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

VERSION 2.0

Actionable Intelligence for Social Policy, Expert Panel Report

Authors

Deja Kemp, JD, and Amy Hawn Nelson, PhD

Contributors

Della Jenkins, Jessie Rios Benitez, Isabel Algrant, TC Burnett, Kristen Egoville, Sharon Zanti, Mary Beth Cole, Emily Berkowitz, Dennis Culhane

NOVEMBER 2025

AISP

Acknowledgments

Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration was originally published by Actionable Intelligence for Social Policy (AISP) in 2022 to provide practical legal guidance for cross-sector data collaboration. Since then, both the legal landscape and the needs of the field have continued to evolve. This 2025 update reflects those changes, incorporating new resources, expanded analysis, and lessons learned from ongoing conversations with legal, policy, and data practitioners across the country. As we continue to navigate complex legal questions in a shifting environment, we are grateful to the many individuals and organizations who have contributed their time, expertise, and lived experience to strengthening this resource.

This resource builds upon AISP's Introduction to Data Sharing and Integration (updated 2025) and AISP's Quality Framework for Integrated Data Systems (2021). It also draws from Legal Issues for IDS Use: Finding a Way Forward (2017), an AISP expert panel report authored by John Petrila, Barbara Cohn, Wendell Pritchett, Paul Stiles, Victoria Stodden, Jeffrey Vagle, and Mark Humowiecki.

We also recognize Samuel Kohn and Paul Hogle, members of our AISP Legal Advisory Workgroup, and Scott Shuchart and Naomi Gilens, from Protect Democracy, who provided invaluable review of this resource. 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 first 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

Suggested citation: Kemp, D., Hawn Nelson, A., Jenkins, D., Rios Benitez, J., Algrant, I., Burnett, T.C., Egoville, K., Zanti, S., Cole, M.B., Berkowitz, E., Culhane, D. (2025). *Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration.* Actionable Intelligence for Social Policy. University of Pennsylvania.

Table of Contents

Table of Contents

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, state longitudinal data systems, 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 in the establishment of cross-sector data integration, which, for the 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 Quality Framework for Integrated Data Systems 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*[1] as a primer on the basics of using, sharing, integrating, and using administrative data.

How to use this document

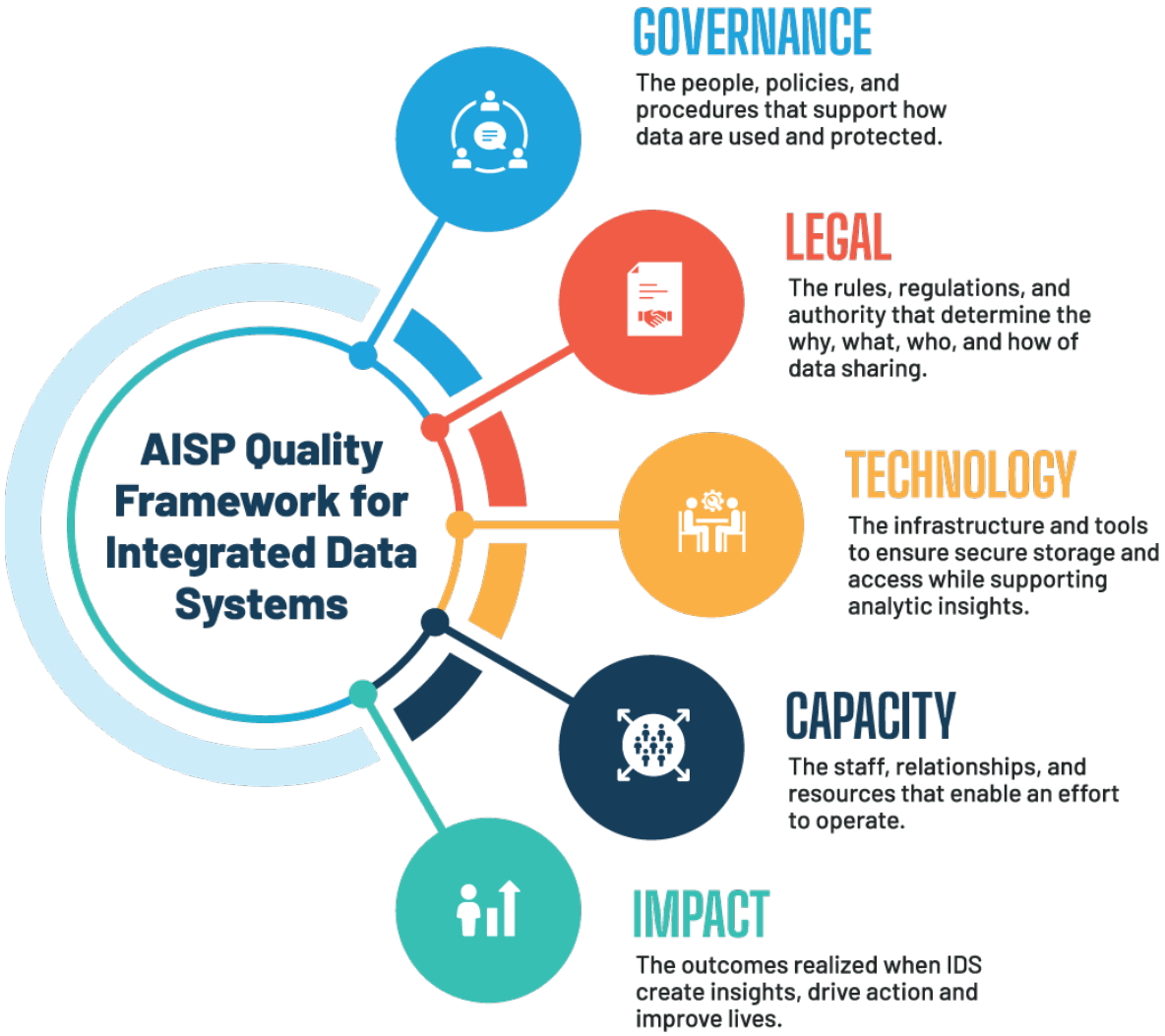
This resource is based on the experience of practitioners who, collectively, have decades of experience developing strong data governance and legal frameworks to support cross-sector data integration. Each section frames out key concepts and then provides prompts for discussion to move toward action.

