integration occurs

Thinking through these concepts can help you to better understand the legal parameters around your data integration efforts.

## Authority

When determining the appropriate legal framework to guide data sharing and integration, begin by identifying relevant legal considerations and authority for data access and use. While contracts (i.e., legal agreements) are the most common legal authority used to facilitate data sharing, cross-sector data integration efforts typically use a combination of authority to support access and use, including these: authorizing legislation that grants authority to an office or agency to lead cross-agency data sharing;<sup>3</sup> legislation specific to data use; policies or rules; executive orders mandating data sharing on a specific policy priority or population; and contracts, the focus of the final section of this resource. Common data sharing contracts include a Memorandum of Understanding, Data Sharing Agreement, Data Use License or Agreement, and Informed Consent. Additionally, judicial interpretation through case law, consent decrees, court orders, and administrative decisions can impact data access and use. As a result, consulting pertinent judicial interpretation can often clarify legal authority.

Examples of common legal authority:

- Executive order to require data sharing to address a specific policy priority  
*Example:* [State of Indiana, Executive Order 17-09](#) ; [State of Pennsylvania, Executive Order 2016-07](#)
- Authorizing legislation for agency or department that grants authority to an office or agency to lead cross-agency data sharing  
*Example:* Indiana Law, [IC 4-3-26](#), creates the Management Performance Hub, an executive agency charged with supporting cross-sector data integration of state agencies (note: the executive order was a precursor to the legislation); consolidation of Health & Human Services Agencies facilitates data sharing, e.g., [North Carolina Department of Health & Human Services \(NCDHHS legislation\)](#), [Rhode Island Executive Office of Health & Human Services \(RIEOHHS legislation\)](#)
- Legislation specific to data use  
*Example:* Massachusetts Law, [Chapter 55](#), permits analysis of administrative data to support policy decisions to end the opioid epidemic
- Policy or rule  
*Example:* NC rule, [10A NCAC 41A .0907](#), release required for communicable disease investigation
- Contracts  
*Example:* [State of Iowa, MOU for Early Childhood Integrated Data System](#) provides the framework for multi-body governance across participating agencies

---

<sup>3</sup> See [Zanti, Jenkins, Berkowitz, Hawn Nelson, Burnett, & Culhane \(2021\)](#).



Four federal statutes and regulations are most relevant to data sharing and integration: the Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), 42 CFR Part 2, and the Federal Education Rights and Privacy Act (FERPA). In addition, states have statutes, regulations, ordinances, orders, and rules that may exceed federal protections for administrative data sharing. For this reason, all relevant legal considerations, specifically authority, should be considered prior to developing a legal framework. For further examples of the basis for legal authority, refer to *Appendices A-E*.<sup>4</sup>

**Access**

Categorizing data can be helpful in thinking through legal implications of sharing and integration. The focus of this resource is to support data integration of restricted data, so it is important to distinguish between the three levels of access and understand how they differ.

Open Data	Restricted Data	Unavailable Data
Data that can be shared openly, either at the aggregate or individual level, based on state and federal law.	Data that can be shared, but only under specific circumstances with appropriate safeguards in place.	Data that cannot or should not be shared, because of legal restriction or another reason (e.g., data quality concerns).

Classifying high-value data assets of agencies and where they fit across these three levels of access is an important first step in determining the appropriate legal framework to support data integration in your context.

<sup>4</sup> For a discussion on Tribal authority, see [Tribal Emergency Preparedness Law](#) (2017, March)

**Positive Practice**

CT Public Act 19-153 mandated the creation of an annual report, [Legal Issues in Interagency Data Sharing](#) (2020), and the [CT Data Catalog](#), high-value data inventories produced by Connecticut executive branch agencies and compiled by the Office of Policy and Management, updated annually. This metadata includes clarity around data that are open, restricted, and unavailable, and around agency roles, including data owner and data steward.

Another way to think about classifying data access considerations is by data output. Legality of use depends on the purpose, how the data are released, and to whom. For example, releasing de-identified row-level data to a researcher for analysis can be permissible. So can releasing identifiable row-level data to a case worker for operational purposes. But these are two very different scenarios, and the legal agreements required depend upon the data output.

Data output	Explanation	Legal considerations	Security considerations
Row-level, identified dataset	Individual-level data that includes personally identifiable information (PII/PHI), e.g., names, addresses, case numbers, registration numbers, birthdates, diagnoses, and dates of service.	Highly protected. PHI relevant to HIPAA; PII relevant to FERPA. <sup>5</sup> May require DSA and/or DUL.	Significant.
Row-level, de-identified dataset	Individual-level data without PII/PHI. Dataset often includes demographic and programmatic information, with identifiers deleted.	Protected. Can be a “limited” dataset, with HIPAA-specific language for dataset that includes diagnoses and dates of service. May require a BAA or DUL.	Less significant, but data are still potentially reidentifiable, especially with merged datasets.
Aggregated	Aggregated data by specified subgroup/population/geography.	May require a DSA and/or DUL and commitment to not attempt reidentification.	Generally much less significant, but if data are aggregated by small geographies or small demographic groupings, they may be cross-tabbed to identify individuals, especially with merged datasets.

**Positive Practice**

Taking the time to design a clear Data Request Form, with potential data outputs, can provide clarity on legality of access and use; see, e.g., [NCDHHS Operational Data Request Form](#).

5 HIPAA and FERPA are discussed in detail in the section on [Federal and State Laws](#).

**Practice: Defining Access and Use to Determine Legality**

Ready to get started? Use the following prompts and examples as a guide to clearly define your data access and use, which then allows you to determine legality.

<p><b>WHY do you want to share and integrate data?</b></p> <p>For example, to:</p> <ul style="list-style-type: none"> <li>• Track indicators at the population level</li> <li>• Identify a target population</li> <li>• Describe cross-enrollment patterns</li> <li>• Identify geographic areas of greatest impact</li> <li>• Evaluate program outcomes</li> <li>• Improve services at the point of intervention</li> <li>• Conduct mandated reporting</li> </ul>	<p><b>WHO do you want to share it with, and who conducts the integration?</b></p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Executive leadership</li> <li>• Agency serving the same client</li> <li>• Probation officers</li> <li>• A community treatment provider</li> <li>• A hospital emergency department</li> <li>• A university-based researcher</li> <li>• An agency-based analyst</li> </ul>
<p><b>WHAT type of data do you want to share and integrate? Is it open, restricted, or unavailable?</b></p> <p>For example:</p> <ul style="list-style-type: none"> <li>• Information that does not identify individuals</li> <li>• Information that does identify individuals</li> <li>• Information that might identify a person</li> <li>• Health information</li> <li>• Educational records</li> <li>• Housing status</li> <li>• Demographics</li> </ul>	<p><b>HOW will you share the data?</b></p> <p>For example, provide:</p> <ul style="list-style-type: none"> <li>• Aggregate counts at the block group level</li> <li>• Credentialed access to source data</li> <li>• Access to public-facing dashboard</li> <li>• View-only access to data underlying a dashboard</li> <li>• Edit access to data underlying a dashboard</li> <li>• Row-level data with identifiers</li> <li>• Row-level data without identifiers</li> </ul>

The legality of these scenarios above is dependent upon the legal framework used to facilitate integration, and the particulars of the data access and use. For example, the sharing and use of even the most sensitive data, such as HIV status, is permissible if aggregated (i.e., combined) by a large geography (e.g., a state). Determining legality involves teasing out the specifics of the use, and supporting agencies in crafting a data request that fulfills their need for data to inform policy making, while adhering to important laws that protect individuals' privacy. It is also important to remember that the initial question of legality is the lowest bar of whether data should be accessed and used. The following sections offer additional guidance and practice questions to help you determine if data sharing is ethical and a good idea.

**Positive Practice**

Understanding the particulars of a request often starts with a Data Request Form. While not a legal document, a Data Request Form is an important part of a legal framework, as it can distinguish between uses (e.g., operational, audit, research) and provides specifics to determine legality. See this example from the [Hartford Data Collaborative](#).

► **Is this ethical?**

Ethics considers what is good for individuals and society, working to balance the rights of both. Ethical data use must ensure that data about individuals are protected, and that data are available to put knowledge into action to benefit society. The ethical foundation of human service data integration stems from the sometimes parallel and opposing principles that data is a public good and the right to privacy is intrinsic.

Research has a fraught history of inflicting harm, particularly on vulnerable and disenfranchised populations. This history—and current surveillance and research practices—is at the root of many ethical concerns around current data practices, including administrative data reuse. Best practices in human subjects research are based upon [The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research](#) (National Commission, 1979), which emphasizes three core principles.

<b>RESPECT FOR PERSONS</b>	<b>JUSTICE</b>	<b>BENEFICENCE</b>
<b>Privacy must be protected</b>	<b>Risks and benefits must be fairly distributed</b>	<b>Benefits must outweigh risks</b>

These principles are not hierarchical and must be equally considered even when they stand in opposition to one another. For example, because administrative data are collected for routine purposes and operational use, data use does not typically require consent. When reused for research, data are typically de-identified, which also does not require consent. This absence of consent is an important consideration for ethical use, and falls under “respect for persons,” as showing respect to a person is giving them the opportunity to choose how their data is used. Yet *not* using these data contradicts the concept of beneficence, as there are significant benefits and limited privacy risks (with appropriate security in place) to using data to inform policy making.

One common approach to balancing oppositional values is rigorous review, which is why **data governance** (covered more in a subsequent section) is central to this work. For researchers, administrative data reuse often requires human subjects research review, most commonly through an **Institutional Review Board** (IRB), a practice that is based upon recommendations from the Belmont Report.

To ensure ethical use—and discernment of respect, justice, and beneficence—legal agreements must operationalize data governance processes that sufficiently consider potential benefits and risks, and ensure that both have been weighed adequately by a variety of stakeholders. If done well, this ongoing collaborative process culminates in social license.

## Social License

Data sharing efforts must develop public approval—the “social license” to operate—in order to ensure ethical use and drive change. Social license comes from an effort’s perceived legitimacy, credibility, compliance with legal and privacy rules, and overall public trust. Earning it requires dedicating time and resources to develop relationships, source and incorporate feedback, and engage with diverse stakeholders on an ongoing basis. It is particularly important to build relationships and social license with Black, Indigenous, people of color, and other historically marginalized groups disproportionately harmed by government systems. Individuals represented “in” the data and frontline staff who support programs should be included in data governance structures and provided authentic opportunities for participation and decision-making. For a detailed discussion of these issues and examples of strategies for building social license with a racial equity lens, and a more nuanced discussion of risks and benefits, see our **Toolkit for Centering Racial Equity Throughout Data Integration**.<sup>6</sup>

Developing clear processes around discernment of potential benefits and risks is an important part of developing and maintaining social license. Perceived benefits and risks are dependent upon individual dimensions of identity, intersectionality, and membership of subgroups. Thorough discernment of benefit and risk requires a range of diverse perspectives. For example, a White woman with an advanced degree living by herself in a rural community may have a very different perspective on ethical administrative data reuse (often viewed as government surveillance) than a Latina, without formal schooling in the United States, living in a multigenerational household with a variety of immigration statuses, in an urban community that has significant Immigration and Customs Enforcement (I.C.E.) activity. Similarly, a case worker and an analyst working in the same agency will likely have different perspectives on data access and use. All perspectives are important, and care must be taken to consider differences in risks and benefits across dimensions of identity and lived experience.

---

6 See [Hawn Nelson, Jenkins, Zanti, Katz, Berkowitz, et al. \(2020\)](#).

## Weighing Legal Risks of Data Integration

Attorneys have ethical and common law duties to competently and reasonably advise their clients on legal risks. At times, legal risk can be difficult to quantify and manage. A key factor in mitigating the legal risks associated with data integration is identifying the potential enforcement and litigation risks to your organization. Data privacy rules such as HIPAA, FERPA, 42 CFR Part 2, and others do not authorize a private right of action for individuals to sue in the event of unauthorized use of data or a data breach.<sup>7</sup> While lawsuits brought by private parties alleging breach of privacy under state law do exist, in general (and particularly with federal laws), only government regulators enforce data privacy and security laws. They are principally looking to ensure that entities have the appropriate legal agreements in place and meet the minimum administrative, physical, and technical data security standards. The model legal agreements contained in this document are designed to help satisfy those legal requirements and mitigate litigation and enforcement risks. Enforcement actions generally focus on particularly egregious events or patterns and practices of behavior that clearly violate legal standards. In this context, a well-designed IDS with established governance practices, proper staffing, and engagement with key stakeholders are all risk mitigation strategies adaptable to state and federal requirements, and compliance-centered practices.

### Practice: Considering Risks and Benefits to Determine Ethical Use

There is a lot to balance when deciding whether and how to use data. Use the following prompts and examples as a guide to consider risks and benefits to determine ethical use.

- Why is this data sharing and integration being conducted? Are there other ways to answer this same question without the release of identifiable information?
- What are the risks of this data integration?
- What are the benefits of this data integration?
- Who will benefit from this data integration? In what ways?
- Who could be harmed from this data integration? In what ways?
- How are risks being mitigated?
- How will the data be shared to protect privacy and prevent redisclosure?

### ► Is this a good idea?

Reusing administrative data to support audit, evaluation, research, and evidence-based practice in public policy and programs is an important goal. However, there are many instances where reuse of data is legal and ethical but still may not be feasible or a good idea. Generally, three categories of considerations—data availability, resources, and action—should be carefully weighed through **data governance** to ensure data sharing is a good idea.

---

<sup>7</sup> See, e.g., *Abdale v. North Shore-Long Island Jewish Health System, Inc.*, 2:13-cv-01238 (E.D.N.Y. Aug. 14, 2015); *Dittman et al. v. The University of Pittsburgh Medical Center*, 196 A.3d 1036 (Pa. 2018); *Payne v. Taslimi*, 998 F.3d 648 (4th Cir. 2021) (holding that no private cause of action exists under HIPAA); *Gonzaga Univ. v. Doe*, 536 U.S. 273 (2002) (holding that no private cause of action exists under FERPA); *Doe v. Broderick*, 225 F.3d 440, 446-49 (4 Cir. 2000) (holding that no private cause of action exists under 42 CFR Part 2); but see *Lawson v. Halpern-Reiss*, 2019 VT 38 (VT 2019) (“we recognize a common-law private right of action for damages based on a medical provider’s unjustified disclosure to third persons of information obtained during treatment”).

## Data availability

Administrative data are collected not for analytic purposes, but rather for programmatic purposes. This means that at times, the actual data and the data quality are insufficient to answer a particular question. For example, if an agency is interested in evaluating racial disparities in program usage, yet the field for “race” is only complete for 30% of clients, then these data are not of sufficient quality for analytic use. Similarly, if the evaluation of a program is focused on household outcomes, yet information on siblings is not collected, then this specific question is not answerable using this data source.

## Resources

Strategic use of data takes resources—most notably, resources for salaries of highly trained (and therefore well compensated) staff. While using data to inform decision-making is often a return on investment, the reality is that resources for data efforts ultimately reduce resources for programmatic efforts. Discernment around the benefits and costs of data use—including use of resources—is essential, and achieved through **data governance**. This tension in relation to resource allotment can be significant, particularly in decisions about technology procurement, which are significant expenditures.

## Action

While possibilities for analytics are endless, many analytics are merely descriptions of problems we already know exist, and the analysis does not lead to productive action. There are countless reasons for inaction, so instead we ask you to focus on the most important question: **How will the findings from this data integration drive action that will improve the lives of residents?**

## Practice: This is legal and ethical. Is it a good idea?

Now that you’ve spent time determining legality and ethical use—an important first step—we also encourage larger considerations of the practicalities of data sharing and integration. Specifically:

- Are available data of sufficient quality to answer the question at hand?
- What action can be taken as a result of this analysis?
- How will programs/policies/lives be improved by this use of integrated data?
- What can reasonably be changed or improved based upon the findings? What cannot be changed?
- Has this question already been answered?
- Will the resources needed to conduct this integration yield more benefit than using these same resources for programmatic or direct funding?
- What is the sociopolitical context of this data integration? Is this building upon previous work? Is this work supplanting previous efforts? Is there a related effort that “went wrong” or needs to be acknowledged in some way?
- What are the political implications of this data use?
- Who is conducting this integration and analysis? Do they have sufficient understanding of the program/policy/population that is being studied?
- Who is “asking” the question? Is this topic of interest to the broader community? Do community members, including those “in” the data, know about and support this work?

## ► How do we know? Who decides?

Determining whether something is legal, ethical, and a good idea is not always a simple task, and requires a variety of diverse perspectives, with clarity around decision-making authority. This is achieved through data governance.

### Data Governance

#### Data governance

The people, policies, and procedures that support how data are managed, used, and protected.

Data governance for a cross-sector data sharing effort can draw upon existing data governance practices within one agency, involve a separate set of policies and procedures, or be a hybrid of the two. Specific policies and procedures will vary widely based on the purpose, vision, mission, and guiding principles for data sharing established by the data partners involved. An ad hoc data integration project to generate indicators and routine reporting will require one governance approach, which will differ significantly from data governance needed to create access to routine real-time integrated data for credentialed users to support operations and service delivery. We recommend that a site devote time up front both internally and with partner organizations to build consensus around what data sharing and integration is intended to achieve. Taking the time to do this at the outset allows each site to establish tailored rules of engagement that best meet its needs and goals.

Data governance for ongoing data sharing and integration should include clearly defined policies and processes to support decision-making, routine meeting structures, and well-documented proceedings—**all fostering a culture of trust, collaboration, and openness.**

Strong and inclusive data governance for cross-sector data sharing and integration should be:

- Purpose-, value-, and principle-driven
- Strategically located
- Collaborative
- Iterative
- Transparent

**Purpose-, value-, and principle-driven**

We encourage sites to first identify the purpose for sharing, and then develop vision, mission, and guiding principles. These should include clear value statements around mutual benefit for data partners and the broader community. The following table outlines common purposes for sharing and some key considerations that illustrate how purpose will inform the overall approach and the most appropriate legal framework for integration:

**Core Purposes and Approaches for Data Sharing and Integration**

Purpose	Indicators and Reporting	Analytics, Research, and Evaluation	Operations and Service Delivery
<b>Approach</b>	Data can be summarized and reported at the aggregate	Data must be curated, shared, linked, and then de-identified for statistical purposes	Data must be identifiable and may include case notes to support client-level services
<b>Legal Framework</b>	Data may be publicly available already or may require a simple Data Use License to receive in de-identified format	Data access will generally require multiple agreements, including a Memorandum of Understanding, Data Sharing Agreement, and Data Use License to clearly outline permissible access and use	Data access may require client consent and non-disclosure agreements. Data agreements must outline parameters for role-based, credentialed access
<b>Data Frequency</b>	Data may be updated based on reporting cycles, quarterly or annually	Archive of select data may be updated periodically depending on availability and analytic requirements	Daily or real-time updates of entire client records may be required
<b>Privacy and Security</b>	A lack of identifiers or small cell sizes means minimal risk of redisclosure	Minimal access to identifiable data and a small group of approved users means that security requirements are essential but basic	Many users and identifiable data means that complex permissions and an audit trail will be necessary
<b>Governance</b>	Minimal	Clear parameters around access and use are required, shared processes involving all agencies	
<b>Example sites</b>	Members of the <a href="#">National Neighborhood Indicators Partnership</a>	<a href="#">Iowa’s Integrated Data System for Decision-Making (I2D2)</a>  <a href="#">Charlotte-Mecklenburg, Institute for Social Capital, UNC Charlotte</a>	<a href="#">Allegheny County Data Warehouse</a>  <a href="#">South Carolina Integrated Data System</a>

## Strategically located

Before determining the optimal organizational roles and legal framework for data sharing and integration in your context, it is helpful to consider two major functions of data governance:

- a. Stakeholder engagement and procedural oversight: Relationship management, convenings, developing policies and procedures, communications, agenda setting, etc.
- b. Data management and integration: Secure data transfer, storage, linking, and access for analysis, etc.

Which partner or partners are best positioned to conduct these two functions will depend on a range of factors, including legal authority to use the data as intended by the identified purpose, perceived neutrality among data partners, staff capacity, and technical capacity for data management. In our experience, it is worth the time and effort to consider these practical and strategic questions early on, which can help avoid major stumbling blocks later in executing agreements and allowing data to flow.

**Privacy preserving technologies (PPTs)** [also referred to as privacy-enhancing technologies (PETs)] are technical approaches that minimize use of and need for personal data, including identifiers, while supporting record linkage through privacy techniques, e.g., homomorphic encryption, trusted enclaves, differential privacy, and secure multi-party computation. There is a wide range of time-tested and emergent technologies. Use of PPTs can decrease the privacy risks of data sharing, and may reduce the need for extensive legal agreements as a result of limited access to individual-level data and the increase in privacy and security protections. PPTs are a growing field, and while they are important technical approaches for safeguarding information, they offer the most support when layered with other forms of data privacy and security measures, including a strong legal framework. We do see PPTs as important in balancing the tension between data utility and privacy concerns, e.g., as shown, for example, in the case of [Spotlight Tulsa](#).