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 that 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

Although every data integration effort is different, we have identified five key components of quality that set successful data integration efforts apart. 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 graphic provides an overview of the five components that make up AISP's Quality Framework for IDS.[2]

[1] See Hawn Nelson, A., Algrant, I., Jenkins, D., Rios Benitez, J., Kemp, D., Burnett, T.C., Zanti, S., Culhane, D. (2025, 2020).
[2] See Jenkins, D., Berkowitz, E., Burnett, T., Culhane, D., Hawn Nelson, A., Smith, K., and Zanti, S. (2021).



Working with Legal Counsel

Lawyers play a critical role in ensuring that data sharing, use, and access practices are legally compliant, ethically sound, and aligned with community expectations. In the context of IDS, legal counsel should be engaged early and often. Legal counsel can help:

- Provide advice and guidance on state and federal laws that govern the collection, use, and sharing of data
- Evaluate and provide counsel on the legal risks and potential liabilities associated with data sharing and integration
- Draft, review, and negotiate data sharing agreements (DSAs), memoranda of understanding (MOUs), or other data agreements or contracts for sharing data
- Develop governance and accountability structures that ensure ongoing compliance and transparency, such as data access protocols, audit processes, and breach response plans
- Defend organizations from lawsuits and enforcement actions that could arise from data sharing and integration

Lawyers also play a critical role throughout the entire data life cycle. Their involvement is especially important in the later stages, where questions often arise about data retention, reuse, ownership, and destruction. Legal counsel can help ensure that disposition plans comply with relevant laws and regulations, including data retention requirements, records management policies, and privacy obligations. They also assist in clarifying contractual obligations, such as whether data must be returned or destroyed at the end of a project, and can help negotiate terms that protect against unintended redisclosure or unauthorized future use. The table on the next page gives examples of how legal professionals can support each stage of the data life cycle.

Stage of Life Cycle	Role of Lawyer
Planning	Help identify legal risks early and shape project scope and legal frameworks accordingly
Data Collection	Draft or review consent language (if applicable) to ensure it is legally valid, understandable, and consistent with intended uses
Data Access	Determine who can legally access the data and under what conditions (e.g., internal users, governmental actors, contractors, researchers)
Data Analysis	Ensure that data use remains within the legal scope authorized by governing agreements and consent terms
Use of Algorithms & Artificial Intelligence	Evaluate whether the use of AI tools introduces legal risks related to bias, disparate impact, or due process concerns
Reporting & Dissemination	Review planned publications or outputs to ensure that they comply with data sharing agreements and privacy protections

In sum, building strong, collaborative relationships with legal counsel enables data efforts to move forward with clarity and confidence.

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?" While this is fundamental, we acknowledge that it is also the lowest bar. To ensure that use is both legal and ethical, we strongly encourage you to grapple with broader considerations to help you decide, together with your interest holders, whether and how to move forward with data integration.

We recommend asking the same four questions throughout all stages of this work:[3]

1. Is it legal?	1. Is it ethical?	3. Is it a good idea?
What legal authority is in place to use these data? Are there federal or state statutes that prevent or constrain this data access or use? What are the specific state and federal law requirements enabling data sharing?	Do the benefits outweigh the risks, particularly for groups historically marginalized by discriminatory systems?	What action can be taken as a result of this data use? What can reasonably be changed or improved based upon this analysis? Is this a priority among marginalized populations and/or individuals included in the data system?
4. How do we know and who decides?		
This is typically determined by agency-involved legal counsel.	This is typically determined by a data governance group, during the review process for data requests, that should include a variety of partners, those "in" the data and users of the data.	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.

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

[3] See Hawn Nelson, A. & Zanti, S. (2023).

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. Although 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 the following: authorizing legislation that grants authority to an office or agency to lead cross-agency data sharing;[4] 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. Importantly, consent may be another legal basis for sharing and using data when no statutory, regulatory, or contractual authority applies. Common data sharing contracts include a Memorandum of Understanding (MOU), Data Sharing Agreement (DSA), Data Use License (DUL) or Agreement (DUA), 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.

Here are several examples of common legal authority:

- Executive order to require data sharing to address a specific policy priority

  Examples: State of Indiana, Executive Order 17-09; State of Pennsylvania, Executive Order 2016-07; Federal Executive Order 14243

- Authorizing legislation for an agency or department that grants authority to an office or agency to lead cross-agency data sharing

  Examples: Indiana Law, IC 4-3-26, creates the Management Performance Hub, an executive agency charged with supporting cross-sector data integration of state agencies (the executive order cited above was a precursor to the legislation); consolidation of Health & Human Services Agencies facilitates data sharing, e.g., North Carolina Department of Health and Human Services (NCDHHS legislation), Rhode Island Executive Office of Health and Human Services (RIEOHHS legislation)

- Legislation specific to data use

  Example: Massachusetts Law, Chapter 55, which permits analysis of administrative data to support policy decisions to end the opioid epidemic