## Management Model

Once the core purpose of the data integration effort is defined, it is helpful to consider what partners will manage the three core activities of data integration:

1. Hosting governance (including stakeholder engagement and procedural oversight)
2. Managing technology (including data storage, integration, and access)
3. Conducting analysis (including research methods, tools, and insights)

While many data integration efforts have one agency that manages the governance, technical approach, and analytics, many other efforts, especially those early in development, divide duties. For example, one partner manages governance, another manages technical integration, and another leads on analytics.

Across these different arrangements, we observe four main management models:

- Executive-led (e.g., mayoral office, state Office of Budget and Management)
- Agency-led (e.g., Health and Human Services, Department of Education)
- University-public partnership
- Nonprofit-led

While each model has distinct advantages and challenges, they are beyond the scope of this resource. Please see [IDS Governance: Setting Up for Ethical and Effective Use](#) (2017) for a more nuanced discussion.

**Why this matters:** The management model can dictate and inform the legal framework for data access and use, specifically the legal authority. For example, an IDS that is situated within a health and human service agency will have clear legal authority for data integration across a number of programs (e.g., [public health authority](#)), and in some cases may exchange data without a contract. In contrast, in a nonprofit-led model, governance is managed by a nonprofit agency or backbone organization (e.g., United Way). In this arrangement, contracts are the only legal authority, and extra care must be taken to ensure that data governance and data security are sufficient. Data Use Licenses (DULs) will be an important mechanism to facilitate access to agency-held administrative data.

### Collaborative

Data governance is inherently people-driven and should be developed cooperatively, with a focus on building trust and strong relationships among the partnering organizations. In practice, this may require multiple layers of engagement. Many successful sites have at least three groups that support governance functions:

- a. **Deciders:** Executive leader group that supports strategic decision-making
- b. **Approvers:** Data subcommittee that supports review and oversight
- c. **Doers:** Staff who are charged with daily operations

Both decider and approver groups should be representative of agency data partners. It is important to outline duties of the two groups of people—data integration staff and agency data partners—that will be largely tasked with facilitating strong data governance. Specific tasks of these groups are commonly memorialized within legal agreements.

### Data Integration Staff

In our experience, staffing is the essential element of an effective data integration effort. Staff are the “doers,” who carry out daily operations while informing and implementing strategy. Where there is a strong legal framework, clear data governance, and effective use of data for policy making, there are highly effective and consistent staff that function as a team.

Within legal agreements, “data integration staff” typically refers to individuals who manage data governance and data management and who conduct analytics. Staff should include people with diverse training and lived experiences, with a variety of identity dimensions and competencies to support both the relational and technical aspects of data sharing. We recommend hiring staff with programmatic and policy experience and with a variety of academic and on-the-job training. Staff diversity supports ethical use. If the data integration effort is staffed appropriately, the initial considerations—is this legal, ethical, and a good idea—will often be taken into account, and obvious issues will be addressed by staff prior to being considered with a broader group of stakeholders.

Data flows at the speed of trust, and the work of data integration is relational, technical, and long term. Efforts must be resourced and staffed appropriately.

Staff manage all data governance processes and procedures, facilitate stakeholder engagement, and serve as the front line in evaluating considerations of a data request that are essential for mitigating risk, including data privacy, data security, and de-identification and anonymization. A primary role of staff is to interact with the data integration partners, who fulfill different roles for the data integration effort.

**Agency Data Partners**

All agencies make decisions about their data assets. Data management decisions are often made by data custodians, who are responsible for the technology used to store, transport, and secure data, rather than for the strategic use of data. While data custodians are essential to the work of data sharing and integration, a variety of agency roles—most importantly, data stewards and data owners—should be involved in decision-making for cross-sector data efforts.

When thinking through data integration use that is legal, ethical, and a good idea, it is important to include all three roles in the discussion, as they will have different perspectives on benefits, limitations, and risks. For example, data owners often have nuanced understanding of political considerations, and data stewards are charged with generating valuable metadata and documenting bias and data quality concerns, while data custodians have detailed understanding of security protocols.

***The Role of Data Owners, Data Stewards, and Data Custodians***

	Role in data sharing and integration process	Role within agency
<b>Data Owner</b>	Accountable for the quality and security of the data and holds decision-making authority over access and use.	Typically agency leadership that has signatory authority
<b>Data Steward</b>	Responsible for the governance of data, including transfer, alteration, storage, retention, disposition, classification, etc. Includes supporting established processes and policies for access and use, documenting limitations and bias, and maintaining metadata.	Typically subject matter experts and data analysts that regularly work with specific data
<b>Data Custodian</b>	Responsible for the technology used to store, transport, and dispose of data, and for activities and safeguards required to maintain confidentiality, integrity, and availability. Communicates with Steward and Owner regarding any data management issues that pose a risk to data security and/or access.	Typically information technology staff or team

**Iterative**

Data governance should be an iterative process that guides the whole project life cycle and is revisited and honed regularly as your data sharing effort evolves. All processes and procedures are living documents and should be refined for continuous process improvement.

## Transparent

Most integration efforts are largely funded with taxpayer dollars. For that reason, transparency around what data are being shared and for what purpose is essential to creating accountability. Demonstrating and communicating the value of integrated data to diverse stakeholders also builds social license. Policies, protocols, and documentation of the data integration effort—as well as any specific projects the effort is engaged in—should be readily available to the public in understandable and accessible formats.

### Positive Practice

Here are some examples of AISP Network Sites with publicly available data governance information: [Linked Information Network of Colorado](#); [Hartford Data Collaborative](#); [Iowa’s Integrated Data System for Decision-Making \(I2D2\)](#); and [Connecticut Office of Policy & Management / P20 Win](#).

## Practice: Considering the Four Questions

In previous sections, we offered practice questions to help you discern if data integration is legal, ethical, and a good idea. Now let’s practice considering who should decide and how they will contribute to data governance.

For discussion: Are these examples of data integration legal, ethical, a good idea? And how do you know? Who should decide?

Example 1:	
An agency is interested in designing a programmatic intervention for families experiencing food insecurity and wants to integrate longitudinal (2011-2021) TANF involvement + receipt of free/reduced lunch (FRL) (2011-2021) + receipt of Pandemic EBT (2020-2021).	
Context:	As a result of the Healthy, Hunger-Free Kids Act of 2010, and implementation of the Community Eligibility Provision (CEP) in 2014, individual-level data on FRL is no longer collected.
Considerations:	<p><u>Legal</u>: This data sharing is determined to be legal.</p> <p><u>Ethical</u>: Family receives immediate benefit through cash assistance.</p> <p><u>Good idea</u>: Data availability challenges (no individual-level FRL data) prevent integration at individual level connecting FRL. Some states and districts decided to grant Pandemic EBT to all students in an eligible school (based on CEP), rather than relying on individual FRL. While individual data sharing is legal and ethical, the originally planned integration is not feasible, so a pivot is necessary.</p>

**Example 2:**

A local education agency is interested in better understanding the connection between attendance, transportation, involvement in an after school enrichment program (ASEP), and academic achievement as demonstrated by standardized tests.

Context:	The data system that includes attendance and achievement data is not connected to the system that manages transportation. The transportation data is managed by a private data management firm, and extracting the data comes with significant cost. The ASEP program only collected age, rather than date of birth, so records cannot be linked by birthdate.
Considerations:	<p><u>Legal:</u> Some ASEP programs are nonprofit organizations, and these data are considered private data, so individual-level consent may be needed.</p> <p><u>Ethical:</u> Immediate benefit to student and family is not clear. Informed consent for use of ASEP data is not in place.</p> <p><u>Good idea:</u> Data integration may not be possible at this time, particularly for ASEP program. Suggestion to plan for this analysis in the future by changing registration form to include DOB (rather than age) and build optional consent into ASEP program enrollment process for next school year.</p>

**Example 3:**

A Department of Health is interested in conducting a large community-wide engagement project to collaboratively design public health indicators, using integrated two-generation data on children and their families. These would be shared via an externally facing dashboard, with the goal to improve service interventions of community-based organizations.

Context:	This agency has experienced 40% turnover in the past 6 months. The governor's race is contentious, and the health commissioner is politically appointed.
Considerations:	<p><u>Legal:</u> Yes, these data will be aggregated according to agreed upon guidelines.</p> <p><u>Ethical:</u> Based on involvement of community health clinics and community partners, these data are actionable and will serve as a support to community-based organizations working in partnership with the Department of Health.</p> <p><u>Good idea:</u> This project was a high priority for the previous commissioner, and is named after the commissioner. It is unclear whether the administrative and technical processes are feasible because of staff turnover within the department, and it is likely that if the governor is not reelected, the project will be abandoned.</p>

**Example 4:**

A philanthropic partner is interested in the causal impact of housing instability for preschool age children. They have asked the local integrated data system to create a list of families who are housing unstable, as indicated by a shelter stay in the previous 18 months, identification as McKinney-Vento within their educational record (through PreK student or sibling), and/or application for a housing voucher in the previous 24 months. They are requesting a list of individuals for a control and intervention group. The philanthropic partner wants to conduct a randomized control trial, evaluating the impact of providing a significant housing subsidy for 20 families.

Context:	The local housing authority and family shelter are unwilling to partner with this philanthropic partner because of previous contractual issues. It is unclear who would administer the housing subsidy. Involved researchers have communicated to the philanthropic partner that a large body of research has consistently demonstrated that housing subsidies are effective for improving educational outcomes. They are resistant to eliminating the research component of the project. Informed consent is in place for use of identifiable data for service provision, but not research.
Considerations:	<p><u>Legal:</u> Appropriate legal authority is in place for operational use (identification of families for subsidy), but not for research purposes.</p> <p><u>Ethical:</u> Families will receive a housing subsidy through random assignment. The cost of the randomized control trial research could fund 20 subsidies.</p> <p><u>Good idea:</u> If the housing subsidy is available, and families are identified for receipt, there is no organization available to administer the support.</p>

**Example 5:**

A task force on violence prevention, convened by the mayor, wants to generate a report on the state of racial disparities in the city, with a focus on social determinants of health.

Context:	There have been two reports created, using the same data sources, on related topics in the previous 2 years. All reports show the same general trends and disparities. Neither report included clear recommendations for action.
Considerations:	<p><u>Legal:</u> Data use agreements are in place.</p> <p><u>Ethical:</u> Unlike previous iterations, this task force will pay participants.</p> <p><u>Good idea:</u> The convener of this work is committed to collaboratively generating recommendations for action, with concrete goals for a variety of sectors.</p>

**Example 6:**

A Health and Human Services agency is interested in vaccination status of individuals who are experiencing homelessness and receiving Medicaid in order to better understand rates of vaccination and usage of medical services. They plan to use Medicaid records and a list of individuals within the homelessness management information system (HMIS) from the past 6 months, and vaccination records from 2021-current. Integration will be conducted by the centralized IT for the agency, and a by name list will be created of individuals who are experiencing homelessness + unvaccinated + receiving Medicaid. This list of names will be given to a case worker within the statewide homeless service agency to support local agencies in incentivizing vaccination for these individuals. This same integration will occur every 6 months to determine if outreach efforts are successful (as measured by the number of names on the list that remain the same over time).

Context:	The agency is authorized through General Statute to “provide the necessary management, development of policy, and establishment and enforcement of standards for the provisions of services . . . to assist all citizens . . . to achieve and maintain an adequate level of health, social and economic well-being, and dignity.”
Considerations:	<p><u>Legal:</u> Layers of legal authority are in place, including authorizing legislation, DSA, DUL, and consent for HMIS involved persons.</p> <p><u>Ethical:</u> In this state, death rates of unvaccinated individuals are 20% higher than those of vaccinated individuals.</p> <p><u>Good idea:</u> This HHS agency has a long track record of strong community involvement and enduring relationships with homeless service providers.</p>

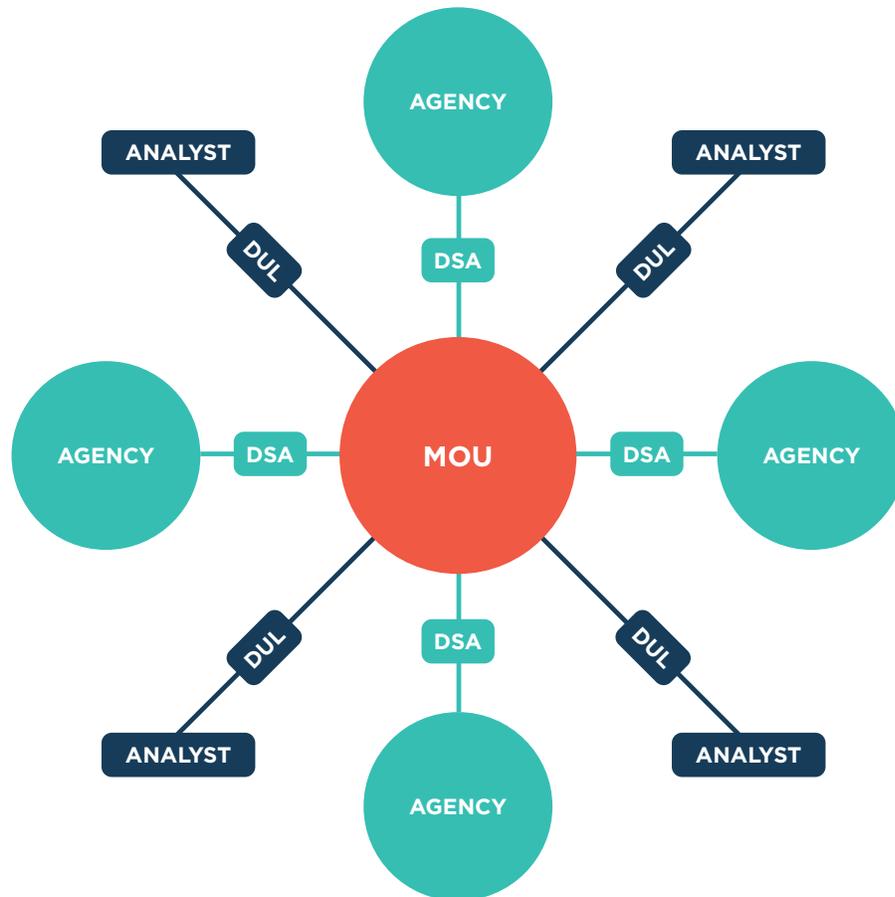
## ❖ How: Drafting the Legal Agreements

Now is the time to pull together all the thinking that you have done around data integration purpose, management model, stakeholders, context, authority, and parties, and begin to consider what legal agreements will be needed for your data integration effort.

Having explicit conversations about data privacy, and memorializing decisions within legal agreements are both important. **Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems** is a helpful resource to guide these discussions, and provides principles, concrete steps, and materials to support engagement practices that can be adapted to your local organizational culture.

### ► Tiered

We recommend a three-tier approach for legal agreements to govern data access and use for integrated data: a Memorandum of Understanding (MOU), Data Sharing Agreement (DSA), and a Data Use License (DUL). Other agreements may also be needed, such as confidentiality or nondisclosure agreements for individual staff. Agencies may use different terms to refer to these documents, including data security agreement, information sharing plan, memorandum of agreement, data sharing agreement, data exchange agreement, and data use agreement. It is helpful to learn the terminology used by the agencies you hope to partner with and to use this terminology consistently.



FOUNDATIONAL LEGAL AGREEMENTS			
LEGAL AGREEMENT	PURPOSE	PROCESS	SIGNATORY
<p><b>Memorandum of Understanding MOU</b></p> <p><i>Overarching process document signed on by all data partners</i></p>	<p>The MOU documents the purpose and governance process. The MOU will be signed by all data partners as they enter the collaboration. The MOU references the DSA, DUL, and relevant policies, and procedures for data access and use.</p>	<p>Drafted in partnership with legal counsel from all participating data partners</p>	<p>Lead agency/ies + all data partners</p>
<p><b>Data Sharing Agreement DSA</b></p> <p><i>Agency-specific to how data will be used for integration</i></p>	<p>The DSA includes the specific terms and conditions that govern how data are transferred, stored, and managed when shared and integrated. The DSA references the MOU and the DUL. This document is specific to data held by a data partner.</p>	<p>Template is drafted in partnership with legal counsel from all participating data partners. Completed according to specific data assets of the data partner. Reviewed and updated annually, or as agreed upon.</p>	<p>Lead agency/ies + data partner</p>
<p><b>Data Use License DUL</b></p> <p><i>Data use-specific once data has been integrated</i></p>	<p>The DUL outlines the role and responsibilities of the data recipient. The DUL is often executed after the Data Request Form is approved. The Request Form and/or DUL should include: purpose, data fields, anonymization procedures, dissemination plan, and timeline of project completion. A DUL must be executed prior to data access.</p>	<p>Template is drafted in partnership with legal counsel from all participating data partners.</p> <p>Once data request is approved, a DUL is executed.</p>	<p>Lead agency/ies + data recipient</p>

► **Standardized but Flexible**

Individual agencies and organizations can operate with hundreds of data sharing agreements, each with different names, terms, structures, and signatories. Coming to agreement on a standard legal framework, particularly legal agreements, is challenging but essential. Standardizing terms and conditions of access and use can improve workflow, support insights, and reduce costs.

We recommend starting with a review of the agreements already used in your jurisdiction before selecting exemplars to template and use routinely across agencies. While this process requires an investment of time up front, it should make each subsequent negotiation faster and more predictable.

Using standard but modular documents can also increase the flexibility of legal agreements. Defining terms can be a complex exercise within one large institution. Collaboratively defining terms across a range of government, nonprofit, and academic institutions? We encourage you to allot adequate time to complete this important part of the legal framework.

Terms should be clearly defined and used consistently throughout the interrelated agreements and process documents. Most often, terms are defined within the MOU, and either included in each related legal agreement (e.g., the DSA and DUL) or in some cases separated out into a separate terms document. These terms are defined in a following section, [Common Definitions](#).

### ▶ **Transparent and Comprehensible**

Legal agreements—in particular those operating at higher levels of the tiered structure, such as the MOU—should be written so that non-lawyers can follow along. We recommend the use of appendices to separate out things like security requirements and data elements from the main text of agreements. In addition, if legal agreements themselves, or at least the existence of the agreements, can be made public, this can help establish trust with the public and earn social license for data sharing.

### ▶ **Memorandum of Understanding (MOU)**

The MOU is a foundational agreement among the parties. The MOU sets forth the core features of the management model (i.e., what agency fulfills the functions of governance, data management and integration, and analytics) as well as the legal rights and responsibilities of each party involved. A good MOU will codify both the legal requirements and operational structure. An MOU should be written in plain language so that anyone can understand its terms. It should also memorialize the mission, values, and ethical framework of the data sharing effort. This is sometimes called an enterprise MOU or interdepartmental MOU.

The MOU is the foundational agreement among the lead IDS agency and the data partners. Some jurisdictions may use other terms, such as data sharing agreement, to refer to the legal agreement between the lead IDS agency and the data partners. The specific name does not change the substantive terms required in the agreement.

In [Appendices E](#) and [F](#), we provide an MOU Inventory, Annotated Draft MOU, and examples of MOUs from IDS from across the United States.

The IDS lead agency can have separate MOUs with each data partner or can craft a single MOU that all data partners sign (we recommend the latter). For example, South Carolina has an MOU template that it uses with each data partner and modifies depending on the type of data. Connecticut has developed an enterprise MOU that all data partners enter (see [P20 Win EMOU](#)). In either case, it is important to include a mechanism to add parties and amend the MOU to accommodate growth in both size and scope of the IDS. This can be accomplished through the use of a joinder agreement (see [LINC MOU](#)).

There is no required structure for an MOU, and agencies may have existing templates or structures they want to deploy. We have developed an MOU checklist that includes provisions that should be part of any IDS MOU; see [Appendix E](#). The goal of the MOU is to outline the purpose, management model, stakeholders, and governance framework that will allow data integration to comply with all applicable local, state, and federal laws.

The variability of MOUs can be traced to legal and organizational culture. Some cultures prefer longer and more detailed agreements; others prefer more compact and flexible documents. Still others do not use legal agreements frequently. For example, Allegheny County does not require legal agreements for data sharing among county agencies (e.g., Health and Human Services) because the county is a single legal entity and does not need to contract with itself. They do utilize an MOU for data sharing with agencies outside the county.

## ► Data Sharing Agreement (DSA)

While the MOU is a broad document that names the purpose, partners, and guiding principles of a data integration effort, the DSA includes the specific terms and conditions that govern how specific data are transferred, stored, and managed when shared and integrated within the IDS. The DSA is a technical document that references the MOU and the DUL, memorializing contractual obligations of the data owner and the IDS. This agreement is specific to the data owner, not the overall purposes of the IDS. For example, an IDS with 10 data partners would likely have one MOU and 10 DSAs. The parties to the DSA are the IDS and the data partner (which owns the data).

The creation of an IDS requires the sharing of personally identifiable information (PII) at the individual level to enable the correct matching of data at the person level. Most state and federal laws permit the sharing of PII for evaluation, audit, and research purposes. The DSA template is written to be flexible to accommodate data sources that are subject to multiple state and federal data privacy laws and regulations, including the Privacy Act (1974), HIPAA, 42 CFR Part 2, and FERPA. The following section, [Federal and State Laws](#), discusses each of these major data privacy regimes and some unique requirements and considerations that may apply.

A DSA often contains many of the same standard contract provisions, including those related to the legal use and protection of confidential data, as the MOU. Ideally, the DSA should include specific parameters for data access and use, and specificity about when these data are open, restricted, or unavailable (e.g., due to statute). The DSA is also an ideal place to identify approved uses of data based upon collaboratively created inquiry and research agendas. [Appendices G](#) and [H](#) provide a DSA Checklist and annotated template that sets forth model language and explanation for each section of the DSA.

## ► Data Use License (DUL)

The DUL sets forth the terms and conditions under which an analyst, researcher, evaluator, or other outside party (“data licensee”) may gain access to data from the IDS for a specific purpose. The parties to the DUL are the IDS and the data licensee.

While these agreements can be called Data Use Agreements (DUAs), we refer to them as Data Use Licenses (DULs). Like other licenses, a DUL is time-bound and revocable. Specifically, the language of license emphasizes the limited nature of the data licensee’s rights to the data. **A DUL grants a data licensee the temporary right to use a limited set of data for a specific purpose under certain conditions.** The data licensee does not gain any ownership interest in the underlying data and is limited by the DUL in terms of data use, sharing of data, and practices such as privacy protections and restrictions on de-identification.

The DUL contains provisions regarding the terms of the license itself (e.g., the specific data elements, the duration of the license, the handling of the data set). In [Appendices I](#) and [J](#), we provide a DUL checklist, template, and examples.

The DUL may vary depending on the type of data licensee and the specific use of the data (e.g., evaluation, research, audit). Data licensees who are performing “research” within the meaning of the Common Rule<sup>8</sup> will be subject to the review of an Institutional Review Board. An IDS may elect to provide the data licensee a de-identified or limited data set<sup>9</sup> in order to limit the release of PII/PHI and reduce the risk that an individual can be identified.

---

<sup>8</sup> See 45 CFR 46.114 (b).

<sup>9</sup> A “limited data set” is a limited set of identifiable patient information that excludes certain direct identifiers of a patient (like names, addresses, and social security numbers). Under the HIPAA Privacy Rule, covered entities can share a “limited data set” with entities that have signed a data use agreement with the covered entity. See 45 CFR Part 164.

## ▶ Consent

Whether consent is needed to share or integrate data largely depends upon the type of data, who is accessing the data, and how the data will be used. Depending on the jurisdiction, there may also be restricted data that can only be accessed with consent (e.g., juvenile records in North Carolina, N.C.G.S. 7B-3001(b)). There are many considerations, and often no clear answer. We strongly recommend that any decisions around consent be carefully considered with a variety of stakeholders through data governance processes. In general, consent is not usually required for research, evaluation, and planning efforts using public data, where individual identifiers will not be seen or used by analysts. This is not the case for private data, such as data from community-based organizations.

We recommend the following resources to deepen your thinking around this important and developing topic:

- [Data Across Sectors of Health, Data Sharing and the Law, Deep Dive on Consent, 2018](#)
- [World Economic Forum, Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction, 2020](#)
- [Office of the National Coordinator for Health Information Technology, Meaningful Consent Overview, 2018](#)

## ▶ Practice: Evaluating Your Legal Agreements

Ready to get started drafting your legal agreements? Consider the following questions before you take off:

### Context

- How are data currently accessed and used?
- What is the culture (shared, learned behavior) of data sharing and integration?
- What is the history of data sharing and integration in this context?
- What legal tools and/or agreements have been used in the past to facilitate data sharing and integration? Successful? Unsuccessful? Why?
- Are there existing contracts (ad hoc or routine) that do a good job of safeguarding data while allowing data to be accessed and used?
- Is there an inventory or list of current and past data sharing agreements in place with proposed data owners? How often are agreements renegotiated or amended?

### Parties

- What is the purpose of this data integration effort?
- Who are the essential data partners to this effort? Who owns the data that is needed to answer essential questions?
- Who is the lead agency/ies?
- Who is managing governance?
- Who is managing technical processes (i.e., data transfer, security, cleaning, entity management, integration, de-identification)?
- Who conducts analytics?

## Legal Authority

- What is the legal authority of the data integration effort (e.g., authorizing statute, Executive Order, legislation, Data Sharing Agreement)?
- What state, federal laws, and orders apply to the data?
- What type of legal entity is your organization—a health provider, a local educational agency, a city? The type of entity might dictate the type of data held and if the law applies to that type of entity (e.g., HIPAA only applies to health plans and providers, not to schools).
- What type of data is being shared—health (PHI), educational (PII), personally identifiable?
- Does the law limit the disclosure of this data? If de-identified, in some cases, there are no limits.
- If there are limits on disclosure, are they mandatory or permissive? Are there any exceptions (e.g., school official exception, business associate exception).
- Which party will be liable for security, disclosures, liability assurance/insurance?

Use the following questions to evaluate your legal agreements:

## Tiered

- If there are existing templates/model agreements, how do these documents work together?

## Standardized but Flexible

- If there are existing templates/model agreements, are they modular or malleable to potential project-specific needs?

## Transparent and Comprehensible

- How accessible is the language, length, and organization of legal agreements?
- Can non-lawyers understand the content?
- Are the agreements publicly available?

These questions offer helpful context and highlight key considerations when identifying and drafting the legal agreements. Once you have determined the appropriate legal framework to use and have begun identifying relevant legal considerations for data access and use, it is important to consider what state and federal laws are implicated.

## ❖ How: Site Examples

*The previous sections of this report are designed to be applicable to a variety of international contexts. The following sections are specific to the U.S. legal context.*

Hesitation to work toward cross-sector data integration often stems from fears that this is uncharted territory. Yet numerous, highly functioning integrated data systems exist, several of which were established decades ago. How did they do it?

This is charted territory; learn from others who have a strong legal framework, data governance, and routine data access and use. See the AISP Network Site Map at [www.aisp.upenn.edu](http://www.aisp.upenn.edu) to explore existing efforts.

Government leaders of all political affiliations have embraced and encouraged the expansion of IDS to facilitate more effective and efficient government. In 2016, U.S. House Speaker Paul Ryan and Senator Patty Murphy drafted the Evidence-Based Policymaking Commission Act of 2016 (HR. 1831), which passed with bipartisan support and was signed by President Obama. The explicit goal of the Commission was to “focus on the most basic prerequisite for evidence-based policy: good data.”<sup>10</sup>

Administrative data reuse to inform policy and practice has become a stated priority at every level of government in the United States.<sup>11</sup>

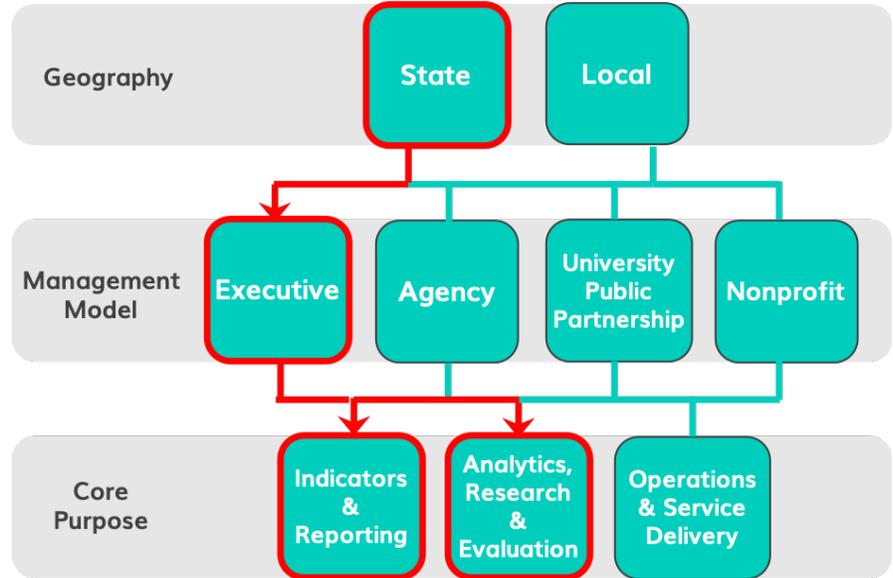
Below, we have provided summaries of selected IDS across the AISP Network. We find it helpful to categorize sites across three main categories: geography, management model, and purpose. We have also included the lead agency/ies, core data partners, and legal authority used for each site.

<sup>10</sup> See [Commission on Evidence-Based Policymaking \(2017, September\)](#).

<sup>11</sup> United States, Executive Office of the President, [Executive Order on Ensuring a Lawful and Accurate Enumeration and Apportionment Pursuant to the Decennial Census](#) [Biden, 2021], Revoking Executive Order on Collecting Information about Citizenship Status in Connection with the Decennial Census [Trump, 2019]; [State Data Sharing Initiative Toolkit](#) (2018); National Association of Counties (2018); [Smart Cities Council of North America](#) (2017, April 13).

## Indiana Management Performance Hub (MPH) Executive, State

The Indiana Management Performance Hub (MPH) is a standalone state agency that governs the enterprise-level integrated data system and drives evidence-based decision making across Indiana. MPH was made possible through a 2014 executive order with the collaboration of the state's Office of Management and Budget and Office of Technology.



► [Learn more about MPH here.](#)

**Lead Agency:** Indiana Management Performance Hub

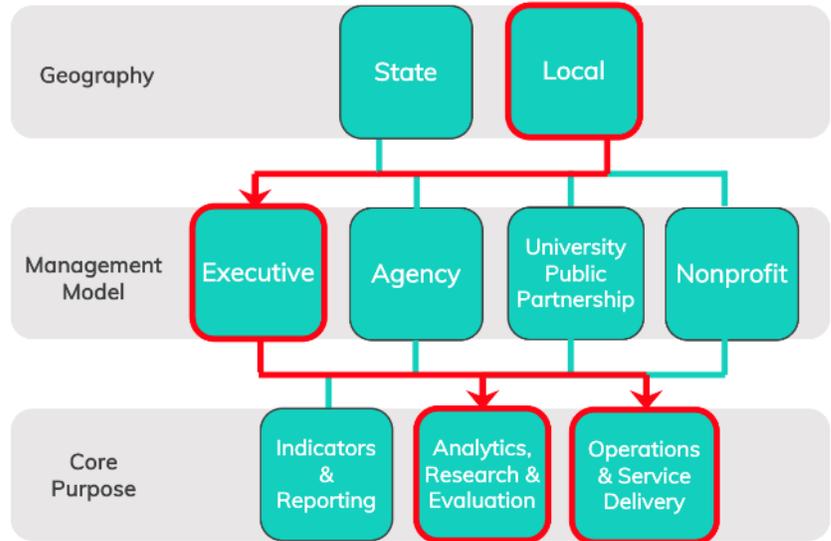
**Data Partners:** [All state agencies](#)

**Legal Authority:** [Executive Order](#), [Authorizing Legislation](#), contracts

**Funding:** Federal, state, fee for service

### NYC Center for Innovation in Data Intelligence (CIDI) Executive, Local

NYC's Center for Innovation in Data Intelligence (CIDI) is housed in Office of the Mayor of the City where they primarily perform policy research and evaluations.



► [Learn more about CIDI here.](#)

**Lead Agency:** Mayor's Office of New York City

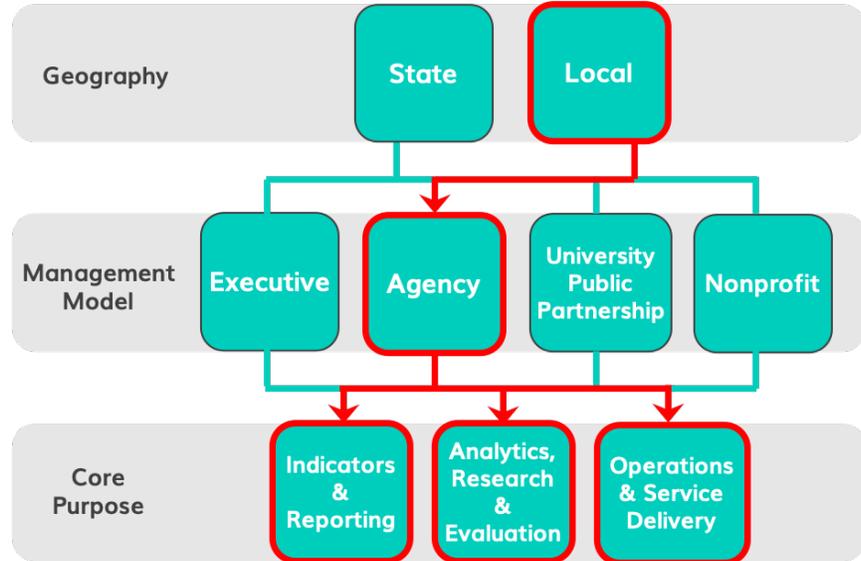
**Data Partners:** [City agencies and service providers](#)

**Legal Authority:** [Executive Order](#), contracts

**Funding:** Federal, state, local, fee for service, philanthropic partners

## Allegheny County Data Warehouse Agency, Local

The Allegheny County Data Warehouse is hosted by the County's Department of Human Services, Office of Analytics, Technology and Planning. Data integration capacity drives research and evaluation across key social policy domain areas as well as service delivery and operations for child welfare.



► [Learn more about Allegheny County here.](#)

**Lead Agency:** Department of Human Services

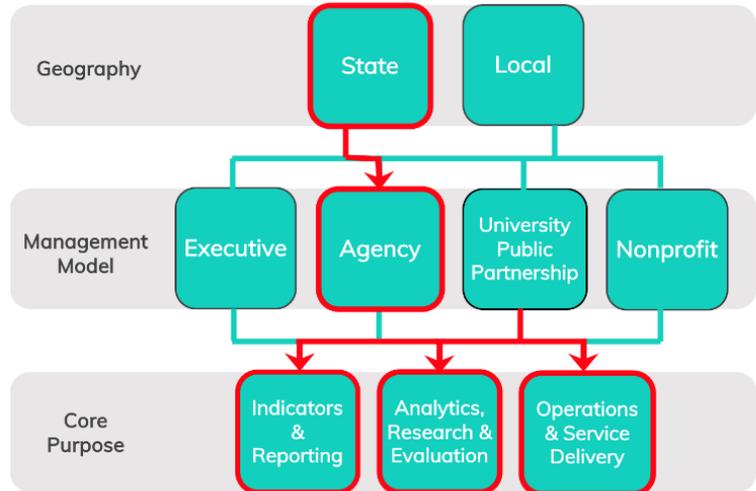
**Data Partners:** Allegheny County's Department of Human Services, Health Department, Medical Examiner, Housing Authority, and Jail; the Fifth Judicial District of Common Pleas, Pittsburgh Police Department, UPMC Health Plan, Pennsylvania Department of Labor and Industry, Pennsylvania Department of Human Services, Housing Authority of the City of Pittsburgh, Community College of Allegheny County, and School Districts—Pittsburgh, Clairton, Woodland Hills, Penn Hills, Sto-Rox, Elizabeth Forward, Duquesne, McKeesport, South Allegheny, Cornell, Steel Valley, West Mifflin, North Hills, Moon, Baldwin-Whitehall, and Propel Charter Schools

**Legal Authority:** Authorizing statute, contracts (e.g., [Data Sharing Confidentiality Agreement](#))

**Funding:** Federal, state, local, fee for service, philanthropic partners

### Rhode Island EOHHS State, Agency

The Rhode Island Ecosystem is using integrated data to improve agency performance and operational analytics, quality improvement, and data-informed decision making among EOHHS and partner Rhode Island agencies. The Ecosystem, which was supported in its early stages by the AISP training and technical assistance Learning Community program, is comprised of an Executive Team of approximately eight personnel responsible for the leadership, management, and technical and operational oversight of the project. A cross-agency eMOU is in place which outlines the data sharing process and permissible uses for cross-agency data. Inquiry projects are prioritized through the governance process, and several high impact uses have been conducted, including projects focused on Opioid Use Disorder (OUD) and Child Maltreatment Prevention.



► [Learn more about Rhode Island EOHHS here.](#)

**Lead Agency:** Executive Office of Health and Human Services

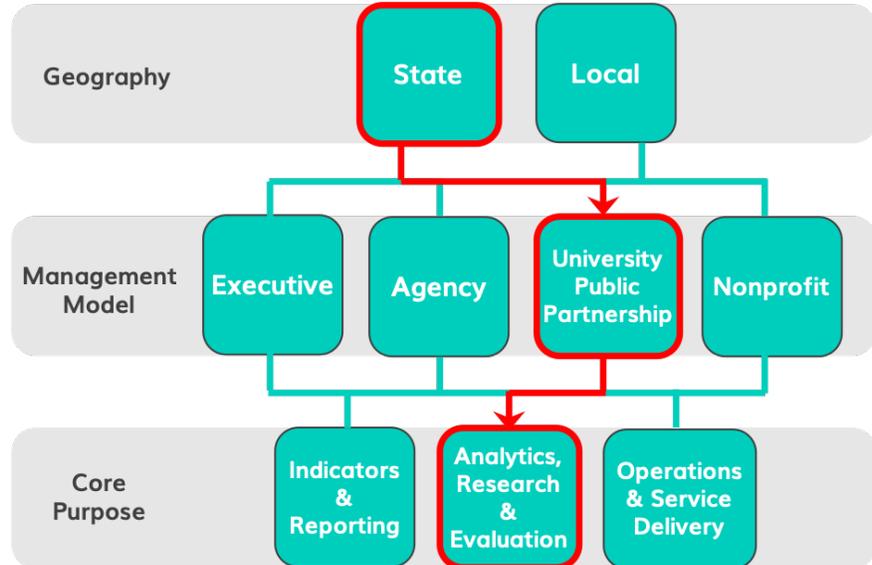
**Data Partners:** Department of Human Services; Department of Labor and Training; Department of Health; Department of Behavioral Healthcare, Developmental Disabilities, and Hospitals; Department of Youth, Children, and Families; Department of Corrections; and the RI Coalition to End Homelessness

**Legal Authority:** Overview of [EOHHS](#); [Authorizing Legislation for EOHHS](#)

**Funding:** State, federal, fee for service, philanthropic partners

## Institute for Research on Poverty (IRP) University Public Partnership, State

Institute for Research on Poverty (IRP) is an independent center within the College of Letters and Science at the University of Wisconsin-Madison. IRP supports and produces interdisciplinary poverty research and facilitates data linkages to affect policy and practice.



▶ [Learn more about IRP here.](#)

▶ [Learn more about WADC here.](#)

**Lead Agency:** University of Wisconsin–Madison

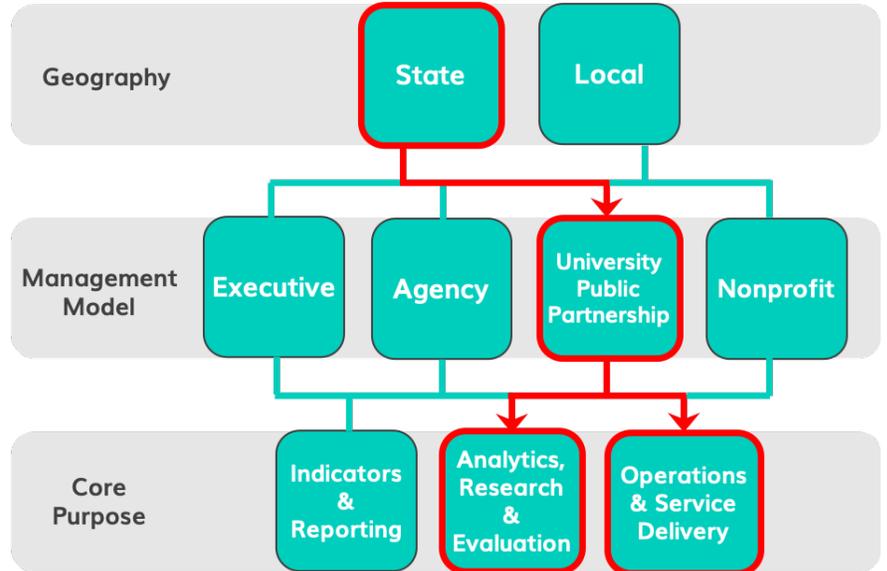
**Data Partners:** Department of Children and Families, Department of Health Services, Department of Workforce Development, Department of Corrections, Department of Public Instruction, Milwaukee County, Wisconsin Court System, and the Wisconsin Homeless Management Information System

**Legal Authority:** Contracts

**Funding:** UW-Madison, federal, state, local, philanthropic partners, fee for service

## Linked Information Network of Colorado (LINC) University Public Partnership, State

The Linked Information Network of Colorado (LINC) is a collaborative partnership between the Colorado Governor’s Office and the Colorado Evaluation Action Lab at The University of Denver. Their capacity for data integration helps strategically target services and benefits to vulnerable populations and identify opportunities to improve services, delivery, and opportunity.