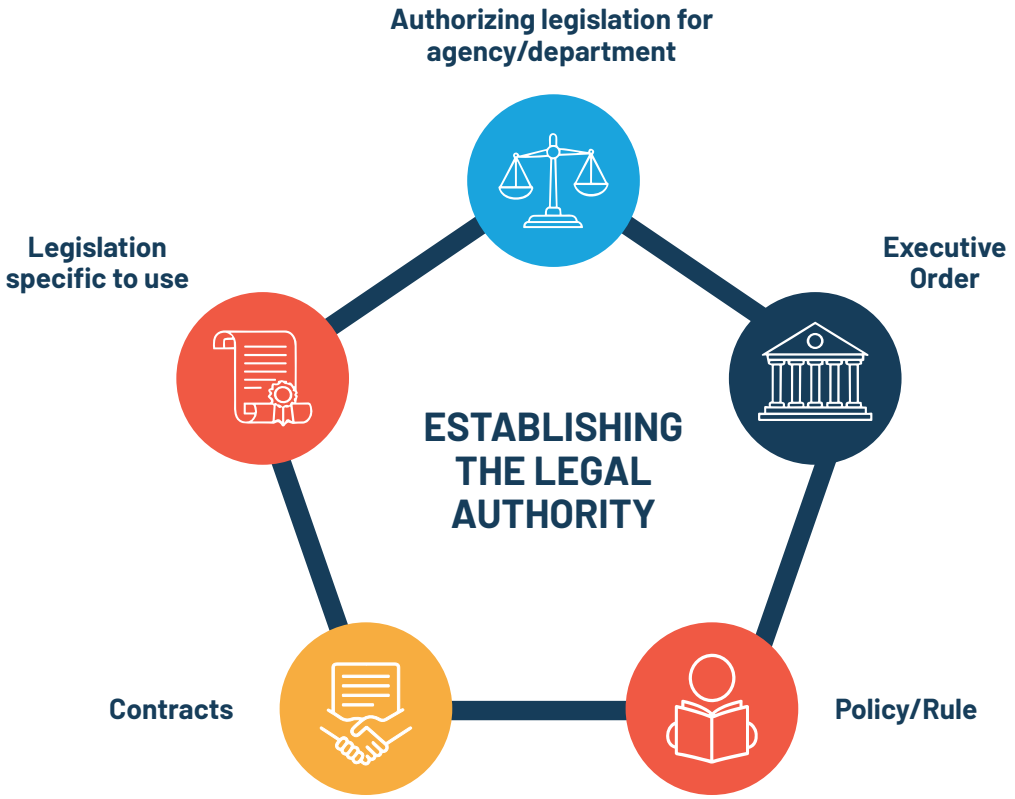
- Policy or rule

  Example: North Carolina rule, 10A NCAC 41A .0406, stipulating that a release is required for immunization records to certain educational institutions

- Contracts

  Example: State of Iowa, MOU for Early Childhood Integrated Data System, which provides the framework for multi-body governance across participating agencies

[4] See Zanti, S., Jenkins, A., Berkowitz, E., Hawn Nelson, A., Burnett, T.C., & Culhane, D. (2021).



Federal statutes and regulations relevant to data sharing and integration include the following: the Privacy Act of 1974,[5] the Health Insurance Portability and Accountability Act[6] (HIPAA), 42 CFR Part 2,[7] and the Federal Education Rights and Privacy Act[8] (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-D*.[9]

The Role of Consent

Consent can also provide a basis of legal authority. 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. The default rule is that identifiable information cannot be shared or disclosed unless consent is obtained or an enumerated purpose or exception exists. There are many considerations regarding whether enumerated purposes and exceptions apply, and sometimes there is no clear answer. We strongly recommend that any decisions around consent be carefully considered with a variety of interest holders through data governance processes. In general, consent is not usually required for research, evaluation, and planning efforts using public agency data, provided individual identifiers will not be seen or used by analysts. This is not the case for privately held data, such as data from community-based organizations. 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)).

5 See Kemp, D. (2025).
6 See Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023).
7 See Kemp, D. (2024).
8 See Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023).
9 For a discussion on Tribal authority, see Centers for Disease Control and Prevention & Office for State, Tribal, Local and Territorial Support (2024, May 16).

For more on consent, see *Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration*.[10] We also 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[11]
- World Economic Forum, *Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction*, 2020[12]
- Office of the National Coordinator for Health Information Technology, *Meaningful Consent Overview*, 2018[13]
- The Sequoia Project, *Moving Towards Computable Consent: A Landscape Review*, 2025[14]

For a sample consent form, see *Appendix N.*

Access

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

Open Data	Protected Data	Unavailable Data
Data that can be shared openly, either at the aggregate or individual level, based on state and federal law. These data often exist in open data portals.	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 state or federal law, lack of digital format (paper copies only), data quality, or other concerns.

Open data are publicly available and can generally be used without restriction. They are often de-identified and released to promote transparency, innovation, or research. These are examples of open data:

- Aggregated public school district performance reports
- Census tract–level demographic statistics from the U.S. Census Bureau
- Data that can be retrieved via a public records request
- Publicly released labor market or unemployment rates

Even open data can be misused (e.g., through re-identification), so ethical and privacy considerations still apply.

10 See Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023).
11 See Data Across Sectors for Health & The Network for Public Health Law (2018).
12 See World Economic Forum (2020).
13 See Office of the National Coordinator for Health Information Technology (2018).
14 See The Sequoia Project (2025).

Protected data include personally identifiable information (PII) or data governed by specific legal requirements. They can be shared under certain conditions, but only with appropriate safeguards and legal authority. These are examples of protected data:

- Individual-level K-12 student records (protected by FERPA)
- Substance abuse disorder records (protected by 42 CFR Part 2)
- Addresses and income information from housing authority databases
- Data shared under data use agreements with limitations on redisclosure

Protected data require clear legal basis, data use agreements, and sometimes consent.

Unavailable data are data that cannot be shared or may be too sensitive or high-risk to share, even if legally permissible. These are examples of unavailable data:

- Data about individuals who have opted out of sharing
- Juvenile court records that are sealed or expunged
- Identifiable tribal health data shared without tribal approval
- Victim or survivor data protected under the Violence Against Women Act or state confidentiality laws
- Data subject to legal privilege (e.g., attorney–client communications, litigation files, confidential personnel files)
- Data stored on a corrupted server without appropriate backup
- Data with significant quality issues

These data types often require special handling or additional legal consultation, or are simply off-limits.

Classifying agencies' high-value data assets 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.

Positive Practice:

CT Public Act 19-153 mandated the creation of an annual report, *Legal Issues in Interagency Data Sharing* (2025), and the CT Data Catalog, a high-value data inventory produced by Connecticut executive branch agencies and compiled by the Office of Policy and Management, is updated annually and available to credentialed Connecticut state employees. This metadata includes clarity around data access (specifying whether data are open, protected, or unavailable) and agency roles (specifying data owner and data steward).

Protecting Privacy

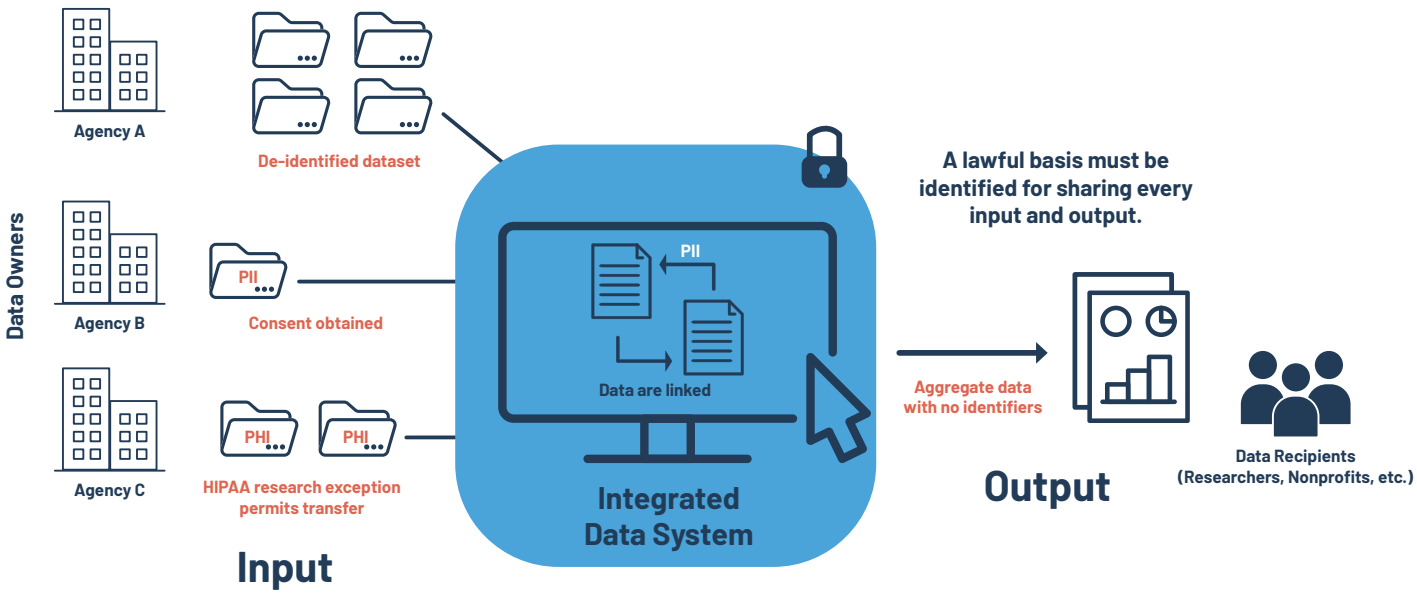
Privacy typically refers to an individual's right to control their personal information, while **confidentiality** refers to the obligation of those who collect or receive information to protect it from unauthorized disclosure. In the context of integrated data systems, privacy shapes what data may be collected and linked in the first place, while confidentiality governs how those data are stored, accessed, and shared once collected.

Legality of use depends on the purpose, how the data are released, and to whom. A helpful way to begin determining whether a transfer of data is legal is by thinking of data access in terms of **input privacy** and **output privacy**.

Input privacy typically refers to how data go "into" the IDS and involves protecting the identifiable information being contributed to a dataset. This might include limiting unnecessary data collection and applying de-identification or privacy-enhancing techniques.

Output privacy typically refers to how data come "out" of the IDS and focuses on protecting individuals from being re-identified or harmed through the results of data analysis, reports, dashboards, or other data products. Output privacy might include releasing findings in the aggregate, suppressing small cell sizes, applying privacy-enhancing techniques, and conducting privacy risk assessments before releasing findings.

As part of the legal analysis, agencies should identify a lawful basis for accessing each **input** (e.g., individual-level data contributed to a dataset) and each **output** (e.g., data products, reports, visualizations generated from the dataset). 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. The diagram below is illustrative:



In the context of the data life cycle, input privacy aligns with the collection and ingestion of data, where safeguards protect personal information as it enters and is linked within the system, while output privacy relates to the reporting and dissemination stages, ensuring that data products, publications, and shared findings do not compromise individual or community confidentiality.

The Role of De-identification in Input and Output Privacy

De-identification, which is often used as a strategy to protect individual privacy and reduce legal obligations by removing or obscuring direct identifiers in a dataset, plays a key role in managing both input privacy (how data enters a system) and output privacy (how data are shared externally). De-identifying data before use may reduce compliance burdens under laws like HIPAA or FERPA, but it can also serve as a mechanism for enabling broader external access or publication of data that would otherwise be restricted. This creates a potential tension: While the data may be legally sharable once de-identified, they may still carry ethical, reputational, or re-identification risks, particularly when datasets are rich, linked, or pertain to small or over-surveilled populations. Additionally, once data are de-identified they may become less useful for analytic purposes when linking across systems because key identifiers needed to connect records are removed or obscured. Practitioners must carefully assess not just whether data are de-identified, but whether their release aligns with the governance framework, the expectations of data subjects, and the principles of responsible data use.

The following table highlights some common scenarios and associated legal and privacy risks depending on the type of data output:

Data output	Explanation	Legal considerations	Privacy and 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.[15] 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 Business Associate Agreement (BAA) or DUL.	Less significant, but data are still potentially re-identifiable, especially with merged datasets.
Aggregated	Aggregated data by specified subgroup/population/geography.	May require a DSA and/or DUL and commitment to not attempt re-identification.	Generally less significant, but if data are aggregated by small geographies or small demographic groupings, they may be combined to identify individuals.[16]

[15] HIPAA and FERPA are discussed in detail in the section on Federal and State Laws.
[16] See North Carolina Department of Health and Human Services, *NCDHHS Operational Data Request Form* (2025).

Positive Practice:

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

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 will then allow you to determine legality.

WHY do you want to share and integrate data? For example, to: Track indicators at the population level Identify a target population Describe cross-enrollment patterns Identify geographic areas of greatest impact Evaluate program outcomes Improve services at the point of intervention Conduct mandated reporting	**WHO do you want to share it with, and who conducts the integration?** For example: Executive leadership Agency serving the same client Probation officers A community treatment provider A hospital emergency department A university-based researcher An agency-based analyst
WHAT type of data do you want to share and integrate? Is it open, restricted, or unavailable? For example: Information that does not identify individuals Information that does identify individuals Information that might identify a person Health information Educational records Housing status Demographics	**HOW will you share the data?** For example, provide: Aggregate counts at the block group level Credentialed access to source data Access to public-facing dashboard View-only access to data underlying a dashboard Edit access to data underlying a dashboard Row-level data with identifiers Row-level data without identifiers

The legality of the above scenarios depends on the legal framework used to facilitate integration and on the particulars of how data will be accessed and used. For example, sharing and using 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 users in crafting a data request that fulfills their need for data to inform policy making, while adhering to important laws that protect individuals' privacy. Remember, 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 whether 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.

One good example is from the Hartford Data Collaborative.[17]

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 services data integration stems from the sometimes parallel and opposing principles that data are a public good and that the right to privacy is intrinsic.

Research has a fraught history of inflicting harm, particularly on vulnerable and disenfranchised populations. This history—along with 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.

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 are 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 administrative data to inform policy making. Ethical data use requires more than checking a legal box; it requires engaging with the communities affected, being transparent about how data will be used, and weighing whether relying solely on legal authority is appropriate in light of potential harms.