► [Learn more about LINC here.](#)

**Lead Agencies:** Governor’s Office and University of Denver

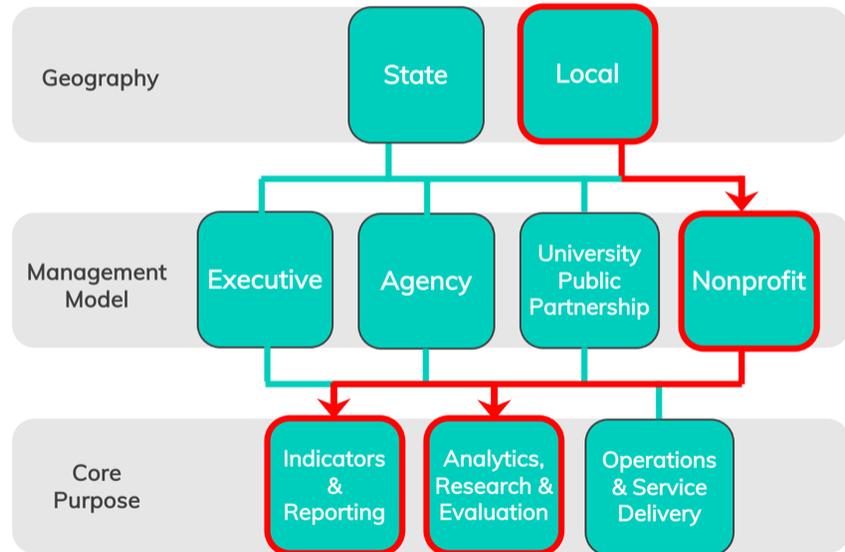
**Data Partners:** Birth and Death Records (CDPHE), Child Welfare (CDHS), Early Intervention (CDHS), Childcare subsidies (CDHS), EC Workforce Data (CDHS), Postsecondary Education (CDHE), Juvenile Justice Services (CDHS), Juvenile Courts (Judicial), Adult Court (Judicial), Denver Police Department (DPD), W-2 Employment and Wages (CLDE), Workforce Training Programs (CDLE), SNAP (CDHS), WIC (CDPHE), Denver Metro Homeless Initiative (HMIS), Denver Public Schools (DPS), see [LINC Data Partners](#)

**Legal Authority:** Contracts (e.g., [EMOU](#), [DSA](#), [DUL](#))

**Funding:** State, federal, philanthropic partners, fee for service

### Baltimore's Promise, Youth Data Hub Nonprofit, Local

Baltimore's Promise is a nonprofit organization that hosts the Baltimore Youth Data Hub—an initiative focused on meeting the needs of the City's children, youth, and families in partnership with other City agencies and community organizations.



► [Learn more about the Youth Data Hub here.](#)

**Lead Agency:** Baltimore's Promise

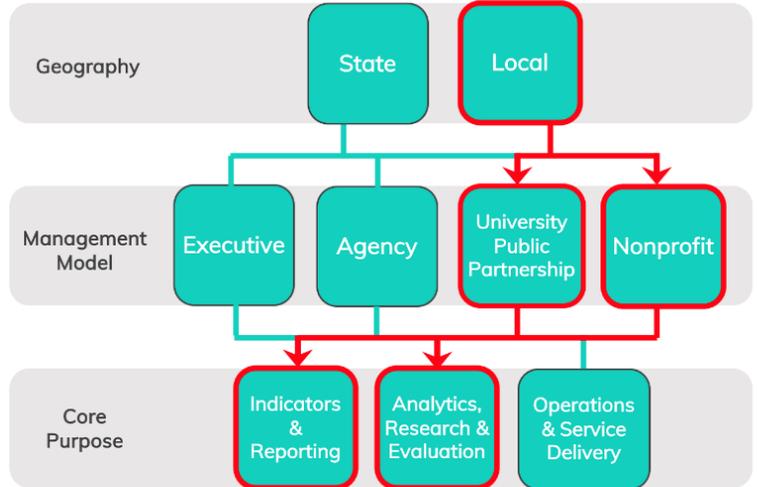
**Data Partners:** Baltimore City, Baltimore's Promise, and Baltimore City Schools, Baltimore City Health Department, nonprofit organizations

**Legal Authority:** [Authorizing legislation](#), contracts

**Funding:** Philanthropic partners, fee for service

### Institute for Social Capital Local, Nonprofit & University Public Partnership

The Institute for Social Capital is located within the University of North Carolina at Charlotte's Urban Institute. It houses the ISC Community Database, an integrated data system created to foster university research and to increase the community's capacity for data-informed decision-making. Through collaboration with nonprofit organizations, governmental agencies, and other organizations in the Charlotte region, ISC serves as a resource to benefit the university and the greater community. By linking data across agencies, the ISC Community Database allows researchers and community agencies to better describe, understand, and serve vulnerable populations.



► [Learn more about Institute for Social Capital \(ISC\) here.](#)

**Lead Agencies:** Institute for Social Capital, Inc. + University of North Carolina at Charlotte

**Data Partners:** UNC Charlotte, Charlotte-Mecklenburg Schools, the Foundation for the Carolinas, Mecklenburg County Department of Social Services, UNC Charlotte Urban Institute, United Way of Central Carolinas, Mecklenburg County Sheriff's Office, Crisis Assistance Ministry, Atrium Health

**Legal Authority:** Contracts

**Funding:** UNC Charlotte, philanthropic partners, fee for service

## ❖ Tribal Data Sovereignty

Tribal data sovereignty is the inherent right of a nation to govern the ownership, collection, and use of its own data.<sup>12</sup> Tribes are sovereign jurisdictions with the authority to self-govern and determine their own form of government and laws.<sup>13</sup> As part of this authority, Tribes necessarily have the authority to protect their citizens and provide human services that they elect.<sup>14</sup> It follows then that Tribal nations have the authority to administer the collection, use, and ownership of their own data.<sup>15</sup> Generally, state governments do not have regulatory authority on Tribal lands. As a result, in a data sharing context, Tribes and state governments can enter into data sharing agreements.<sup>16</sup> Under federal law, however, Congress has the authority to legislate on tribal issues, and Tribes are subject to the plenary power of the federal government. In the data sharing context, this means that in certain circumstances Tribes may be subject to federal law. For example, when a tribal health department provides HIPAA-covered services, it is considered a “covered entity” and must ensure HIPAA compliance.<sup>17</sup> As a result, the legal frameworks discussed previously can be helpful for Tribes intending to share data with state and local partners. *Appendix B* provides a sampling of Tribal laws pertinent to data sharing.

## ❖ Federal and State Laws

There are discrete statutes and regulations that must be considered in creating an IDS. Some are federal, some are state. Not all of these laws apply in every situation, and on occasion laws may be in apparent conflict. For example, all states protect the confidentiality of certain types of information. Of particular relevance are state laws governing highly confidential information such as arrest records, mental health records, and other sensitive types of information. The confusion that sometimes arises is when there is a perceived or real conflict between federal and state law. In addressing this conflict, it is worth keeping certain principles in mind: Some federal laws, for example HIPAA, create a floor for protecting confidentiality, and states must meet the minimum requirements but are free to set more stringent requirements. Given the above, there are some substantive areas (mental health, HIV, criminal justice) where state laws must be consulted in determining applicable confidentiality rules.<sup>18</sup> The graphic below identifies some of the laws most likely to be relevant to the discussion. For further legal resources by federal and state statute, see [Appendices A](#) and [B](#).

12 [Williams v. Lee](#), 358 U.S. 217, 271 (1959).

13 [Nat’l Farmers Union Ins. Companies v. Crow Tribe of Indians](#), 471 U.S. 845, 856 (1985).

14 See [Tsosie \(2019\)](#).

15 See [Tauli-Corpuz \(2016\)](#).

16 For information on jurisdictional coordination between states and Tribes, see [Tribal Legal Preparedness Project](#).

17 See [Milam \(2020\)](#).

18 See [Hodge, Kaufman, and Jaques \(2011\)](#).

← FEDERAL →

				
<p><b>HMIS</b> Protects information collected through the Homeless Management Information System (HMIS), under the guidance of the U.S. Department of Housing and Urban Development (HUD).</p>	<p><b>FERPA</b> FERPA protects the confidentiality of education records.</p>	<p><b>PRIVACY ACT</b> Regulates personally identifiable records maintained by federal agencies.</p>	<p><b>HIPAA</b> HIPAA regulates the protection of individually identifiable health information.</p>	<p><b>42 CFR PART 2</b> Stringent federal regulations (referred to commonly as 42 CFR Part 2) protect the confidentiality of alcohol and substance abuse treatment records.</p>

<p>↑ STATE ↓</p>	<p><b>CRIMINAL &amp; JUVENILE JUSTICE RECORDS</b></p>	<p>State laws typically govern access to criminal records, such as arrest records, and juvenile justice records, such as juvenile court files.</p>
	<p><b>MENTAL HEALTH RECORDS</b></p>	<p>States typically have statutory provisions governing the confidentiality of mental health records.</p>
	<p><b>MEDICAID RECORDS</b></p>	<p>Access to Medicaid records is generally controlled by the state agency that administers the Medicaid program.</p>
	<p><b>HIV LAWS</b></p>	<p>Most states have special laws protecting the confidentiality of information that may disclose a person's HIV status.</p>

RELEVANT LAWS

## ▶ Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to **protected health information**<sup>19</sup> (PHI) and is likely to arise as an issue whenever any type of health information is considered as part of an IDS. HIPAA also has provisions governing the security of electronic data, and those are considered.<sup>20</sup> Three points are worth noting about HIPAA:

- HIPAA establishes a minimum standard for protecting PHI. If a state law provides more protection, then the state law applies. This will often be the case when mental health records are involved.
- HIPAA only applies to “covered entities,”<sup>21</sup> defined as “health plans” (e.g., insurance companies, Medicaid agencies, Medicare); “health providers,” such as hospitals and licensed health professionals; and “health care clearinghouses,” which are entities that standardize health information for functions such as billing. HIPAA does not apply to courts and other entities that may produce or hold health-related information.
- HIPAA provides specific information on the “de-identification” of PHI. In addition, HIPAA provides for creation of a “limited data set”<sup>22</sup> (similar but not identical to a “de-identified data set”) as an alternative to the use of PHI. So it is always worth considering whether it is essential to use information that identifies individuals for the functions of the IDS, or whether de-identified information will suffice (or be the only type of information that is politically possible to use).

## ▶ Federal Education Rights and Privacy Act (FERPA)

**FERPA** regulates the confidentiality of education records. It defines education records broadly as those records directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.<sup>23</sup> FERPA also protects PII about the student that is different than the PHI covered by HIPAA. Four points about FERPA are worth noting, with more detail provided in the reference section:

- Because researchers often had difficulty accessing records protected by FERPA, the U.S. Department of Education (DOE) promulgated a rule intended to expand access for research: DOE noted that the restrictive interpretation given FERPA was unwarranted “given Congress’ intent in the American Recovery and Reinvestment Act to have states link data across sectors.”<sup>24</sup>
- DOE makes clear that “these final regulations allow FERPA-permitted entities to disclose PII from education records without consent to authorized representatives, which may include other state agencies, or to house data in a common state data system, such as a data warehouse administered by a central state authority for the purposes of conducting audits or evaluations of federal- or state-supported education programs.”<sup>25</sup> Note the specific reference to a “data warehouse.”

19 45 CFR § 160.103.

20 See [Scholl, Stine, Nash, et al.](#) (2008, under revision 2021).

21 45 CFR § 160.103.

22 45 CFR § 164.514.

23 34 CFR § 99.3.

24 See [discussion of the regulation with DOE commentary within Federal Register \(2011, Dec. 2\)](#).

25 See [Federal Register, 2011, 76\(No. 232\), p. 75637](#).

FERPA provides for the release of de-identified records if certain requirements are met, and the National Center for Education Statistics (2010) has a comprehensive [guide](#) on this subject.<sup>26</sup> The Privacy Technical Assistance Center (2017) has also released [guidance](#) specifically addressing concerns around IDS and student privacy.<sup>27</sup>

Finally, there may be confusion between which parts of a student record are covered by FERPA and which sections may be covered by HIPAA. The federal government has prepared [guidance](#) on this issue.<sup>28</sup>

## ▶ Federal Regulations Governing the Confidentiality of Alcohol and Substance Abuse Treatment Records (42 CFR Part 2)

Stringent federal regulations (referred to commonly as [42 CFR Part 2](#)) protect the confidentiality of alcohol and substance abuse treatment records. While HIPAA protects PHI in the possession of covered entities, 42 CFR protects information regardless of who has possession, as long as the information was “received or acquired by a federally assisted alcohol or drug program.”<sup>29</sup> Three points about 42 CFR Part 2 are worth noting here:

- Despite the stringent nature of the regulations, they do provide for the use of covered information for research without the individual’s consent if the director of the federally assisted program finds certain conditions are [met](#).
- As with FERPA, there is crossover with HIPAA in some circumstances (42 CFR).<sup>30</sup>
- Many state laws on substance abuse track (or in some cases may exceed) protections in 42 CFR. In thinking about an IDS, it is important to look at state law as well as the federal regulations.

## ▶ The Homeless Management Information System (HMIS)

Federal law establishes the definition of “homelessness” that policy makers, researchers, and others will often use, for its uniformity across jurisdictions. Federal law also protects the confidentiality of information collected through the Homeless Management Information System (HMIS), under the guidance of the U.S. Department of Housing and Urban Development (HUD).<sup>31</sup> HMIS protects the confidentiality of protected personal information (PPI), which is similar though not identical to the definitions of protected categories of information under other federal laws. Three points about HMIS are worth noting here.

- PPI can be disclosed externally or used internally by the homeless organization only if the use or disclosure is permitted by law and is described in the organization’s privacy policy. One of those uses is for research.
- Disclosure for research can occur only pursuant to a research agreement between the HMIS provider and the researcher.
- As with other federal laws, HMIS data can be used in de-identified form.<sup>32</sup>

---

26 See [SLDS Technical Brief: Guidance for Statewide Longitudinal Data Systems](#) (2010, November).

27 See U.S. Department of Education, [Integrated Data Systems and Student Privacy \(2017, January\)](#).

28 See [Joint Guidance on the Application of the FERPA and HIPAA to Student Health Records](#) (2008, revised 2019).

29 42 CFR § 2.11.

30 See [Kamoie and Borzi \(2001, August\)](#).

31 See 42 USC § 11360a; 24 CFR § 578.7; 24 CFR § 578.57; 24 CFR § 578.103; 69 FR 45888.

32 See [Sokol and Gutierrez \(2005, July\)](#).

## ▶ The Privacy Act

The Privacy Act (1974) has stringent confidentiality provisions but permits disclosure without the subject's consent for a "routine use," defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected."<sup>33</sup> This definition has been used to permit researcher access even to identifiable data.

## ❖ Conclusion

There is no one right path to data sharing and use that is legal, ethical, and a good idea. Clear legal frameworks can help you get your footing to find the way that is right in your context. These frameworks are also essential to mitigate inevitable risks and to protect privacy, and guide responsible data use. We hope this guide has shown you that, while this task is complex, it is possible and worthwhile. With the right team asking and considering the right questions, agencies and their partners can "find a way forward" to share and integrate data.

---

33 5 USC § 522a (a)(7).

## ❖ Common Definitions

**Administrative data:** data collected during the routine process of administering programs.

**Administrative data reuse:** using data in a way not originally intended (e.g., for evaluation, research, and planning).

**Aggregate data:** information collected from multiple sources that is compiled into a summary form, often for reporting purposes.

**Anonymized data:** data that have been de-identified and then anonymized, including, but not limited to, the removal of all personally identifiable information and aggregated at sufficient geography and cell size or perturbed.

**Confidential data:** data that is restricted by law, including personally identifiable information.

**Cross-sector data sharing:** the practice of securely providing access to information not otherwise available across agencies.

**Data breach:** the intentional or unintentional release and use of protected data (generally understood as data that can lead to identification of a person)—for example, a malicious intruder with intent to use stolen data.

**Data integration:** involves data sharing that includes identifiable information (e.g., name, date of birth, SSN), so that records can be linked, or integrated at the individual level.

**Data licensee/data user/data recipient:** an individual receiving data for approved use.

**Data owner/data partner/data provider:** the owner of confidential data that has agreed to grant access for approved use.

**Data security:** the process of protecting data from unauthorized access and use throughout the data life cycle. Appropriate data security is the best protection against a data breach. A well-designed IDS will include industry-standard data security measures covering legal, physical, technical, and procedural safeguards. Data security within the IDS may be more rigorous than the security applied to the original source data. While the risk of a data security event can never be fully eliminated, the IDS lead agency can manage these risks through a layered approach, including:

- ▶ **Legal safeguards:** organizational structure (e.g., entity with authority to conduct data integration, entity with liability/board/cyber insurance); data sharing agreements, including MOUs, DULs, cooperation agreements, and confidentiality agreements; data license process; data security plans
- ▶ **Physical safeguards:** hardened work stations; locked offices
- ▶ **Technical safeguards:** routine security audits; passwords (dual authentication); encryption (data at rest, data in transfer); secure servers (e.g., public cloud, private cloud, on-premise); data integrity measures (e.g., backups); controlled, limited access; private network; de-identification/anonymization standards and procedures

- ▶ **Procedural safeguards:** strong data governance; regular communication among staff, both vertical and horizontal; clear standard operating procedures; regular staff training; oversight of board that includes data stewards/data owners; incident response protocols; logs (audit trail); data quality review

**Data Sharing Agreement (DSA):** an agreement, generally between data owners, with specific terms and conditions that govern how specific data are transferred, stored, and managed when shared and integrated within the IDS.

**Data Use License (DUL):** an agreement that sets forth the terms and conditions under which an analyst, researcher, evaluator, or other outside party may gain access to data from the IDS for a specific purpose.

**Institutional Review Board (IRB):** an administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated.

**Memorandum of Understanding (MOU):** an agreement, generally between data owners and a lead agency, that sets forth the core features of the management model (i.e., what agency fulfills the functions of governance, data management and integration, and analytics) as well as the legal rights and responsibilities of each party involved.

**Privacy:** Privacy applies to the individual. Privacy measures are concerned with the settings and methods of information gathering. Privacy is also concerned with the type of information being collected. For a nuanced discussion of privacy, see [Nothing to Hide: Tools for Talking \(and Listening\) About Data Privacy for Integrated Data Systems](#), p. 12.

**Security incident:** an event that leads to a violation of established security policies and puts protected data at risk of exposure—for example, a malware infection, unauthorized access, insider breach, or loss of equipment

**Stakeholders:** define term to indicate group that is put together to determine collaborative decision-making—each data integration effort will include a different group of stakeholders

## References

- Finch, K., Hawn Nelson, A., Jenkins, D., Burnett, T.C., Oliver, A., Martin, R. et al. (2018). **Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems.** Future of Privacy Forum & Actionable Intelligence for Social Policy.
- Actionable Intelligence for Social Policy and Future of Privacy Forum. (2018). **Nothing to Hide: Tools for Talking (and Listening) About Data Privacy for Integrated Data Systems.**
- Allison-Jacobs, R. (2018, November). **IDS Case Study: The Institute for Social Capital.** Actionable Intelligence for Social Policy, University of Pennsylvania.
- Asemio. (2021.). **Unlocking Insights: How Tulsa Built Momentum with Easier, Faster, and Safer Data Sharing.**
- Center for Regional Economic Competitiveness (CREC). (2018). **Data Sharing Toolkit.** State Data Sharing Initiative.
- Centers for Disease Control and Prevention. Office for State, Tribal, Local and Territorial Support. (2017, March 2). **Tribal Emergency Preparedness Law.**
- Commission on Evidence-Based Policymaking. (2017, September). **The Promise of Evidence-Based Policymaking.**
- Connecticut Office of Policy and Management. (2020, January 15). **Legal Issues in Interagency Data Sharing.**
- Connecticut Office of Policy and Management. Connecticut Open Data. (revised 2021). **2019 CT Data Catalog (Non GIS).**
- Connecticut Office of Policy and Management. (2022). **Governance.**
- CTData Collaborative: Hartford Data Collaborative. (n.d.). **HDC Governance Structure.**
- CTData Collaborative: Hartford Data Collaborative. (n.d.). **HDC Data Request Process.**
- Data Across Sectors for Health and The Network for Public Health Law. (2018). **Data Sharing and the Law, Deep Dive on Consent.**
- Flanagan, A., King, J., and Warren, S. (2020, July). **Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction.** World Economic Forum.
- Gibbs, L., Hawn Nelson A., Dalton E., Cantor, J., Shipp, S., and Jenkins D. (2017). **IDS Governance: Setting Up for Ethical and Effective Use.** Actionable Intelligence for Social Policy, University of Pennsylvania
- Hawn Nelson, A., Jenkins, D., Zanti, S., Katz, M., Berkowitz, E., et al. (2020). **A Toolkit for Centering Racial Equity Throughout Data Integration.** Actionable Intelligence for Social Policy, University of Pennsylvania.
- Hawn Nelson, A., Jenkins, D., Zanti, S., Katz, M., Burnett, T., Culhane, D., Barghaus, K., et al. (2020). **Introduction to Data Sharing and Integration.** Actionable Intelligence for Social Policy, University of Pennsylvania.
- Hodge, J., Kaufman, T., and Jaques, C. (2011). **Legal Issues Concerning Identifiable Health Data Sharing Between State/Local Public Health Authorities and Tribal Epidemiology Centers in Selected U.S. Jurisdictions.** Council of State and Territorial Epidemiologists.
- Iowa's Integrated Data System for Decision-Making. (2021). **Governance.**
- Jenkins, D., Berkowitz, E., Burnett, T., Culhane, D., Hawn Nelson, A., Smith, K., and Zanti, S. (2021). **Quality Framework for Integrated Data Systems.** Actionable Intelligence for Social Policy, University of Pennsylvania.
- Kamoie, B., and Borzi, P. (2001, August). **A Crosswalk Between the Final HIPAA Privacy Rule and Existing Federal Substance Abuse Confidentiality Requirements.** Health Policy and Management Issue Briefs. Paper 10.