[17] See CTData Collaborative: Hartford Data Collaborative, *Data Request Process* (n.d.).

One common approach to balancing oppositional values is rigorous review, which is why data governance (covered more in AISP Network Survey Series: Governance[18] 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.[19]

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 interest holders. 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 interest holders on an ongoing basis. Building relationships and social license is particularly important 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, 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.[20]

Developing clear processes that help discern 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 who did not receive formal schooling in the United States and is living in a multigenerational household with a variety of immigration statuses, located 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 risk and benefit across dimensions of identity and lived experience.

[18] See Berkowitz, E., Jenkins, D., Hawn Nelson, A. (2025).
[19] See U.S. Department of Health and Human Services & Office for Human Research Protections (2025, June 6).
[20] See Hawn Nelson, A., Zanti, S., Jenkins, D., Algrant, I., Rios Benitez, J., et al. (2025, 2020).

Ethics in a Time of Increased Federal Enforcement

These ethical considerations are especially urgent in the current national context, where (at the time of publication) administrative data collected for one purpose are reportedly being accessed by the federal government and repurposed for immigration enforcement, surveillance, or other punitive actions.[21] As Executive Order 14243 calls on federal agencies to break down data silos and increase data interoperability to improve service delivery, the stakes of ethical data use are rising. While the stated purpose of the executive order is to support more coordinated public programs, it also raises critical concerns about how shared data might be misused beyond its original purpose. High-profile examples of state data being used to support I.C.E. operations or other federal enforcement priorities erodes public trust and jeopardizes current and future data sharing initiatives.[22] For impacted communities, assurances about privacy or data being used "just for research" may feel hollow amid mounting and well-founded fears that data could be weaponized against them or their families. Ethical data sharing cannot be separated from these broader realities. IDS leaders and legal counsel must weigh not only what is legally permissible, but also what is contextually responsible and community-informed. This includes being transparent about potential government access, carefully limiting secondary use, and ensuring that governance decisions are not made in isolation from those most affected by data sharing.

Weighing Legal Risks of Data Integration

Attorneys have ethical and common law duties to competently and reasonably advise their clients on legal risks. A key factor in mitigating the legal risks associated with data integration is identifying the potential enforcement and litigation risks to your organization.

Although there are currently no reported court cases directly involving IDS,[23] legal decisions from other contexts—particularly those involving private entities—highlight real and specific risks that public agencies and data collaboratives must take seriously. These include the risk of unauthorized disclosure, where data are accessed or shared beyond the scope of consent or legal authority; misuse of data, including applying information in a way that causes harm to individuals or communities; and security breaches, where personal data are exposed as a result of inadequate safeguards.

For example, courts have held private entities liable for breach of contract and/or negligence claims for failing to implement adequate security measures under state consumer protection laws, and for using data in ways that exceeded the scope of user consent or contractual terms. In *In re Shields Health Care Group, Inc. Data Breach Litigation*, the court found that the provider violated contractual obligations implied in law to protect patients' private medical information.[24] Courts have also held governmental actors responsible for failure to protect private information. For example, in *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, the court held that the plaintiffs could sue for damages under the Privacy Act as a result of a data breach at the Office of Personnel Management (OPM) after OPM failed to implement adequate security safeguards.[25] Although these cases arise in contexts outside of IDS settings, they illuminate potential legal theories, such as negligence, breach of contract, and violations of statutory privacy rights, that could plausibly be asserted against public or quasi-public data systems under state law or constitutional claims. For more case law on potential causes of action, see *Appendix E*.

[21] See Joffe-Block, J., & Fowler, S. (2025, May 9).

[22] See Friedland, J. (2018, January 25); see also Center for Democracy & Technology & The Leadership Conference's Center for Civil Rights and Technology (2025, May 9).

[23] We are specifically referring to the absence of cases in which an IDS itself, or the governance entity that oversees it, has been named as party to litigation. For this reason, we do not include recent legal challenges against federal agencies, which, while relevant for understanding broader data use disputes, do not directly involve IDS as parties.

[24] *In re Shields Health Care Group, Inc. Data Breach Litigation*, 721 F.Supp.3d 152 (2024).

[25] *AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.)*, 928 F.3d 42 (2019).

On the other hand, 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.[26] Although lawsuits brought by private parties alleging breach of privacy under state law do exist, in general (and particularly with federal laws), only government regulators have legal standing to 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 partners are all risk mitigation strategies adaptable to state and federal requirements and compliance-centered practices.

Legal risk is not limited to regulatory noncompliance; it also encompasses reputational harm, political fallout, and community distrust. A thoughtful legal risk assessment should therefore consider not only whether a practice is technically lawful, but whether it is defensible, documented, and aligned with ethical commitments. Strong governance, clear legal agreements, and intentional community engagement are essential tools for mitigating these risks and building a legally and socially sustainable IDS. For a helpful example of a legal risk assessment, see this one created by the U.S. Department of Health and Human Services Office.[27]

The Emerging Role of AI in Integrated Data Systems

As artificial intelligence (AI) tools become increasingly embedded in public sector decision-making, IDS are entering a new era of opportunity and risk. AI and machine learning can help identify patterns across large datasets, support predictive modeling, and surface insights that may inform policy or resource allocation. However, applying AI in the IDS context raises serious concerns about transparency, accountability, bias, and equity. Without proper oversight and governance, these tools can reinforce or exacerbate existing harms, particularly for communities already over-surveilled or marginalized by public systems.[28] IDS leaders must carefully evaluate whether and how AI tools are used, ensure that algorithms are subject to public scrutiny, and include legal, ethical, and community perspectives in the design, deployment, and monitoring of automated decision-making systems. As AI capabilities evolve, so too must the governance frameworks that guide responsible and equitable data use. For more information on AI implementation in the IDS setting, see *A Toolkit for Centering Racial Equity Throughout Data Integration*[29] and *Building a Secure Generative Artificial Intelligence Environment for Research Use*.[30] For a helpful resource on managing bias in AI, refer to *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*.[31] For a helpful model on AI readiness, see *State of Indiana Standard AI Readiness Assessment Methodology*.[32]

[26] 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"). Note however, that although these federal statutes do not provide a private right of action, an aggrieved party can sue under the Administrative Procedure Act to challenge the federal government for violations of these acts. See *Compliant*, *Pallek v. Rollins*, No. 1:25-cv-01650 (D.D.C. filed July 16, 2025).

[27] U.S. Department of Health and Human Services (2025, January 15).

[28] See Hofmann, V., Kalluri, P. R., Jurafsky, D., & King, S. (2024, August 28).

[29] See Hawn Nelson, A., Zanti, S., Jenkins, D., Algrant, I., Rios Benitez, J., et al. (2025, 2020).

[30] See Rodriguez, B., El-Amin, A., Tiderman, L. (2024).

[31] See Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022, March).

[32] See Indiana Management Performance Hub (2025, May 29).

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 that data sharing is a good idea.

Data availability

As administrative data are collected for programmatic rather than analytic purposes, the actual data and the data quality can be 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 considerable, particularly in decisions about technology procurement, which can be a significant expense.

Action

Although possibilities for analytics are endless, many analyses are merely descriptions of problems we already know exist, and the analysis does not lead to productive action. There are countless reasons for such inaction. Rather than listing those possibilities, we instead ask you to focus on the most important question: **How could 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 and 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, which includes the people, policies, and procedures that support how data are managed, used, and protected.

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, can involve a separate set of policies and procedures, or can 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 the 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 their needs.

> 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**.

A good place to start is to develop a vision, mission, and guiding principles that together articulate 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 your purpose or use case for data sharing will inform the most appropriate legal framework for integration.

We distill the purpose of data sharing and integration into three categories: Indicators and Reporting; Analytics, Research, and Evaluation; and Operations and Service Delivery. The core purpose (or purposes) of your IDS will determine your governance, legal, technology, capacity, and impact. Possible approaches based on these purposes are highlighted in the following table.

	Indicators & Reporting	Analytics, Research, & Evaluation	Operations & Service Delivery
Purpose	Fulfills cross-agency planning and reporting requirements, and makes program outcomes more transparent.	Enables detailed cross-agency analyses of long-term outcomes and impact of service utilization.	Facilitates sharing of detailed cross-agency data to improve service delivery and care coordination.
Audience	Agencies, policymakers, the public	Researchers, evaluators, research and planning staff	Case workers, service providers
Example	A collective impact initiative wants to report on a set of common indicators through a publicly available dashboard.	City agencies want to understand how outcomes vary for clients based on demographic characteristics and participation in multiple programs.	County agencies want to link their data in near real-time to enable coordination for improved delivery and increased quality of care.
Governance	Minimal	Shared processes and clear parameters around access and use are required.	
Legal	Data may be publicly available already, or access and use may require a simple agreement to receive data in de-identified or aggregate format.	Data are protected and access generally requires multiple agreements to clearly outline permissible use.	Data are protected and data sharing agreements must outline parameters for role-based, credentialed access. Access may also require client consent and non-disclosure agreements.
Technology	Data are linked and anonymized, and results are reported at the aggregate level.	Data are linked, de-identified, and shared for a specific analytic purpose.	Data are identifiable and may include case notes to support client-level services.
Capacity	Costs and staffing are minimal.	Costs and staffing are moderate.	Costs and staffing are significant.
Impact	Increased transparency and potential for data to drive public discourse, advocacy, and collective impact.	Increased research capacity and potential for data to drive cross-agency coordination on policy and practice.	Increased care coordination, streamlined referrals, and potential for cross-program enrollment.

While the Quality Framework provides high-level considerations for the data system as a whole, the specific ways in which data are managed will also depend on the purpose for data integration. In the next table on page 23, we highlight key legal considerations with a focus on moving, receiving, ingesting, and releasing data.

	Indicators & Reporting	Analytics, Research, & Evaluation	Operations & Service Delivery
Privacy and Security	A lack of identifiers or small cell sizes means minimal risk of redisclosure, although data are potentially re-identifiable.	Minimal access to identifiable data and small group of approved users means that security requirements are essential but often procedural rather than technically advanced.	Many users and identifiable data mean that staff training, complex permissions, and audit trails are necessary.
Data Frequency	Data may be updated based on reporting cycles, often quarterly or annually.	Data may be updated periodically depending on availability and analytic requirements for approved projects.	Daily or real-time updates of entire client records may be required.
Data Quality Standards and Documentation	Data are evaluated for correctness, missingness, accuracy, and stability over time.	Data correctness, missingness, and accuracy are critical to support meaningful analysis.	Clients should have the opportunity to correct errors.
Legal Authority	When needed, legal authority is established through agreements, often simple two-party data sharing agreements.	Legal authority varies widely based on the management model. Legal agreements are complex and focus on the purpose for data use, specific terms and conditions governing data access, and roles and responsibilities of the data provider and data recipient.	Data sharing agreements often supplement authorizing legislation that enables data sharing for operational purposes.
Legal Framework	Data sharing agreements among data partners allow for data to be compiled, stored, and displayed by the managing entity.	Tiered data sharing agreements among partners allow data to be linked by the managing entity and shared with authorized external parties.	Data sharing agreements provide consent for the managing entity to link and share data with role-based access.
Terms of Access and Reuse	Data are available in pre-determined outputs (e.g., static report, dashboard) with limited ability to access or reuse row-level data.	Data sharing templates (e.g., data license request forms) streamline the process of granting access for approved use.	Data providers may ask individuals to provide consent to share data for use in service delivery as part of standard processes.

For more on moving from purpose to implementation in an SLDS-specific context, see an expanded discussion and version of this table in Defining Modern, User-Centered State Longitudinal Data System Design.[33] For more information on how purpose drives design within a data system, see AISP's Introduction to Data Sharing and Integration.[34]

[33] See Actionable Intelligence for Social Policy, Data Quality Campaign, Education Commission for the States, & West Ed's Data Integration Support Center (2025).

[34] See Hawn Nelson, A., Algrant, I., Jenkins, D., Rios Benitez, J., Kemp, D., Burnett, T.C., Zanti, S., Culhane, D. (2025, 2020).

Privacy-preserving technologies (PPTs) (also referred to as privacy-enhancing technologies or PETs) are technical approaches that minimize the 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 although 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, as shown, for example, in the case of Spotlight Tulsa.[35]

Management Model

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

1) Hosting governance (including partner 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, share 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 Management and Budget)
- Agency-led (e.g., Health and Human Services, Department of Education)
- University-public partnership
- Nonprofit-led

Each model has distinct advantages and challenges; an explication of those differences is beyond the scope of this guide. See Leveraging Integrated Data for Program Evaluation: Recommendations from the Field,[36] AISP Network Survey Series: Capacity,[37] and IDS Governance: Setting Up for Ethical and Effective Use[38] for a more nuanced discussion.