- Kitzmilller, E. (2014, March). **IDS Case Study: South Carolina**. Actionable Intelligence for Social Policy, University of Pennsylvania.
- Linked Information Network of Colorado. (n.d.). **How LINC Works**.
- Milam, S. (2020, March). **Tribal HIPAA Hybrid Entity FAQs**. The Network for Public Health Law.
- National Association of Counties. (2018). **Using and Sharing Data**.
- National Center for Education Statistics. (2010, November). **SLDS Technical Brief: Guidance for Statewide Longitudinal Data Systems**.
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Office for Human Research Protections. (1979, April 18). **The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research**. [Bethesda, Md.]: The Commission.
- National Neighborhood Indicators Partnership. (2022). **Partner Profiles**.
- North Carolina Department of Health and Human Services. (2021). **NCDHHS Operational Data Request Form**.
- Petrila, J., Cohn, B., Pritchett, W., Stiles, P., Stodden, V., Vagle, J., Humowiecki, M., and Rosario, N. (2017). **Legal Issues for IDS Use: Finding a Way Forward**. Actionable Intelligence for Social Policy, University of Pennsylvania.
- Scholl, M., Stine, K., Nash, J., Bowen, P., Johnson, L., Smith, S., and Steinberg, D. (2008, under revision 2021), **An Introductory Resource Guide for Implementing the HIPAA Security Rule**. National Institute of Standards and Technology.
- Smart Cities Council of North America. (2017, April 13). **Three Ways Data Sharing Is Advancing Cities**.
- Sokol, B., & Gutierrez, O. (2005, July). **Technical Guidelines for Unduplicating and De-identifying HMIS Client Records**. U.S. Department of Housing and Urban Development and Office of Community Planning and Development.
- Tauli-Corpuz, V. (2016). Preface. In **Indigenous Data Sovereignty: Toward an Agenda**, xxi, xxi-xxii. ANU Press.
- Tribal Legal Preparedness Project. (n.d.). University of Pittsburgh.
- Tsosie, R. (2019). **Tribal Data Governance and Informational Privacy: Constructing “Indigenous Data Sovereignty.”** *Montana Law Review*, 80, 229–268.
- U.S. Department of Education. Privacy Technical Assistance Center. (2017, January). **Integrated Data Systems and Student Privacy**.
- U.S. Department of Health & Human Services. Office for Human Research Protections. (2018). **Institutional Review Board Written Procedures: Guidance for Institutions and IRBs**.
- U.S. Department of Health & Human Services. Office of the National Coordinator for Health Information Technology. (2018). **Meaningful Consent Overview**.
- U.S. Department of Health & Human Services and U.S. Department of Education. (2008, revised 2019). **Joint Guidance on the Application of the Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records**.
- Zanti, S., Jenkins, D., Berkowitz, E., Hawn Nelson, A., Burnett, T., and Culhane, D. (2021). **Building and Sustaining State Data Integration Efforts: Legislation, Funding, and Strategies**. Actionable Intelligence for Social Policy, University of Pennsylvania.



**Appendix A: Relevant Federal Law and Policy**

Authority	Overview	Notable Exceptions and/or Exemptions for Disclosure
<p>Family Educational Rights and Privacy Act (FERPA)</p>	<p>FERPA regulates the confidentiality of education records. It defines education records broadly as those records directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution (34 CFR 99.3).</p> <p>*Note: De-identified data is not a “student record” and therefore not PII.</p>	<p>School Official (34 CFR §§ 99.31(a)(1), 99.7(a)(3)(iii))                      Audit or Evaluation (34 CFR §§ 99.31(a)(3), 99.35)                      Studies (34 CFR § 99.31(a)(6))</p>
<p><a href="#">Student Privacy at the U.S. Department of Education (U.S. Department of Education, 2021)</a></p> <p><a href="#">Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records (U.S. Department of Health and Human Services and U.S. Department of Education, 2019)</a></p> <p><a href="#">The Family Educational Rights and Privacy Act Guidance on Sharing Information with Community-Based Organizations (U.S. Department of Education, 2021)</a></p> <p><a href="#">Data Transfer in the Larger Education Ecosystem (U.S. Department of Education, 2020)</a></p> <p><a href="#">Federal Register Vol. 76 No. 232 (U.S. Department of Education, 2011)</a></p> <p><a href="#">Webinar on Integrated Data Systems and Student Privacy (U.S. Department of Education, 2017)</a></p> <p><a href="#">Integrated Data Systems and Student Privacy (U.S. Department of Education, 2017)</a></p> <p><a href="#">The Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements (U.S. Department of Education, 2015)</a></p> <p><a href="#">Responsibilities of Third-Party Service Providers under FERPA (U.S. Department of Education, 2015)</a></p>		
<p>42 CFR Part 2</p>	<p>Stringent federal regulations (referred to commonly as 42 CFR Part 2) protect the confidentiality of alcohol and substance abuse treatment records. While HIPAA protects PHI of alcohol and substance abuse treatment records in the possession of covered entities, 42 CFR protects information regardless of who has possession, as long as the information was “received or acquired by a federally assisted alcohol or drug program.”</p>	<p>Research (42 CFR 2.52)</p>
<p><a href="#">The Council of State Governments Justice Center. Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (Petrila, J. &amp; Fader-Towe, H., 2010)</a></p> <p><a href="#">Frequently Asked Questions (FAQs) and Fact Sheets regarding the Substance Abuse Confidentiality Regulations (U.S. Substance Abuse and Mental Health Services Administration, 2022)</a></p> <p><a href="#">Future Trends in State Courts (National Center for State Courts, 2012)</a></p>		

**Appendix A**

<p>Homeless Management Information System (HMIS)</p>	<p>Federal law establishes the definition of “homelessness” that policy makers, researchers, and others will often use for its uniformity across jurisdictions. Federal law also protects the confidentiality of information collected through the HMIS under the guidance of the U.S. Department of Housing and Urban Development (HUD). HMIS protects the confidentiality of “protected personal information” (PPI), which is similar though not identical to the definitions of protected categories of information under other federal laws.</p>	<p>Research (Privacy Standard 4.1.3)</p>
<p><b>FY 2022 HMIS Data Standards (Manual) (U.S. Department of Housing and Urban Development, 2021)</b></p> <p><b>HMIS Privacy and Security Standards: Emergency Data Sharing for Public Health or Disaster Purposes (U.S. Department of Housing and Urban Development, 2020)</b></p> <p><b>Snap Shot: Homeless Management Information Systems (The Network for Public Health Law, 2018)</b></p> <p><b>OCR Privacy Brief: Summary of the HIPAA Privacy Rule (U.S. Department of Health and Human Services, 2003)</b></p>		
<p>Privacy Act of 1974</p>	<p>Regulates personally identifiable records maintained by federal agencies.</p>	<p>Routine Use (5 USC 522a (a) (7))</p>
<p><b>Overview of the Privacy Act of 1974, 2020 Edition (U.S. Department of Justice, 2020)</b></p> <p><b>Computer Matching Agreements (U.S. Department of Education, 2007)</b></p> <p><b>Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment (Department of Justice, 2010)</b></p>		
<p>Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Part 164</p>	<p>HIPAA regulates the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.</p>	<p>Health Care Operations (Business Associates) Research (See, generally, 45 CFR § 164.512)</p>
<p><b>Covered Entities and Business Associates (U.S. Department of Health and Human Services, 2017)</b></p> <p><b>Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule (U.S. Department of Health and Human Services, 2004)</b></p> <p><b>HIPAA Research (U.S. Department of Health and Human Services, 2003)</b></p> <p><b>Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (U.S. Department of Health and Human Services, 2012)</b></p> <p><b>Agreement for Use of Centers for Medicare &amp; Medicaid Services (CMS) Data Containing Individual Identifiers (Centers for Medicare &amp; Medicaid Services, 2010)</b></p> <p><b>Business Associates (U.S. Department of Health and Human Services, 2003)</b></p> <p><b>Direct Liability of Business Associates (U.S. Department of Health and Human Services, 2021)</b></p>		

## Appendix B: Selected State & Tribal Laws, Policies, and Rules

The following table is a sampling of state and Tribal laws, policies, and rules related to data integration. This resource is not intended to be exhaustive.

Authority	Overview	Sample Rules
Medicaid 42 USC §§ 1396-1396v 42 USC § 1902(a)(7)(A); 42 USC § 1396a(a)(7)(A)	While federal law outlines several provisions governing the acquisition, use, and disclosure of Medicaid enrollees' health information, the state agency administering the Medicaid program sets the criteria and conditions for the disclosure and use of information about applicants and recipients.	Massachusetts: 130 CMR 515.007 (B)
Additional Guidance & Resources	<a href="#">Toolkit: Data Sharing for Child Welfare Agencies and Medicaid (U.S. Department of Health and Human Services Administration for Children &amp; Families, 2022)</a>  <a href="#">Facilitating Collaborations for Data Sharing between State Medicaid and Health Agencies (Centers for Medicare &amp; Medicaid Services (CMS), 1998)</a>	
Criminal Justice & Juvenile Justice	States have varying rules dealing with the confidentiality of adult and juvenile offender information.	North Carolina: G.S. 7B-3100 Connecticut: C.G.S. § 18-87k Tribal: Absentee Shawnee Juvenile Code, Section 317(e)-(f)
Additional Guidance & Resources	<a href="#">Collecting Data and Sharing Information to Improve School-Justice Partnerships (National Council of Juvenile and Family Court Judges, 2017)</a>  <a href="#">Research Policy Update: American Indian and Alaska Native Youth in the Juvenile Justice System (National Congress of American Indians Policy Research Center, 2020)</a>  <a href="#">The Council of State Governments Justice Center. Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (Petrla, J. &amp; Fader-Towe, H., 2010)</a>	
Child Welfare	To receive funding under the Child Abuse Prevention and Treatment Act (CAPTA), states must ensure and protect the privacy and confidentiality of the child, child's parents, and guardians. Jurisdictions have promulgated statutes and regulations that address confidentiality.	North Carolina: G.S. 108A-80, G.S. 7B-302(a1), and 7B-2901(b) Alabama: Ann. Code § 26-14-8 Tribal: <a href="#">Colville Confederated Tribes Code, Section 3-4-3(c)</a>
Additional Guidance & Resources	<a href="#">Data Sharing for Courts and Child Welfare Agencies (Administration for Children &amp; Families, 2018)</a>  <a href="#">Disclosure of Confidential Child Abuse and Neglect Records (Child Welfare Information Gateway, 2017)</a>  <a href="#">Reimagining Data at ACF (Administration for Children &amp; Families, 2018)</a>  <a href="#">TANF and Child Welfare Programs: Increased Data Sharing Could Improve Access to Benefits and Services (U.S. Government Accountability Office, 2011)</a>  <a href="#">Data Sharing Between TANF and Child Welfare Agencies (Office of Family Assistance, 2015)</a>  <a href="#">Data Sharing Policy Letter 17-02 (Administration for Children &amp; Families, 2017)</a>	
Mental & Behavioral Health	Some states have passed laws that add additional protection, beyond HIPAA, for protected behavioral health information	Colo. Rev. Stat. Ann. § 12-43-218
Additional Guidance & Resources	<a href="#">Behavioral Health Data Exchange Consortium, ONC State Health Policy Consortium Project (2014)</a>	

**Appendix B**

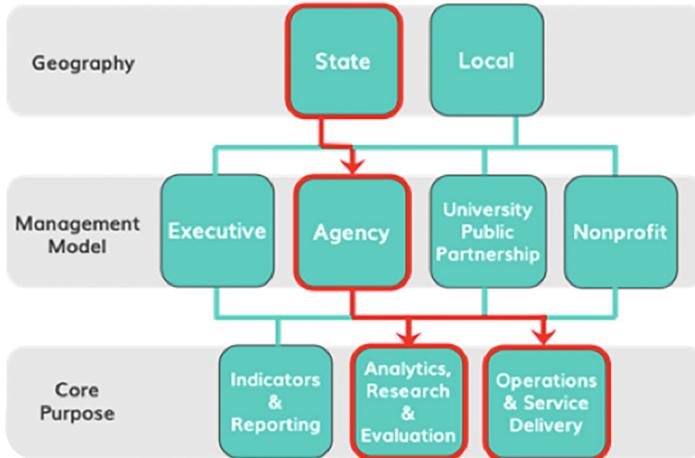
Data Sharing	Some states have passed laws to facilitate data sharing among state agencies.	Indiana: IC 4-3-26 et seq.
Additional Guidance & Resources	<p><a href="#">Summary of State Laws that Facilitate Data Sharing Among State Agencies (The Network for Public Health Law, 2019)</a></p> <p><a href="#">UNC School of Government. Internal Sharing of Information Within a County Department of Social Services (Nickodem, K., 2022)</a></p> <p><a href="#">Balancing Client Privacy with First Amendment Rights in Local Health Department Clinics (The Network for Public Health Law, 2021)</a></p> <p><a href="#">Data Privacy, Data Use, and Data Use Agreements (DUAs) (Center for Medicare &amp; Medicaid Services, n.d.)</a></p> <p><a href="#">The Council of State Governments Justice Center. Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (Petrila, J. &amp; Fader-Towe, H., 2010)</a></p>	
Student Records	Conn. Gen. Stat. § 10-234bb requires boards of education to enter into written contracts with consultants and operators (collectively, “contractors”) prior to providing contractors with, or allowing them to access, student information, student records, or student-generated content. (For federal guidance on student records refer to FERPA; see Appendix A.)	Connecticut: <b>§§ 10-234aa et seq.</b>
Vital Records	The legal responsibility for recording vital records, such as births and deaths, rests with the States.	Georgia: O.C.G.A. 31-10-25  North Carolina: G.S. 130A-93.(e) Access to vital records
Public Records	Most jurisdictions provide a broad right of access to records of public agencies.	Maryland: GP §§ 4-101 through 4-601  North Carolina: G.S. 132-1 et seq.
Additional Tribal Guidance and Resources	<p><a href="#">Improving Data Sharing for Tribal Health: What Public Health Departments Need to Understand About HIPAA Data Privacy Requirements (Milam, S., 2021)</a></p> <p><a href="#">Policy Brief: Native Nation Rebuilding for Tribal Research and Data Governance (Hiraldo, K., Russo Carroll, S., David-Chavez, D., Jager, M., Jorgensen, M., 2021)</a></p> <p><a href="#">Webinar: Charting a Path Forward for Responsible Data Sharing (National Congress of American Indians, 2019)</a></p> <p><a href="#">Tribal Public Health and the Law: Selected Resources (Centers for Disease Control and Prevention, 2016)</a></p> <p><a href="#">Tribal Epidemiology Centers Designated as Public Health Authorities Under the Health Insurance Portability and Accountability Act (Centers for Disease Control and Prevention, 2015)</a></p>	

**Appendix C: Sample Executive Orders and Legislation to Facilitate Data Integration**

Federal	
Executive Order	<a href="https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-ensuring-a-data-driven-response-to-covid-19-and-future-high-consequence-public-health-threats/">https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/21/executive-order-ensuring-a-data-driven-response-to-covid-19-and-future-high-consequence-public-health-threats/</a>
Legislation	<a href="https://www.congress.gov/bill/114th-congress/house-bill/1831">https://www.congress.gov/bill/114th-congress/house-bill/1831</a>
State & Tribal	
Indiana	Executive Order: <a href="https://www.in.gov/gov/files/EO_17-09.pdf">https://www.in.gov/gov/files/EO_17-09.pdf</a> Authorizing Legislation for Agency to support Data Integration: <a href="http://iga.in.gov/legislative/laws/2021/ic/titles/004#4-3-26-1">http://iga.in.gov/legislative/laws/2021/ic/titles/004#4-3-26-1</a>
Michigan	Executive Order: <a href="https://www.michigan.gov/documents/snyder/EO_2016-24_546395_7.pdf">https://www.michigan.gov/documents/snyder/EO_2016-24_546395_7.pdf</a>
Ohio	Executive Order: <a href="https://governor.ohio.gov/media/executive-orders/2019-15">https://governor.ohio.gov/media/executive-orders/2019-15</a>
Pennsylvania	Executive Order: <a href="https://www.governor.pa.gov/wp-content/uploads/2016/04/2016-07.pdf">https://www.governor.pa.gov/wp-content/uploads/2016/04/2016-07.pdf</a>
Tribal	Resolution: <a href="https://oneida-nsn.gov/wp-content/uploads/2016/02/01-12-05-A-Open-Records-and-Open-Meetings-Law.pdf">https://oneida-nsn.gov/wp-content/uploads/2016/02/01-12-05-A-Open-Records-and-Open-Meetings-Law.pdf</a>
Local	
Baltimore City, MD	Authorizing Legislation: <a href="https://mgaleg.maryland.gov/2022RS/bills/hb/hb1276E.pdf">https://mgaleg.maryland.gov/2022RS/bills/hb/hb1276E.pdf</a>
Montgomery County, MD	Authorizing Legislation: <a href="https://health.maryland.gov/psych/pdfs/Medicalreports.pdf">https://health.maryland.gov/psych/pdfs/Medicalreports.pdf</a>
Philadelphia, PA	Executive Order: <a href="https://www.phila.gov/media/20220330152115/executive-order-2022-02.pdf">https://www.phila.gov/media/20220330152115/executive-order-2022-02.pdf</a> (phila.gov)

## Appendix D: Definitions for Legal Framework for StateIDS

The following Appendices will be based upon a legal framework for a hypothetical State Integrated Data System (StateIDS). This approach is consistent with legal frameworks currently in place across the United States with a variety of management models, purposes, and technical infrastructure. It is important to note that this framework is currently in use with federated and nonfederated data systems, and both cloud-based and on-premise servers.



The StateIDS is based within an agency that is charged with data integration for state agencies. Data integration is largely conducted for Analytics and Research & Evaluation, but can be used for Operations & Service Delivery with a Data Use License in place.

While we recommend defining terms within each legal document to prevent duplicative pages in this report, we are including one list of definitions. The following terms are used through the interconnected suite of legal agreements that form the Legal Framework for StateIDS.

**Lead Agency:** State’s Office of Data Integration (“OODI”)

**Data Partners:** All state agencies

**Legal Authority:** Executive Order, Authorizing Legislation, contracts

**Funding:** Federal, state, fee for service

### Definitions

- a. **Anonymized Data:** Data where personal identifiers have been removed for a Data Recipient such that the likelihood of being able to re-identify individuals is extremely low. The terms of the DSA and/or DUL may require that data are anonymized prior to release to a Data Recipient.
- b. **Applicable Law:** Including, but not limited to, FERPA (34 CFR, Part 99), HIPAA (42 USC § 1320-d6), 42 CFR Part 2, 26 USC § 6103, 42 USC § 67, 42 USC § 503, 26 USC § 3304, subpart B of 20 CFR Part 603.
- c. **Authorized Personnel:** The members of the Data Recipient team who have been listed in this DUL as having approved access to the Licensed Data and agree to abide by the terms of the DUL.
- d. **Confidential Data:** Data submitted by the Data Provider that are restricted by law, including personally identifiable information.
- e. **Data Integration Staff:** The individuals within the Lead Agency who will have the approved responsibility of handling and securing relevant Confidential Data from Parties for approved Data Use License. The Data Integration Staff will consult with Party staff, clean Confidential Data, link Confidential Data, and prepare Licensed Data.
- f. **Data License Request Form:** The document that is reviewed by the StateIDS Data Oversight Committee for approval, revision, or rejection decisions. The approved Data Use License Request Form is attached to the DUL as Exhibit 1.
- g. **Data Provider:** An entity in the Party organization that has direct responsibility for a source of Confidential Data that can be contributed to approved Data Licenses. This may be an Office or Division of the Party organization, and in other cases it will be the Party itself.
- h. **Data Recipient:** The individual or organization that makes a request to the StateIDS for data analysis, research, or evaluation purposes, and is approved for a Data Use License. The Data Recipient may be an employee from a Party, strategic partner, or an external researcher.

## Appendix D

---

- i. Data Sharing Agreement (DSA): An agreement between each Data Provider and the Lead Agency that documents the specific terms and conditions for sharing Confidential Data with the Lead Agency for access and use. The DSA will include High Value Data Assets, Data Use Priorities, how Confidential Data is transferred and secured for Data Recipients and will refer to the EMOU as needed.
- j. Data Use License (DUL): Agreement between the Lead Agency and the StateIDS Data Recipient that outlines the role and responsibilities of the StateIDS Data Recipient. The DUL shall include the data use objectives, methodology, data description, data security plan, completion date, reporting requirements, data privacy requirements, and terms for data destruction. A standard DUL with terms will be approved by the Executive Committee.
- k. Data Use Priorities: Data use that is prioritized by Data Provider and/or Executive Committee.
- l. High Value Data Assets: Identified by each Data Provider, and relevant to data priorities. The High Value Data Asset inventory lists these assets as part of Attachment A of Data Sharing Agreement and is updated regularly as determined by the Lead Agency.
- m. Institutional Review Board (IRB): Administrative body established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated.
- n. Lead Agency: The Lead Agency will host governance (including stakeholder engagement and procedural oversight); manage technology (including data storage, integration, and access); and as needed, conduct analysis (including support for research methods, development of tools, and insights). Parties will transfer Confidential Data to the Lead Agency for linkage, cleaning, and anonymization, as stipulated in any applicable DSA(s). The Lead Agency will be responsible for transferring Licensed Data to the approved Data Recipient under the terms of an applicable DUL.
- o. Licensed Data: Data released to the Data Recipient, based upon the terms and conditions of the Data Use License.
- p. Major Change Request: Substantive changes to the DUL, such as additional research questions; change in organization using data; change in dissemination plan, etc.
- q. Minor Change Request: Procedural or administrative changes to the DUL, such as a change in key personnel, a first-time extension of up to six months, etc.
- r. Personal Identifiers: Any information about an individual that can directly or indirectly distinguish or trace an individual's identity, associate or link an individual to private information, distinguish one person from another, or be used to re-identify individuals. This includes PII and PHI.
- s. StateIDS Data Oversight Committee: The committee composed of representatives from each Data Provider within the Party with program, policy, or data expertise. At least one of these designated representatives must have decision-making authority over the use of their Confidential Data. The StateIDS Director will facilitate the StateIDS Data Oversight Committee but will not be a voting member.
- t. StateIDS Director: The individual who is responsible for facilitating committees, developing and managing partnerships with Party organizations, overseeing staff, consulting with Data Recipients, monitoring Data Licenses, and managing the inventory of documents associated with operations and Data Licenses.
- u. StateIDS Executive Committee: The committee comprised of at least one representative from each Party that shall be responsible for establishing, reviewing, and implementing this EMOU and any applicable DSA or DUL. This committee will also be responsible for appointing members of the StateIDS Data Oversight Committee, setting priorities for data access and use, and reviewing/approving the fee structure used for Data Use Licenses.

**Appendix E: EMOU Checklist**

¶	Question	Additional Information
	Title	Provide a descriptive title that clarifies the purpose of EMOU and makes it easily distinguishable from other agreements between the parties.
1	Preamble	Introductory paragraph that identifies the type of agreement, the parties to the agreement, the general intent of the parties. Articulates the mission, vision, and guiding principles of data integration effort.
2	Parties	<p>This section documents the legal names and contact information of the parties. For purposes of these foundational legal agreements, there are three major types of parties: Lead IDS Agency, Data Provider, and Data Licensee.</p> <p>The Lead IDS Agency is the legal entity that will administer the IDS. The Lead IDS Agency ultimately assumes responsibility for complying with all legal requirements, including data security, data privacy, and governance of the IDS, and fulfilling the expectations of all parties involved. [If these duties are fulfilled by more than one agency, the agreements should reflect roles (e.g., an agency leads on technical integration and another leads on governance)]. The Lead IDS Agency will be a party to all DSAs by which data is contributed by Data Providers in the IDS. It will also be a party to all DULs by which data is shared from the IDS with a Data Licensee.</p> <p>The Data Providers are the entities that own, steward, and agree to share administrative data with the IDS. In addition to facilitating data transfer to the IDS on a regular basis, the Data Provider will provide critical information about the data variables to ensure that its limitations and definitions are well understood. The Data Provider may also participate in the governance of the IDS.</p> <p>The Data Licensees are any entity that seeks to use data from the IDS. Data Licensees are often governmental agencies or academic researchers.</p>
3	Definitions	Defines key terms in this agreement. Includes even standard terms if there is potential for misinterpretation across agencies.
4	Justification	Reiterates the purposes for the IDS and clearly states the need. Section can also be used to describe the structure of the IDS (if not laid out in other sections). Describes model for governance, technical integration, and analytics.
5	Purpose	Provide context for the agreement. Identify specific purpose of the agreement within the legal framework, and define and limit the scope of specific data sharing relationship.
6	Financial Understanding	If funds are to be obligated under the agreement, the financial arrangements to all parties must be clearly stipulated. If no funds are obligated under the agreement, a statement should be included which makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement. If the agreement results in the exchange of money between agencies, state the estimated cost or costs not to exceed, terms of payments, and dispute resolution conditions. We recommend starting with the presumption that fees will be charged and make a decision on a case-by-case basis.
7	Governance Framework	Paragraphs A-F should describe the governance for the IDS, including determining Data Use Priorities; the Data License Request Process; Data Management Process; Oversight; and Communications.
7a	Data Use Priorities	Describes how data uses are prioritized by partners.
7b	Data Use License Request Process	Describes the data request process, including how a request is made.
7c	Data Use License Review and Decision Process	Describes how a request is reviewed and how decision regarding permitting access is made.
7d	Data Management Process	Describes how data are managed, referring to the DSA.
7e	Oversight of Data Use Requests	Describes the Data Governance oversight process, including staff roles and governance structures (e.g., StateIDS Data Oversight Committee and Executive Board).
7f	Communications	Describes the reporting and dissemination requirements that must be met by Data Licensee.
8	Counterpart Clauses	A counterpart clause permits the parties to the contract to sign different copies of the contract.
9	Term & Termination	State specific start and end dates of EMOU. Should also contain a provision whereby each party may terminate the agreement with a specified time frame.
	Exhibit A: Joinder Agreement	Amends the MOU to add a new party.

## Appendix F: Annotated EMOU Template

The following template can be used for drafting an EMOU (or MOU) between the Lead IDS Agency and the Data Contributor(s), also referred to as data partners, providers, and owners, depending on jurisdiction and preference. No single paragraph is required in all EMOUs. Instead, the length, formality, and comprehensiveness of the document and language may vary depending on the organizational legal culture. Even the name given to the agreement may vary depending on jurisdiction.

**TITLE:** Provide a descriptive title that clarifies the purpose of EMOU and makes it easily distinguishable from other agreements between the parties.

# Enterprise Memorandum of Understanding

## 1. Preamble

Data sharing is often an indispensable component of the cross-system collaboration needed to achieve the best government solutions for residents. For this reason, it is important to make interagency data sharing more streamlined and efficient, increasing the integration and analysis of data across programs. At the same time, the State is committed to preserving and strengthening the critical privacy safeguards in place to protect residents. In that spirit, this Enterprise Memorandum of Understanding (EMOU) has been developed for the Integrated Data System for the State (StateIDS) to facilitate an efficient and robust, data-driven cross-system collaboration that shields against disclosure of protected data as required by law.

**PREAMBLE:** Introductory paragraph that identifies the type of agreement, the parties to the agreement, the general intent of the parties.

**PARTIES:** This section documents the legal names and contact information of the parties. For purposes of these foundational legal agreements, there are three major types of parties: Lead IDS Agency, Data Provider, and Data Licensee.

The Lead IDS Agency is the legal entity that will administer the IDS. The Lead IDS Agency ultimately assumes responsibility for complying with all legal requirements, including data security, data privacy, and governance of the IDS, and fulfilling the expectations of all parties involved. [If these duties are fulfilled by more than one agency, the agreements should reflect roles (e.g., an agency leads on technical integration and another leads on governance)]. The Lead IDS Agency will be a party to all DSAs by which data is contributed by Data Providers in the IDS. It will also be a party to all DULs by which data is shared from the IDS with a Data Licensee.

The Data Providers are the entities that own, steward, and agree to share administrative data with the IDS. In addition to facilitating data transfer to the IDS on a regular basis, the Data Provider will provide critical information about the data variables to ensure that its limitations and definitions are well understood. The Data Provider may also participate in the governance of the IDS.

The Data Licensees are any entity that seeks to use data from the IDS. Data Licensees are often governmental agencies or academic researchers.

## 2. Parties

This StateIDS EMOU is entered into by the undersigned entities, hereafter collectively referred to as the "Parties." In order for any entity to be added as a Party to the EMOU, a joinder in the form of Exhibit A shall be executed. Such joinder does not constitute an amendment to the EMOU. Its sole effect is to add an additional entity as a Party and bind such entity to the terms of the EMOU in their entirety.

## 3. Definitions

See APPENDIX E

**JUSTIFICATION:**

Reiterate the purposes for the IDS and clearly state the need. Section can also be used to describe the structure of the IDS (if not laid out in other sections). Describes model for governance, technical integration, and analytics.

**4. Justification for State Integrated Data System**

The Parties share a mutual vision of more effective and responsive policies and programs for residents supported by timely and cost-efficient data analysis, research, and evaluation using integrated data across the respective Parties. The Parties have concluded that the StateIDS is needed to achieve this vision in many cases. StateIDS is a collaborative among the Parties that includes participation in the governance framework described in this EMOU, as well as usage of the Lead Agency for Data Use License Requests, the State’s Office of Data Integration (“OODI”).

This EMOU does not obligate Parties to use StateIDS in all cases if a different pathway for data access and linkage is preferred by Parties whose data are requested.

The Parties have concluded that StateIDS makes improved data sharing possible by:

- ▶ Establishing consistent data sharing and linking processes that adhere to all applicable state and federal laws, rules, and authoritative policies and guidelines
- ▶ Limiting the transfer of Confidential Data to only a centralized Lead Agency that employs staff with the required expertise and authorization to handle such Confidential Data
- ▶ Reducing the burden on Parties’ legal counsel and data management teams
- ▶ Taking a person- or family-centered approach to data use as opposed to an exclusively institution-centered approach.
- ▶ Building capacity for routine cross-system data-driven collaboration
- ▶ Increasing the efficiency of data sharing for cross-system research and analytic needs

**5. Purpose of the EMOU**

The Parties jointly enter the EMOU. The purpose of the EMOU is to establish the governance framework necessary to operate the StateIDS. This includes processes for establishing StateIDS priorities; requesting data; reviewing, determining approval for, and monitoring data use license requests in addition to disseminating information about each request to the appropriate StateIDS committees. The governance framework of this EMOU is implemented through the accompanying Data Sharing Agreement (DSA) between each Party and the Lead Agency, and a Data Use License (DUL) between the Lead Agency and Data Recipient.

**PURPOSE:** Provide context for the agreement. Identify specific purpose of the agreement within the legal framework, and define and limit the scope of specific data sharing relationship.

**6. Financial Understanding**

The StateIDS will be supported through a fee-for-use model to fund procedural and technical support. A fee will only be charged to Data Recipients. Parties to this EMOU will not be charged to participate in the StateIDS unless they are Data Recipients. This fee may include the costs incurred by Parties to this agreement for their efforts to provide data. The fee structure will be developed by the StateIDS Director and approved by the StateIDS Executive Committee before implementation.

**FINANCIAL UNDERSTANDING:** If funds are to be obligated under the agreement, the financial arrangements to all parties must be clearly stipulated. If no funds are obligated under the agreement, a statement should be included which makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement. If the agreement results in the exchange of money between agencies, state the estimated cost or costs not to exceed, terms of payments, and dispute resolution conditions. We recommend starting with the presumption that fees will be charged and make a decision on a case-by-case basis.

## 7. StateIDS Governance Framework

### A. Data Use Priorities

There are two ways that priorities will be established. The first is for the Data Provider to establish criteria for a request of their data to be considered (e.g., federal requirements, strategic priority data uses of the Party), as specified in Attachment C (“Data Use Priorities”) in the Data Sharing Agreement (DSA). The second is for the StateIDS Executive Committee to establish cross-system analytic, research, and evaluation topic areas that would benefit from using StateIDS.

**GOVERNANCE FRAMEWORK (¶A-F):** Paragraph A-F should describe the governance for the IDS, including determining Data Use Priorities; the Data License Request Process; Data Management Process; Oversight; and Communications.

### B. Data Use License Request Process

The Data Use License Request (DLR) process is intended to be transparent, efficient, and provide the StateIDS Data Oversight Committee with the information needed to review a Data Use License Request, to ensure data use is in alignment with the mission and vision. The Data Use License Request process will consist of two steps: (1) consultation with the StateIDS Director and (2) submission of a Data Use License Request.

1. **Consultation with the StateIDS Director.** Requestors shall complete an initial screening form and schedule a phone or in-person consultation with the StateIDS Director to discuss their proposed request. This consultation will also provide guidance on the appropriate Data Use License Request, whether for Research, Operational Data Use, or Aggregate requests. If applicable, the StateIDS Director will provide the requestor with an estimated fee before the Data Use License Request is submitted to the StateIDS Data Oversight Committee.

The StateIDS Director will conduct an initial review of the Data Use License Request to ensure that only responsive StateIDS DLRs are forwarded to the StateIDS Data Oversight Committee. The initial review will be limited to the following:

- a. Confirming that the request form is complete (i.e., no blank fields)
- b. Ensuring the request benefits residents and targets established data use priorities
- c. Verifying the requested elements are included in High Value Data Asset Inventories
- d. Confirming the data security plan meets requirements

Non-responsive requests will be returned with feedback to the requestor. Responsive requests will be forwarded to the StateIDS Data Oversight Committee.

2. **Submission of a Data Use License Request.** The Data Use License Request form is intended to capture the information the StateIDS Data Oversight Committee needs to make a decision around appropriate StateIDS access and use. The Data Use License Request is reviewed and approved by the StateIDS Data Oversight Committee. At minimum, the Data Use License Request will include:

- a. Purpose (general data analysis, research, or evaluation)
- b. Objectives (primary questions being answered)
- c. Data Recipient(s)
- d. Benefit to residents
- e. Population of study (e.g., age, demographics, geography, years)
- f. Data sources (program or organization directly associated with Data Provider)
- g. Data elements

- h. Design and analytic method
- i. Data Use License start and end date (anticipated release of findings to partners)
- j. Funding source(s) and, if applicable, estimated fee for Licensed Data
- k. Key personnel and credentials
- l. Potential risks and mitigation
- m. If applicable, IRB approval (or submission date)
- n. Data security plan

**C. Data Use License Review and Decision Process**

The review process is intended to ensure legal and ethical use. The StateIDS Director will perform an initial review of all proposals as described above, and the StateIDS Data Oversight Committee will make the decision on the Data Use License Request (i.e., reject, revise, approve) according to the following guidelines.

1. **StateIDS Data Oversight Committee review and decision.** This committee will convene as needed, in person or virtually, with the agenda and meeting dates publicly available.
  - a. An adhoc subcommittee, the Data Use License Request Review Committee (DLR Review Subcommittee), will be called to review Individual Data Use License Requests (DLR). The DLR Review Subcommittee shall include a member of each agency whose data is requested, as well as other members, typically selected for content or methodological expertise. The DLR Review Subcommittee membership may change based upon the type of Data Use License Request (Research, Operational, Aggregate). Any member of the StateIDS Data Oversight Committee (in addition to the Data Providers, who are required) can volunteer to participate in the DLR Review Subcommittee.
2. **Each Data Provider** will nominate at least one representative to the StateIDS Data Oversight Committee who will be responsible for reviewing Data Use License Requests for ethical (e.g., risk versus benefit of data access and use) and methodological considerations (e.g., appropriate data elements and analytic approach).

Data Providers have veto power over the use of their own data only. When invoking veto power, they must provide a clear rationale for why their data cannot be used for the request or may provide alternative data options to meet needs of the Data Use License Request. StateIDS Data Oversight Committee members will be given the opportunity to offer solutions to address the reason for the veto during the DLR Review Subcommittee process. If there is no solution that addresses the reason for the veto to the satisfaction of the Data Provider, the veto will stand.

StateIDS Director and support staff shall communicate StateIDS Data Oversight Committee schedules and require the requestor to be available to answer questions during the meeting, either virtually or in person. The specific review procedures shall be approved by the StateIDS Data Oversight Committee and allow reasonable flexibility for virtual participation, proxy membership, and email voting, as permissible. Key steps in the process include:

- a. Prior to the StateIDS Data Oversight Committee meeting, members of the ad hoc DLR Review Subcommittee shall complete a DLR review rubric and will make an initial recommendation of reject, revise, or approve. The expectation is that DLR Review Subcommittee members will have consulted, as needed, within their organization prior to the meeting or bring to the meeting representatives so that a decision can be made.
- b. The StateIDS Director and support staff shall synthesize the initial review information from the DLR Review Subcommittee members prior to the meeting and facilitate the discussion during the meeting.

c. Each Data Provider that has data being requested for a Data Use License Request will have one vote. Voting decisions include:

**Approve:** Does not require substantive changes or clarification to the proposal. The StateIDS Data Oversight Committee may require minor changes or offer suggestions to strengthen the DLR. The request does not need to return to the full committee, and the Director can oversee the required changes and update the StateIDS Data Oversight Committee.

**Revise:** Requires changes or clarification to the proposal that necessitate further consideration. The StateIDS Data Oversight Committee will typically consider revised proposals at the next meeting. Expedited reviews of revised proposals can occur at the StateIDS Data Oversight Committee's discretion.

**Reject:** The potential benefits of the data access and use do not outweigh identified concerns or risks. There is no appeal process, and decisions are final.

d. Approval must be given by all Data Providers involved in the Data Use License Request (unanimous approval). Should one or more Data Providers reject a request, the Data Use License Request can be revised to remove the data that was not approved and be resubmitted.

e. The StateIDS Director shall send StateIDS Data Oversight Committee and StateIDS Executive Committee members a summary of DLR decisions quarterly. The Director will consult as needed with the Executive Board to prioritize DLR timelines.

f. The StateIDS Director shall send a letter to the requestor conveying the decision, synthesizing reviewer comments, and outlining next steps (if applicable). A timeline and final cost estimate shall also be provided for approved DLRs.

### D. Data Management Process

The Data Management Process applies only to approved DLRs. All aspects of the Data Management Process are initiated by the Lead Agency staff, with specific roles referenced below when applicable.

1. The Lead Agency will execute a DUL with the Data Recipient. The DUL will specify data security requirements and the Data De-identification Policy for public dissemination (e.g., reports, presentations, publications), and will conform to any and all Party-specific requirements.
2. The Data Integration Staff shall adhere to all applicable state and federal laws, rules, and authoritative policies and guidelines for training and authorization to handle the Confidential Data from participating Parties. The Data Integration Staff will be responsible for securely receiving and storing Confidential Data from each Party as outlined in the DSA(s).
3. The Data Integration Staff shall use standardized and replicable identity resolution strategies to integrate the Confidential Data for Licensed Data. Parties may consult with the Data Integration Staff about preferred approaches.
4. As applicable, a process for anonymization will be developed by Data Integration Staff and approved by the StateIDS Data Oversight Committee before it is used in practice. In all cases, DLRs will use the minimum required Confidential Data to achieve the approved Data Use License Requests.
5. The Data Integration staff will securely transfer the Licensed Data to the Data Recipients under the agreed upon terms of the DUL.
6. After Licensed Data are provided to the Data Recipient, the Lead Agency will store, return, or destroy data from each Party according to the DSA(s).

7. Except as provided under applicable federal and state law, any and all data that are protected under federal and state privacy regulations will not be shared through State's Public Records Act requests. StateIDS will always comply with federal and state laws and will default to sharing Licensed Data only with the approved Data Recipient.

**E. Oversight of Data Use License Requests**

Oversight processes for the Data Use License Requests are intended to facilitate transparency and mutualism. Transparency ensures that all stakeholders have information about compliance with legal and ethical requirements as well as the outcome of data license requests. Mutualism refers to all Parties, the Lead Agency, and Data Recipients having consistent and timely communication so the data use can benefit their organizations and the lives of residents.