35 See Asemio (2021).
36 See Zanti, S., Berkowitz, E., Katz, M., Hawn Nelson, A., Burnett, T. C., Culhane, D., & Zhou, Y. (2022, August 24).
37 See Berkowitz, E., Jenkins, D., Hawn Nelson, A. (2025).
38 See Gibbs, L., Hawn Nelson, A., Dalton E., Cantor, J., Shipp, S., Jenkins, D. (2017).

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 services agency will often have clear legal authority for data integration across a number of programs (e.g., public health authority[39]), 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 may be the primary 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.

Governance structures

Each data sharing effort must decide how to structure their governance body or bodies to fit their context and support their core purpose for sharing data, in alignment with their management model and legal authority. For a full landscape view of how cross-sector data integration efforts in the AISP Network structure their data governance, see the AISP Network Survey Series: Governance.[40] When considering representation on governance bodies, remember that the answer to the first three questions in our framework (is it legal, is it ethical, and is it a good idea?) will depend on who is part of the deliberation. For this reason, participatory governance, such as a community advisory group on either a standing or project-by-project basis, is a best practice. Some efforts even include a set number of executive board seats for community representatives to ensure that they share in decision-making authority and further build social license. See Participatory Governance: Longform Work in Action for examples.[41]

Governance roles

In our experience, staffing is key to successful data governance, which should be iterative. 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, 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; data stewards generate valuable metadata and document bias and data quality concerns; data custodians are responsible for safeguarding data through rigorous security protocols.

39 See Network for Public Health Law (n.d.).
40 See Berkowitz, E., Jenkins, D., Hawn Nelson, A. (2025).
41 See Hawn Nelson, A., Algrant, I., Jenkins, D., et al. (2025).

The Roles of Data Owners, Data Stewards, and Data Custodians

	Role in data sharing and integration process	Role within agency
Data Owner	Accountable for data quality and security; holds decision-making authority over access and use.	Typically agency leadership that has signatory authority
Data Steward	Responsible for data governance, 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
Data Custodian	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 Data Steward and Data Owner regarding any data management issues that pose a risk to data security and/or access.	Typically IT staff or team

The Role of Legal and Privacy Experts in Governance

Effective data governance requires interdisciplinary participation, and lawyers and privacy officers must be treated as necessary, not optional, members of any decision-making body that oversees data access, use, and sharing. These professionals bring essential expertise in interpreting laws, assessing legal risk, identifying appropriate legal authorities, and ensuring that privacy protections are embedded into data practices from the start. We strongly advise against the impulse to consult these professionals only when problems arise. Including legal and privacy experts early on can help ensure that governance frameworks are grounded in current law, anticipate compliance obligations, and avoid unnecessary delays or last-minute denials. Their participation also helps bridge the gap between legal requirements and operational realities, providing practical guidance to analysts, program staff, and community partners. When lawyers and privacy officers are integrated into governance structures as collaborative partners, they enhance the system's credibility, accountability, and long-term sustainability.

Positive Practice

Here are some examples of AISP Network Sites with publicly available data governance information: North Carolina Department of Health and Human Services[42]; Linked Information Network of Colorado[43]; Hartford Data Collaborative;[44] Iowa's Integrated Data System for Decision-Making (I2D2);[45] and DataLinkCT.[46]

42 See North Carolina Department of Health and Human Services Data Office, Hawn Nelson, A., et al. (2025, June).
43 See Linked Information Network of Colorado (n.d.).
44 See CTData Collaborative: Hartford Data Collaborative, *HDC Governance & Legal Agreements* (n.d.).
45 See Iowa's Integrated Data System for Decision-Making (2021).
46 See Connecticut Office of Policy and Management (2025).

How: Drafting the Legal Agreements

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

Purpose of the Legal Agreements

Legal agreements are foundational tools for enabling responsible data sharing. They serve to document the legal authority for data use, clearly define the roles and responsibilities of each party, provide clarification when the law is silent or unclear, and establish the requirements for how data will be accessed, stored, used, and shared. These agreements translate legal and policy requirements into concrete, actionable items. They also help build trust among partners by promoting transparency, reducing ambiguity, and providing a mechanism for accountability. A well-drafted agreement not only supports compliance with the law but also operationalizes ethical data use practices that align with program goals and community values.

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.[47]

Tiered

We recommend a three-tier approach for legal agreements to govern data access and use for integrated data: a Memorandum of Understanding (MOU), a Data Sharing Agreement (DSA), and a Data Use License (DUL). Tiered agreements provide a consistent legal backbone while allowing customization for specific agencies, jurisdictions, or projects. This helps accommodate different statutory requirements or sensitivities (e.g., when working with tribal data, education records, or health information). 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.

[47] See Finch, K., Hawn Nelson, A., Jenkins, D., Burnett, T.C., Oliver, A., Martin, R. et al. (2018).

Tiered Agreements

Data Use License (DUL)

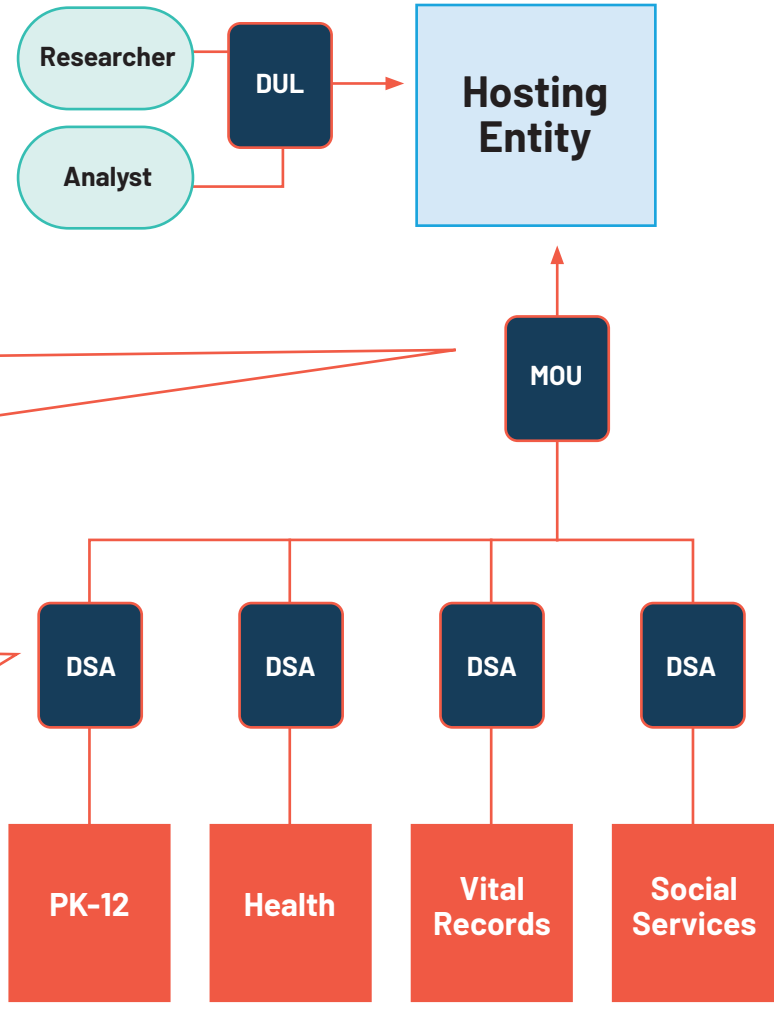
- Between Hosting Entity and Data Recipient
- Roles and responsibilities of the Data Recipient, often executed after a Data Request is approved