Should a Data Recipient use the Licensed Data for purposes that were not approved, a Data Provider will immediately terminate access to their data by the Data Recipient. It is the responsibility of the StateIDS Director to communicate and confirm this terminated access.

The StateIDS Director shall monitor timely completion of the following documents: (1) Regular Data Use License Reports, (2) Key Findings and Interpretations Release Requests, and (3) Certification of Data Use License Completion & Destruction of Data. Data Recipients shall initiate on an as needed basis (4) Change Reports, and (5) Data Use License Updates and Announcements.

1. Regular Data Use License Reports (May be required as part of DUL): Data Recipients must submit reports to the StateIDS Data Oversight Committee, annually or at the midterm point of the term of the license cycle, whichever comes first. The report shall be a standard form automatically distributed by the StateIDS Director or support staff and shall require:
  - Summary of progress to date
    - How data use is informing policy or practice
    - Description of unanticipated findings
    - Description of challenges encountered and how they are being resolved
  - Products and key findings publicly released to date
  - Funding source (if applicable)
2. Change Requests (As needed): Data Recipients will initiate, when necessary, a Data Use License change request. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the StateIDS Director. Major requests (e.g., additional research questions; change in organization conducting analyses) will be reviewed by the StateIDS Data Oversight Committee.
3. Key Findings and Interpretations Release Request (Required): Data Recipients are required to share DLR findings to the StateIDS Data Oversight Committee prior to any public release. Data Recipients shall submit key findings and interpretations in a standard format provided by the Director or support staff. StateIDS Data Oversight Committee members shall confirm in writing, via a standard form, that key findings have been reviewed and are ready for release. The StateIDS Data Oversight Committee members can request product specific reviews (e.g., presentations, publications).
4. Data Use License Updates and Announcements (Optional): Data Recipients may initiate at any time a Data Use License update or opportunity. These reports are a way to share newly released products, media coverage, or announcements for interested parties to attend a dissemination event or be updated on policy or practice informed by a Data License Request.
5. Certification of Data Use License Completion & Destruction of Data (Required): This is a standard form automatically distributed by the StateIDS Director or support staff and shall require confirmation of data destruction consistent with the DUL.

**F. StateIDS Communications**

1. The StateIDS Data Oversight Committee shall receive prior to each quarterly meeting (a) Regular Reports as appropriate for each Data Use License timeline, (b) Major Change Requests, and (c) summary of Minor Change Requests and Destruction of Data Reports to get necessary feedback.
2. Executive Committee shall receive after each quarterly meeting an update on StateIDS’s use, review results, key findings from existing Data Licenses, opportunities to learn more about Data Use Licenses that are in the dissemination phase, and abstracts of new DLRs.
3. The StateIDS Data Oversight and StateIDS Executive Committee members shall alert the StateIDS Director about any concerns regarding fulfillment of DLRs and any of the governance processes outlined in this EMOU. The StateIDS Director will be responsible for working with the Parties to resolve any concerns. The Parties can decide to suspend StateIDS involvement until the concerns are resolved.

**8. Counterparts.**

This EMOU may be executed in one or more counterparts, each of which shall be considered to be one and the same agreement, binding on all Parties hereto, notwithstanding that all Parties are not signatories to the same counterpart. Furthermore, duplicated signatures, signatures transmitted via facsimile, or signatures contained in a Portable Document Form (PDF) document shall be deemed original for all purposes.

**COUNTERPARTS:** A counterpart clause permits the parties to the contract to sign different copies of the contract.

**9. EMOU Effective Date and Terms.**

The effective date of the EMOU shall be \_\_\_\_\_, 20 \_\_\_\_\_. The EMOU will remain in effect until the StateIDS Executive Committee terminates the EMOU. An individual Party to the EMOU can end its involvement upon a termination request by their appointed Executive Committee member. Termination halts all future StateIDS requests for that Party’s data, but Data Use Licenses approved prior to termination will be completed.

**TERM & TERMINATION:** State specific start and end dates of EMOU. Should also contain a provision whereby each party may terminate the agreement with a specified time frame.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their duly authorized representatives.

Party: \_\_\_\_\_

Dated: \_\_\_\_\_

**EXHIBIT A**

**(Sample Form)  
Joinder Agreement**



**JOINDER:** A Joinder Agreement is an amendment to the MOU that adds a new party to the MOU.

Pursuant to, and in accordance with the StateIDS Enterprise Memorandum of Understanding (EMOU), effective \_\_\_\_\_, 20\_\_\_, as may be amended from time to time, the entity signing this Joinder Agreement (the “New Party”) hereby acknowledges that it has received and reviewed a complete copy of the EMOU. The New Party agrees that upon execution of this Joinder, it shall become a Party, as defined in the EMOU, to the EMOU and shall be fully bound by and subject to all of the terms and conditions of the EMOU. In witness thereof, the New Party has caused its duly authorized representative to execute this Joinder Agreement, as follows:

[New Party’s Name]

By: \_\_\_\_\_

[Name of Official, Title]

Date: \_\_\_\_\_

**Appendix G: DSA Checklist**

¶	Question	Additional Information
1	Preamble	Introductory paragraph that identifies the type of agreement, the parties to the agreement, the general intent of the parties. May contain “WHEREAS” statements. The preamble might also contain the legal names and contact information of the parties.
2	Transfer of Data from Provider to OODI	Describe how the data will be securely transferred or accessed.
3	OODI’s Rights to Share/Redistribute the Data	Describe whether any data can be shared or redistributed.
4	Data Access, Security, Use, and Deletion	Address record usage, duplication, and re-disclosure restrictions: limitations on the access to, disclosure, and use of information. Who can access the data? Limitations on identifiable data? Where can research/analysis be done?
4a	Limited Access	Specify who will have access to data. Recommend limiting access to only those individuals who have a bona fide need to access.
4b	Secure Storage	Outline the technical guidelines for maintaining a secure environment of data that is compliant with State and federal policies, standards and guidelines.
4c	Use	Define the scope and process of using data, as well as data transfer protocols. Consider whether the data subject to these administrative records will be made available to researchers or to the public. Are restricted data use licenses implicated? What kind of public disclosures need to be made?
4d	Data Deletion	Detail what records shall be retained for the use contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained. Specify what records should be destroyed and a timeline for the destruction of the data.
5	Anonymization of StateIDS Licensed Data	Describe the policies and procedures to protect the confidentiality and safety of data. Discuss specific protocols for physical and virtual/electronic security—be specific about proposed security arrangements and demonstrate full understanding of applicable statutes, regulations and traditional practices; how parties can inspect security arrangements for the purpose of confirming the user is in compliance with data security procedures and requirements specified by the agreement.
6	Data Provider Responsibilities for Meeting Legal Requirements	Specify the Provider’s obligation to comply with applicable laws.
7a	Confidentiality	Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description).

7b	Breach Notification	<p>Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data. Describe the responsibilities for notification by points of contact of each party to the DUL, any criminal/civil penalties that may apply for unauthorized disclosure of information, indemnification language and limitations of liability and any liquidated damages for breach of agreement if applicable.</p> <p>May want to specify Parties negotiating an agreement often make an explicit agreement as to what each party's remedy for breach of contract shall be.</p>
8	Modification; Assignment; Entire Agreement	<p>Establish relationship of this agreement with other understandings or agreements between the parties. Set forth the process for amending the DUL.</p>
9	No Further Obligations	<p>Clarify that there are no additional obligations created by the Agreement—namely, the obligation to enter into future agreements or furnish future data.</p>
10	Compliance with Law, Applicable Law	<p>State the specific authority that allows for the discretion to disclose/re-disclose/mandate and discretion to evaluate/mandate to evaluate. Should cite specific statutes, executive orders, disclosure laws, paperwork reduction acts, etc.</p>
11	Term of Agreement	<p>State specific start and end dates of the DSA. If the completion date is not known and the period of the agreement is expected to stretch over a number of years, the completion date may be listed as indefinite. Should also contain a provision whereby each party may terminate the agreement with a specified time frame.</p>
12	Use of Name	<p>Neither the Provider nor OODI will use the name of the other party or its employees in any advertisement or press release without the prior written consent of the other party.</p>
13	Definitions	<p>Define key terms in this agreement. Include even standard terms if there is potential for misinterpretation.</p>
14	Indemnification	<p>Specify whether the parties will indemnify or defend one another for breach or loss.</p>
	Attachment A: High Value Data Asset Inventory	<p>Compile list of data that have been identified by Data Provider as a strategic asset.</p>
	Attachment B: Confidentiality Agreement	<p>Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description).</p>
	Attachment C: Approved Data Use Priorities	<p>Enumerate the specific uses and priorities to support IDS data access and use.</p>

## Appendix H: Annotated DSA Template Between IDS Lead and Data Provider

### DATA SHARING AGREEMENT

#### 1. Preamble

This Data Sharing Agreement (“Agreement”) is by and between \_\_\_\_\_ (“Data Provider”) and the State’s Office of Data Integration (“OODI”), and is effective as of the last date of signature shown below (the “Effective Date”).

**WHEREAS**, OODI will act as the Lead Agency of the Integrated Data System of the State (StateIDS).

**WHEREAS**, Data Provider wishes to share data with OODI in accordance with the terms and conditions of this Agreement and approved under the terms and conditions of the StateIDS Enterprise Memorandum of Understanding (EMOU), a copy of which is attached and incorporated herein.

**NOW, THEREFORE**, the parties, in consideration of mutual promises and obligations set forth herein, the sufficiency of which is hereby acknowledged, and intending to be legally bound, agree as follows:

#### 2. Transfer of Data from Provider to OODI

If not otherwise stored within the StateIDS, the Data Provider will submit to OODI, or otherwise permit OODI’s Data Integration Staff to electronically access, the data associated with an approved Data Use License Request (DLR) in accordance with the StateIDS EMOU. If Data Provider is transmitting Confidential Data to OODI (as opposed to providing access for downloading), Data Provider will transmit the Confidential Data electronically only via encrypted files and in accordance with OODI’s data security standards and the State’s cybersecurity policies.

#### 3. OODI’s Rights to Share/Redistribute the Data

Except as expressly provided in this Agreement and the StateIDS EMOU, any data submitted to the StateIDS by the Data Provider will not be further distributed without Provider’s written approval.

#### 4. Data Access, Security, Use, and Deletion

OODI will comply with the following access and security requirements:

- a. Limited Access. OODI will limit access to the Confidential Data to Data Integration Staff who have signed the Confidentiality Agreement in Attachment B and are working on a specific DLR with the Data Provider under the terms of the StateIDS EMOU. Only Licensed Data will be provided to Data Recipients of approved DLRs as defined in the accompanying StateIDS EMOU.
- b. Secure Storage. OODI agrees to proceed according to requirements, contained in (FISM) NIST SP800-39, Managing Information Risk. Furthermore, OODI shall be responsible for maintaining a secure environment compliant with State policies, standards and guidelines, and other Applicable Law that supports the transmission of Confidential Data in compliance with the specifications. OODI shall follow the specifics contained in (FISM) NIST SP800-47, Security Guide for Interconnecting Information Technology Systems and shall use appropriate safeguards to prevent use or disclosure of Confidential Data other than as permitted by the StateIDS EMOU, the (FISM) NIST SP800-47, and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Confidential Data. Appropriate safeguards shall be those required by Applicable Law related to data security, specifically contained in (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations.
- c. Use. OODI shall use the Confidential Data solely for purposes approved through the StateIDS EMOU (“Purpose”). OODI shall only disclose the Confidential Data to Data Integration Staff who have the authority to handle the data in furtherance of the Purpose. OODI will only provide approved Licensed Data to Data Recipients who have signed the Data Use License.

- d. Data Deletion. OODI shall retain the Data Provider's Confidential Data for Data Use Licenses for a period of twelve months after providing the Licensed Data to the Data Recipient, unless otherwise agreed to by the Data Provider and OODI within the terms of the DSA. After this twelve-month period, all Confidential Data and Licensed Data will be deleted by OODI.

**5. Anonymization of StateIDS Licensed Data**

- a. Criteria for Licensed Data that Is Anonymized. Licensed Data may only be released to Data Recipients who have been approved to receive Licensed Data. Terms of the DSA and/or DUL may require that Licensed Data is Anonymized, meaning Data Integration Staff remove all personal identifiers which can be used to identify an individual. Unless otherwise specified in DSA and/or DUL, personal identifiers shall include those consistent with a HIPAA Limited Data Set (§ 164.514(b)(2)). These include name, social security number, residential address smaller than town or city, telephone and fax numbers, email address, unique identifiers, vehicle or device identification numbers, web universal resource locators, internet protocol address numbers, and biometric records.
- b. Data De-identification Policy. OODI agrees that DLRs, including data from the Data Provider in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.), must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than 15 observations may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than 15 observations. Individual level records may not be published in any form, electronic or printed. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than 15 observations cannot be identified by manipulating of any combination of dissemination materials generated through the use of Licensed Data. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

**6. Data Provider Responsibilities for Meeting Legal Requirements**

Data Provider has collected the Confidential Data from individuals. Accordingly, Data Provider is solely responsible for ensuring that all legal requirements have been met to collect data on individuals whose Confidential Data are being provided to StateIDS.

**7. Confidentiality and Breach Notification**

- a. Confidentiality. All Data Integration Staff shall be informed of the confidentiality obligations imposed by this Agreement and must agree to be bound by such obligations prior to disclosure of Confidential Data to Data Integration Staff, as evidenced by their signature on the Confidentiality Agreement in Attachment B. OODI shall protect the Confidential Data by using the same degree of care as OODI uses to protect its own confidential information, and no less than a reasonable degree of care.
- b. Breach Notification. OODI is responsible and liable for any breach of this Agreement by any of its Data Integration Staff. OODI shall report to the Data Provider all breaches that threaten the security of the State's data systems resulting in exposure of Confidential Data protected by federal or state laws, or other incidents compromising the security of the State's information technology systems. Such reports shall be made to the Data Provider within 24 hours from when OODI discovered or should have discovered the occurrence. OODI shall also comply with any Applicable Law regarding data breaches.

**8. Modification; Assignment; Entire Agreement**

This Agreement may not be modified except by written agreement of the Data Provider and OODI. This Agreement may not be assigned or transferred without the Data Provider and OODI's prior written consent. Subject to the foregoing, this Agreement will be binding upon and inure to the benefit of, and be enforceable by, the Data Provider and OODI and its successors and assigns. Notwithstanding anything to the contrary, each party has the right to disclose the terms and conditions of this Agreement to the extent necessary to establish rights or enforce obligations under this Agreement. This Agreement supersedes all previous Data Sharing Agreements, whether oral or in writing.

**9. No Further Obligations**

The Data Provider and OODI do not intend that any agency or partnership relationship be created by this Agreement. No party has any obligation to provide any services using or incorporating the Confidential Data unless the Data Provider agrees and approves of this obligation under the terms of the StateIDS EMOU. Nothing in this Agreement obligates the Data Provider to enter into any further agreement or arrangements, or furnish any Confidential Data, other information, or materials.

**10. Compliance with Law, Applicable Law**

The Data Provider and OODI agree to comply with all applicable laws and regulations in connection with this Agreement. The Data Provider and OODI agree that this Agreement shall be governed by the laws of the State of ABC, without application of conflicts of laws principles.

**11. Term of Agreement**

The parties may terminate this Agreement upon sixty (60) days' written notice to the other party. The terms of this Agreement that by their nature are intended to survive termination will survive any such termination as to Confidential Data provided, and performance of this Agreement, prior to the date of termination, including Sections 2, 3, 4, 5, 6, 7, 8, 9, 10, and 14.

**12. Use of Name**

Neither the Data Provider nor OODI will use the name of the other party or its employees in any advertisement or press release without the prior written consent of the other party.

**13. Definitions**

See APPENDIX E

**14. Indemnification**

StateIDS and Data Provider shall not be liable to each other or to any other party for any demand or claim, regardless of form of action, for any damages of any kind, including special, indirect, consequential or incidental damages, arising out of the use of the Data Provider's data pursuant to and consistent with the terms of this DSA or arising from causes beyond the control and without the fault or negligence of a Data Provider.

*[Remainder of page left intentionally blank, continue on subsequent page]*

**PARTY REPRESENTATIVES**

The Parties' contacts for purposes of this Agreement are:

For Provider:	For State's Office of Data Integration:
---------------	-----------------------------------------

IN WITNESS WHEREOF, the undersigned have executed this Agreement as of the Effective Date.

**STATE'S OFFICE OF DATA INTEGRATION**

**BY:**

\_\_\_\_\_  
NAME

\_\_\_\_\_  
TITLE

\_\_\_\_\_  
DATE

**PROVIDER**

**BY:**

\_\_\_\_\_  
NAME

\_\_\_\_\_  
TITLE

\_\_\_\_\_  
DATE

**Attachment A:  
High Value Data Asset Inventory**

Attachment A is a listing of variables that have been identified by the Data Provider as being important for using data as a strategic asset for inclusion within the StateIDS.

**SUGGESTED TEMPLATE FOR DATA THAT CAN BE SHARED:**

Suggestion to include 1 table per application/dataset.

Application/Dataset Name and Description:					
Data Repository where asset is contained:					
Function / Utilization:					
Frequency of Update for Source Data:					
Data Steward:					
Data Custodian:					
Data Owner:					
Protected Data, including PHI / PII:					
Deidentification guidelines:					
Data destruction guidelines:					
Relevant Legal restrictions of use:					
Notes:					
Ref #	Table name	Variable name	Attribute	Data type	Quality Indicator

Suggested Template for Data that Can Not Be Shared:

Include application / datasets / variables that cannot be shared

Application/Dataset Description:
Permissible use: Non permissible use:
Relevant statute / rule / reason:
Notes:

**Attachment B:**  
**State's Office of Data Integration**  
**Confidentiality Agreement**



**CONFIDENTIALITY:**  
Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description).

I, \_\_\_\_\_, hereby acknowledge that, with regard to a request for information through the Integrated Data System for the State (StateIDS) and the associated Data Sharing Agreement ("Agreement") between the State's Office of Data Integration (OODI) and \_\_\_\_\_ (Data Provider), I may acquire or have access to confidential information or personally identifiable information associated with residents.

Confidentiality Agreement Acknowledgment:

I understand that I may have access to data that is confidential under State or federal law. I will maintain the confidentiality of data in accordance with this agreement and applicable State and federal law as well as the requirements set forth by OODI. I understand that unauthorized access or disclosure may be a violation of State and/or federal law.

I will limit my access and use of the data to that which is minimally necessary to accomplish the Purpose set forth in this agreement.

I will keep any account credentials granted private. I will not share my account credentials with other users or any unauthorized individual. I will neither request nor use another person's account credentials, other credentials, or other unauthorized means to access data.

I will provide notice of any violations of this confidentiality agreement, including suspected and confirmed privacy/security incidents or privacy/security breaches involving unauthorized access, use, disclosure, modification, or destruction of data, including a breach of any account credentials. Notice shall be provided directly by phone and email to \_\_\_\_\_ within twenty-four (24) hours of the incident first being discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the Recipient shall report the incident within one (1) hour after the incident is first discovered.

I understand that my failure to abide by the terms set forth in this Confidentiality Agreement may result in consequences that include, but are not limited to, the immediate termination of my access and disciplinary action up to termination of my employment or contract.

By signing below, I affirm that I have read this Confidentiality Agreement and agree to be bound by the terms therein.

Executed:

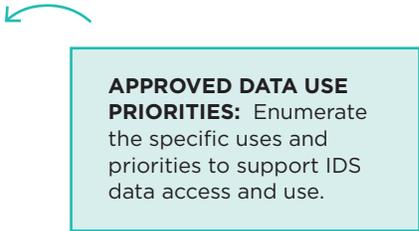
---

SIGNATURE	DATE
PRINTED NAME	ORGANIZATION NAME
PHONE	EMAIL

## Attachment C: Approved Data Use Priorities

**1) State's Office of Data Integration (ODI) will use data to further advance its mission to improve the health, safety, and well-being of all state residents by working toward the following goals:**

- a) Advance health equity by reducing disparities in opportunity and outcomes for historically marginalized populations across the state.
- b) Build a coordinated, and whole-person—physical, mental and social health—centered system that addresses both medical and non-medical drivers of health.
- c) Turn the tide on State's opioid and substance use crisis.
- d) Improve child and family well-being so all children have the opportunity to develop to their full potential and thrive.
- e) Support individuals with disabilities and older adults in leading safe, healthy and fulfilling lives.
- f) Achieve operational excellence by living our values—belonging, joy, people-focused, proactive communication, stewardship, teamwork, and transparency.



**APPROVED DATA USE PRIORITIES:** Enumerate the specific uses and priorities to support IDS data access and use.

### 2) General Permission to Access Data for Data Quality and Strategic Use Purposes

Unless otherwise specified by the Data Provider in Attachment A to this Agreement, the Data Provider agrees and authorizes Data Integration Staff and persons or entities performing activities on behalf of Data Integration Staff or Data Provider, to utilize the minimum necessary Data for both: 1) Data Quality Assessment and Improvement Activities; and 2) Operational Activities ("Data Quality and Strategic Use Purposes").

Permission to access the Confidential Data for Data Quality and Strategic Use Purposes is limited to Data Integration Staff and persons or entities performing activities on behalf of Data Integration Staff or the Data Provider, and strictly for OODI's Data Quality and Strategic Use Purposes, unless otherwise specified by the Data Owner under this Agreement in Attachment A to this Agreement.

Access and use of the Confidential Data specified by the Data Owner in Attachment A to this Agreement is strictly limited to purposes directly connected with the administration of specific programs and specific purposes where required or otherwise limited by law or policy.

### 3) Division / Office / Agency Specific Priorities

[Outline priorities of the Data Owner for data access and use. This could include linking to a strategic plan, listing routine data integration use cases currently underway, and/or including a co-created learning agenda.]

**Appendix I: DUL Checklist**

¶	Question	Additional Information
1	Preamble	Introductory paragraph that identifies the type of agreement, the parties to the agreement, the general intent of the parties. May contain “WHEREAS” statements. The preamble might also contain the legal names and contact information of the parties.
2	Definitions	Define key terms in this agreement. Include even standard terms if there is potential for misinterpretation.
3	Financial Understanding	If funds are to be obligated under the agreement, the financial arrangements to all parties must be clearly stipulated. If no funds are obligated under the agreement, a statement should be included which makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement. If the agreement results in the exchange of money between agencies, state the estimated cost or costs not to exceed, term of payments, and dispute resolution conditions.
4	Permitted Data Use License: Approved Use and Data Elements	Define the scope and process of using data, as well as data transfer protocols. Specify the uses which the other agency can use administrative records. Consider whether the data subject to these administrative records will be made available to researchers or to the public. Are restricted data use licenses implicated? What kind of public disclosures need to be made?
5	Data Ownership and Accuracy	<p>Should set forth the ownership rights and responsibilities for the data that is subject to the DUL (including responsibility for veracity, security, updates, and responding to compliance violations). Should also specify the custodian of the shared data (including contact information). This person should be personally responsible for carrying out the provisions of this agreement (including security controls, disclosure protocols, access protocols, etc.).</p> <p>May include disclaimer language such as: “Parties to this DUL do not make any representation or warranty, express or implied, as to the accuracy or completeness of any furnished information or other due diligence materials, and no Party, or any of its directors, trustees, officers, employees, shareholders, owners, affiliates, representatives, or agents, has or will have any liability to any other Party or person resulting from any reliance upon or use of, or otherwise with respect to, any furnished information or other due diligence materials.”</p>
6	Data Transfer	Describe how the data will be securely transferred or accessed.
7	Safeguarding Data	Describe the policies and procedures to protect the confidentiality and safety of data. Discuss specific protocols for physical and virtual/ electronic security—be specific about proposed security arrangements and demonstrate full understanding of applicable statutes, regulations and traditional practices; how parties can inspect security arrangements for the purpose of confirming the user is in compliance with data security procedures and requirements specified by the agreement.
8	Data License Authorized Personnel	Address record usage, duplication, and re-disclosure restrictions: limitations on the access to, disclosure, and use of information. Who can access the data? Limitations on identifiable data? Where can research/ analysis be done?

## Appendix I

9	Accountability: Unauthorized Access, Use, or Disclosure	<p>Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data. Describe the responsibilities for notification by points of contact of each party to the DUL, any criminal/civil penalties that may apply for unauthorized disclosure of information, indemnification language and limitations of liability and any liquidated damages for breach of agreement if applicable.</p> <p>May want to specify Parties negotiating an agreement often make an explicit agreement as to what each party's remedy for breach of contract shall be.</p>
10	Data Use License Reporting Requirements	<p>Describe protocols for providing notice of dissemination of findings from data analyses. If the parties are releasing any documents or research related to the exchange of administrative data, specify the subject matter, rights, and responsibilities pertaining to the public use of data. Data citations should also be discussed here as well as definitions for documenting data linking and cleaning process.</p> <p>May also wish to include provisions for an evaluation of the Data Licensee process and use of the shared data, if desired.</p>
11	Data Retention and Destruction	<p>Detail what records shall be retained for the use contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained. Specify what records should be destroyed and a timeline for the destruction of the data.</p>
12	Term & Termination	<p>State specific start and end dates of the DUL. If the completion date is not known and the period of the agreement is expected to stretch over a number of years, the completion date may be listed as indefinite. Should also contain a provision whereby each party may terminate the agreement with a specified time frame.</p>
13	Indemnification	<p>Specify whether the parties will indemnify or defend one another for breach or loss.</p> <p>*Note that this is a mutual indemnity, where each party bears the cost and risk of their own actions; there might be situations where parties may want to shift the risk to the party using the data.</p>
	Exhibit 1: Data Use License Request Form	<p>Form by which Data Recipient requests a DUL. Form specifies requested data, data output, purpose and use.</p>
	Appendix 1: Certification of Data Use License Completion & Destruction of Data	<p>Certification that confirms that access to data has been rescinded and confirms data has been destroyed.</p>

## Appendix J: Annotated DUL Template Between IDS Lead Agency and Data Licensee (or Recipient)

### Data Use License

#### 1. Preamble

This Data Use License (“DUL”) is entered as of \_\_\_\_\_ (the “Effective Date”) by and between the State’s Office of Data Integration (“ODI”) in its capacity as the Integrated Data System of the State (StateIDS) Lead Agency and \_\_\_\_\_ (“Data Recipient”).

This DUL addresses the conditions under which ODI will disclose, and the Data Recipient may use, the Licensed Data as specified in this DUL and/or any derivative file(s) (collectively, the “Licensed Data”). The terms of this DUL are consistent with those in the StateIDS Enterprise Memorandum of Understanding (EMOU) and can be changed only by a written and signed amendment to this DUL or by the parties terminating this DUL and entering a new DUL, after approval by the StateIDS Data Oversight Committee. The parties agree further that instructions or interpretations issued to the Data Recipient concerning this DUL, or the Licensed Data specified herein, shall not be valid unless issued in writing by the ODI signatory to this DUL.

#### 2. Definitions

See APPENDIX E

#### 3. Financial Understanding

If applicable, the Data Recipient agrees to pay a fee of \$\_\_\_\_\_ to be invoiced upon secure transfer of the Licensed Data. Payment is due within 30 days of receipt of invoice.

#### 4. Permitted Data Use License: Approved Use and Data Elements

This DUL pertains to the Data Use License Request Form entitled: \_\_\_\_\_. This Data Use License Request was approved by the Data Oversight Committee on \_\_\_\_\_ (Date) and the approved Data Use License Request Form is attached and incorporated into this DUL as Exhibit 1.

The approved Data Use License Request Form details the permitted use of the Licensed Data as well as the approved data elements to be included in the Data Use License. This DUL pertains only to the use and data elements identified in this approved Data Use License Request Form, attached as Exhibit 1.

The Data Recipient shall not use the Licensed Data for any purpose independent of, separate from or not directly connected to the purpose(s) specifically approved by the StateIDS Data Oversight Committee.

#### 5. Data Ownership and Accuracy

Data Recipient acknowledges that Data Recipient has no ownership rights with respect to the Licensed Data, and that the Data Recipient may only receive and use the Licensed Data for the purposes approved by the StateIDS Data Oversight Committee.

The Licensed Data is current as of the date and time compiled and can change. The Data Providers do not ensure 100% accuracy of all records and fields. Some data fields may contain incorrect or incomplete data. ODI and Data Providers cannot commit resources to explain or validate complex matching and cross-referencing programs. Data Recipient accepts the quality of the data they receive. Questions related to Licensed Data completeness (i.e., approved data elements in the attached Exhibit 1 were received) or matching accuracy shall be sent to the StateIDS Director within sixty (60) days of receipt. Licensed Data that has been manipulated or reprocessed by the Data Recipient is the responsibility of the Data Recipient. ODI cannot commit resources to assist Data Recipient with converting data to another format or answering questions about data that has been converted to another format. Additional issues with the Licensed Data shall be noted in the Regular Data License Report(s) (described in Section 10 below).

**6. Data Transfer**

Licensed Data will be transferred to the Data Recipient through a Secure File Transfer Protocol (SFTP) provided or approved by OODI. The Data Recipient will be provided secure access to the SFTP and will be allowed to download the Licensed Data file(s) for a limited period of time after which access to the SFTP will be removed.

**7. Safeguarding Data**

Security Controls. The Data Recipient shall implement and maintain the data security controls specified in the Data Use License Request Form (attached as Exhibit 1) that has been approved by the StateIDS Data Oversight Committee.

Re-Disclosure of Data. Data Recipient shall not use the Licensed Data for any purpose beyond that specified in Exhibit 1, attached hereto. Furthermore, Data Recipient shall not use the Licensed Data in an attempt to track individuals, link to an individual's data from other data sources, determine real or likely identities, gain information about an individual or contact any individual. Re-disclosure of data shall result in the immediate suspension of the Data Use License and possible termination of the Data Use License by the StateIDS Data Oversight Committee. Furthermore, individuals engaging in re-disclosure of data will not be approved Authorized Personnel on future requests.

Data De-identification Policy. The Data Recipient agrees that any use of Licensed Data in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) concerning the specified purpose must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than \_\_\_ observations may be displayed. This is the most stringent cell size allowable among the Data Providers for the DLR specified in this DUL. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than \_\_\_ observations. Individual level records may not be published in any form, electronic or printed. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than \_\_\_ observations cannot be identified by manipulating Licensed Data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through this Licensed Data. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

**8. Data Use License Authorized Personnel**

Any person or entity that processes or receives the Licensed Data and its agents must be obligated, by contract, to adhere to the terms of this DUL and agree to follow the data security controls approved in the attached Exhibit 1, prior to being granted access to Licensed Data. The following named individuals, and only these individuals, will have access to the Licensed Data. The Data Recipient will submit a Data Use License Change Request to the StateIDS Director when an individual no longer has access to Licensed Data. The Data Recipient will obtain written approval from the StateIDS Director for additions to this list prior to granting access to Licensed Data.

Name	Role	Organization

**9. Accountability: Unauthorized Access, Use, or Disclosure**

Data Recipient shall take all steps necessary to identify any use or disclosure of Licensed Data not authorized by this DUL. The Data Recipient will report any unauthorized access, use or disclosure of the Licensed Data to OODI via the StateIDS Director within two business days from learning or should have learned of the unauthorized access, use, or disclosure. In the event that OODI determines or has a reasonable belief that the Data Recipient has made or may have made use or disclosure of the Licensed Data that is not authorized by this DUL, OODI may, at its sole discretion, require the Data Recipient to perform one or more of the following, or such other actions as OODI, in its sole discretion, deems appropriate:

- a. promptly investigate and report to OODI the Data Recipient's determinations regarding any alleged or actual unauthorized access, use, or disclosure;
- b. promptly resolve any issues or problems identified by the investigation;
- c. submit a formal response to an allegation of unauthorized access, use, or disclosure;

- d. submit a corrective action plan with steps designed to prevent any future unauthorized access, use, or disclosures; and
- e. return all Licensed Data or destroy Licensed Data it has received under this DUL.

The Data Recipient understands that as a result of OODI's determination or reasonable belief that unauthorized access, use, or disclosures have taken place, OODI may refuse to release further Licensed Data to the Data Recipient for a period of time to be determined by OODI, in its sole discretion.

## 10. Data Use License Reporting Requirements

**Regular Data Use License Reports.** Data Recipients must submit Regular Data Use License Reports to the StateIDS Data Oversight Committee, annually or at the midterm point of the Data Use License cycle, whichever comes first. The report shall be a standard form automatically distributed by the StateIDS Director or support staff and shall require:

- a. Summary of progress to date
  - How data use is informing policy or practice
  - Description of anticipated and unanticipated findings
  - Description of challenges encountered and how they are being resolved
- b. Dissemination materials and key findings to date
- c. Funding source (if applicable)

**Change Requests.** Data Recipients will initiate, when necessary, a Data Use License change request. Minor Change Requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the StateIDS Director. Major Change Requests (e.g., additional research questions; change in organization using data; change in dissemination plan) will be reviewed by the StateIDS Data Oversight Committee.

**Key Findings and Interpretations Release Request.** Data Recipients are required to share Data Use License findings to the StateIDS Data Oversight Committee prior to any public release. Data Recipients shall submit key findings and interpretations in a standard format provided by the StateIDS Director or support staff. StateIDS Data Oversight Committee members shall confirm in writing, via a standard form provided by the StateIDS Director, that key findings have been reviewed and are ready for release. The StateIDS Data Oversight Committee members can request review of specific dissemination materials (e.g., presentations, publications).

**StateIDS Acknowledgement.** All publicly-released materials resulting from this DUL shall include the following acknowledgement: "This work would not be possible without data provided by the State Integrated Data System in the State's Office of Data Integration. The findings do not necessarily reflect the opinions of the State's Office of Data Integration or the organizations contributing data."

**Final Publication(s).** The Data Recipient shall provide the StateIDS Director with an electronic copy of all published work associated with this DUL within 30 days of publication.

## 11. Data Retention and Destruction

The Data Recipient agrees to destroy all Licensed Data by the approved Data Use License end date, in accordance with the methods established by the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS). The Data Recipient may request an extension of the Data Retention Period by submitting a written request that includes justification to the StateIDS Data Oversight Committee via the StateIDS Director. This extension request must be submitted 30 days prior to the Data License end date.

When retention of the Licensed Data is no longer justified, the Data Recipient agrees to destroy the Licensed Data and send a completed "Certification of Data Use License Completion & Destruction of Data" form (Appendix 1 to this Agreement) to OODI via the StateIDS Director by the approved Data License end date. The Data Recipient agrees not to retain any Licensed Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and Licensed Data are destroyed unless the StateIDS Data Oversight Committee grants written authorization. The Data Recipient acknowledges that such date for retention of Licensed Data is not contingent upon action by OODI.

**12. Term and Termination**

By signing this DUL, the Data Recipient agrees to abide by all provisions set out in this DUL. This DUL will become effective upon the last date of execution by OODI and the Data Recipient to this DUL. Unless terminated sooner pursuant to Sections 6 and 8 above, this DUL will remain effective in its entirety until the completed "Certification of Data Use License Completion & Destruction or Retention of Data" has been received by the OODI.

**13. Indemnification**

StateIDS and Data Provider shall not be liable to each other or to any other party for any demand or claim, regardless of form of action, for any damages of any kind, including special, indirect, consequential or incidental damages, arising out of the use of the Data Provider's data pursuant to and consistent with the terms of this DUL or arising from causes beyond the control and without the fault or negligence of a Data Provider.

*[Remainder of this page left intentionally blank]*

**14. Signatures**

The effective date of the DUL shall be \_\_\_\_\_, 20 \_\_\_\_.

The DUL will remain in effect until \_\_\_\_\_, 20 \_\_\_\_.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be executed by their duly authorized representatives.

[OODI SIGNATORY]

\_\_\_\_\_ Dated: \_\_\_\_\_

TITLE, STATE'S OFFICE OF DATA INTEGRATION

[DATA RECIPIENT NAME]

\_\_\_\_\_ Dated: \_\_\_\_\_

DATA RECIPIENT TITLE AND ORGANIZATION

# EXHIBIT 1

## Data Use License Request Form, Research Purposes

Internal Use. Request #:

### 1. Does this research request align with data use priorities?

- Yes  No  Unsure

### 2. Has this study been approved by an Institutional Review Board?

- Yes, an IRB approved this study and a copy of the application, materials, and determination letter is attached.  
 No, an IRB has not approved this study, but I have submitted an application (attached).  
 Other (please specify):

### 3. Requestor's Contact Information

Name of Requestor:

Title / Role:

Institution:

Phone number:

Email:

I have read and agree to the Terms and Conditions of Data Use Yes

My CV or resume is attached to this request Yes

I understand that a Data Use License will need to be executed prior to receipt of requested data. I understand that the Data Use License must be signed by an individual at my institution with signatory authority. Yes

I understand that a fee may be charged for fulfilling this research data request. If applicable, I will be provided with a fee estimate prior to the fulfillment of request. Yes

### 4. Description of the Requested Data

How often does the Data Recipient want to receive the data?

- This will be a one-time provision of data  
 Daily  Weekly  Monthly  Quarterly  Annually  
 Other

What is the date by which you would like to receive the requested data? (e.g., by 6/15/22)

By date:

Please list the data elements that are being requested in the table below.

Time period	Data element	Description/Notes	Data Source (INTERNAL)
E.g., from 3/1/2022 to 10/1/2022	E.g., total COVID-19 test results	E.g., total count of COVID-19 test results (negative, positive, undetermined)	

(please add rows as needed)

**5. What is your requested data output?  
Please note that informed consent or waiver is required for release of identifiable data.**

**a. Aggregate, Data Use Agreement may be required**

- Aggregated data by specified subgroup / population / geography from a single agency
- Aggregated data by specified subgroup / population / geography from multiple agencies
- Linked and aggregated data by specified subgroup / population / geography from multiple agencies

**b. Row level, Data Use Agreement may be required**

- Row level data that has been de-identified
- Row level data with identifiers

**c. Integrated Row level, Data Use Agreement may be required**

- Row level data without identifiers to link with another data source owned by state agency linked within OODI data infrastructure
- Row level data with identifiers, linked with another data source owned by state agency linked within OODI data infrastructure
- Row level data with identifiers to link with another data source not owned by state agency, linked within OODI data infrastructure
- Other (please specify):

**6. If you have requested identifiable data,**

- I have obtained written informed consent and if applicable, HIPAA authorization, from every person whose data is included in the requested data set. I am able to provide OODI with copies of informed consents and HIPAA authorizations upon request.
- An IRB has approved a waiver of HIPAA authorization for this request in accordance with 45 CFR § 164.512, attached.
- An IRB has approved a waiver of informed consent for this project, attached.

**7. What is the purpose of this request? What are you trying to understand better? What generalizable body of knowledge are you contributing to? How will this serve the residents of State ABC?**

**8. Please describe the security characteristics of the location where the OODI data will be stored (e.g., physical and technical safeguards, encryption applied to transmissions as well as files at rest, etc.).**

**9. How will you address issues of racial equity and bias within this research?**

**10. How will you ensure that privacy risks of re-disclosure or re-identification are mitigated?**

**11. How will the findings from this research be used and disseminated?**

Data Recipient Agreement

I have reviewed and agree to the OODI Terms and Conditions of Data Use. I agree to regularly communicate with OODI Data Office Staff and promptly respond to any questions or concerns. I agree to only use data as described in this request. I agree to report promptly to Data Integration Staff all problems or any incident with possible adverse events involving OODI data.

---

Signature of Data Recipient (electronic signature is permissible)

Signature Date

*\* Note that a signed Data Use License may also be executed prior to the release of any data pursuant to this request.*

Data Use License Information, if applicable

**1. What is the desired DUL effective date?**

**2. Is there a funding, publishing, or other deadline related to the desired effective date? If yes, please explain:**

**3. Names of principal research and co-investigators, as well as anyone else who will have access to the data:**

Name: \_\_\_\_\_ Role: \_\_\_\_\_

**4. Expected project completion date:**

**5. Name and title of the authorized signatory official who will sign the DUL:**

---

NAME

TITLE

---

EMAIL

---

MAILING ADDRESS

**APPENDIX 1**

Certification of Data Use License Completion & Destruction of Data

---

DATE OF DATA USE LICENSE COMPLETION:

---

DATE OF REMOVAL OF DATA ACCESS AND/OR DATA DESTRUCTION:

---

PERSON PROVIDING OVERSIGHT FOR REMOVAL OF ACCESS/DESTROYING DATA:

---

TITLE:

AGENCY:

---

PHONE NUMBER:

E-MAIL:

---

TERM OF DATA USE LICENSE:

DATA USE LICENSE NUMBER:

**I confirm that, as applicable, all access to Licensed Data permitted pursuant the above referenced Data Use License has been rescinded and all Licensed Data received under the above referenced Data Use License has been destroyed, including data held and/or accessed by all Data Recipient staff, as defined under the Data Use License.**

By signing below, I confirm that Licensed Data was destroyed and access to Licensed Data was rescinded, as applicable, on Click here to enter text. This destruction was carried out as follows:

1. Information in electronic format was destroyed in compliance with the minimum standards set out in the Guidelines for Media Sanitization (NIST 800-88) guideline issued by the US Dept of Commerce (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>).
2. Information in hardcopy or printed format was destroyed using a cross-cut shredder or an equivalent destruction method.

---

SIGNATURE

---

NAME

---

TITLE

AGENCY



**Actionable Intelligence for Social Policy**

University of Pennsylvania

3701 Locust Walk, Philadelphia, PA 19104

215.573.5827 | [www.aisp.upenn.edu](http://www.aisp.upenn.edu)