Memorandum of Understanding (MOU)

- Between Hosting Entity and Data Partners
- Establishes the specific context in which the host may access and use the data in the IDS
- MOU references the DSA, DUL, and relevant policies, and procedures for data access and use

Data Sharing Agreement (DSA)

- Between Hosting Entity and Data Partners
- includes the specific terms and conditions that govern how data are transferred, stored, and managed when shared and integrated
- DSA references the MOU and the DUL



Adapted with permission from Data Integration Support Center

FOUNDATIONAL LEGAL AGREEMENTS

LEGAL AGREEMENT	PURPOSE	PROCESS	SIGNATORY
Memorandum of Understanding (MOU) *Overarching process document signed by all data partners*	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.	Drafted in partnership with legal counsel from all participating data partners.	Lead agency/ies + all data partners
Data Sharing Agreement (DSA) *Agency-specific to how data will be used for integration*	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. The DSA is the primary mechanism to get data "into" the IDS.	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.	Lead agency/ies + each data partner
Data Use License (DUL) *Data use-specific once data has been integrated*	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 the following: purpose, data fields, anonymization procedures, dissemination plan, and timeline of project completion. The DUL is the primary mechanism to get data "out" of the IDS. A DUL must be executed prior to data access.	Template is drafted in partnership with legal counsel from all participating data partners. Once a data request is approved, a DUL is executed.	Lead agency/ies + data recipient

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 save time, improve workflow, support insights, and reduce costs. In North Carolina, the Department of Health and Human Services estimated an 80% reduction in both staff time spent and overall time to execute legal agreements per use case after an enterprise legal framework for data sharing was implemented.[48]

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

> Before organizations can responsibly share data, they must first understand the agreements that govern its use and exchange. Conducting a data sharing agreement inventory is a crucial step in this process, helping organizations identify existing agreements, assess their legal and policy implications, and ensure compliance with relevant laws and standards. A sample checklist can be found in *Appendix F.*

Using standard but modular documents can also increase the flexibility of legal agreements. Defining terms can be a complex exercise within one large institution and can be equally complex when doing so 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 subsequent 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 in plain language so that non-lawyers can understand them. 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 the foundational agreement among the lead IDS agency and the data partners. 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. 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.

[48] See Hawn Nelson, A., Hogle, P., Zanti, S., Proescholdbell, S., & Tenenbaum, J.D. (2024).

In *Appendices F* and *G,* we provide an MOU Inventory, Annotated Draft MOU, and examples of MOUs from IDS 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, some sites have 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 DataLinkCT, formerly P20 Win, EMOU). In either case, its mechanisms are provided 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 H*. The goal of the MOU is to outline the purpose, management model, interest holders, 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, Pennsylvania, 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. It does utilize an MOU for data sharing with agencies outside the county.

A Note of Caution on MOUs

Although MOUs are widely used in data sharing initiatives to outline roles, responsibilities, and shared principles between partners, their legal enforceability depends heavily on how they are written and the intent of the parties. Courts have reached different conclusions about whether MOUs are binding legal agreements. In some cases, such as *Gates Corp. v. Bando Chemical Industries, Ltd.*, courts have enforced MOUs where the terms were sufficiently specific and where evidence showed that both parties intended to create binding obligations.[49] Similarly, in *Clarke County Development Corporation v. Affinity Gaming, LLC,* the court treated an MOU as a binding agreement as a result of the specificity of its terms and the context in which it was executed.[50]

On the other hand, courts have declined to enforce MOUs that were vague, lacked essential terms, or explicitly stated that they were not intended to be binding. In *C.A.F. & Associates, LLC v. Portage, Inc.*, the court found that the MOU was unenforceable because it lacked numerous material terms.[51] The takeaway is that the intent of the parties—as reflected in both the language of the document and the surrounding circumstances—is critical.

For IDS efforts, this means that if partners intend to create enforceable legal obligations (such as data security requirements, permitted uses, or breach protocols), they should use a more formal agreement, like a data sharing agreement (DSA) or interagency contract. But if the goal is simply to document a shared understanding without creating legal enforceability, then an MOU may be appropriate. Still, parties should be deliberate and clear about their intent, and ensure that the document language supports that purpose.

[49] *Gates Corp. v. Bando Chemical Industries, Ltd.*, 4 Fed.Appx. 676 (2001).
[50] *Clarke County Development Corporation v. Affinity Gaming, LLC*, 826 F.3d 1090 (2016).
[51] *C.A.F. & Associates, LLC v. Portage, Inc.*, 913 F.Supp.2d 333 (2012).

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. The DSA is most often used to get data "into" 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 lead agency and host and the data partner (which owns the data).

The creation of an IDS usually 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 section Federal and State Laws (see page 40) 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 as the MOU, including those related to the legal use and protection of confidential data. 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 inquiries and research agendas. *Appendices H* and *I* 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 lead agency or host and the data licensee. The DUL is most often used to get data "out" of the IDS.

These agreements can be called Data Use Agreements (DUAs), but we refer to them as Data Use Licenses (DULs). Like other licenses, a DUL is time-bound and revocable. Specifically, the language of the 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 dataset). In *Appendices J* and *K,* 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[52] 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 dataset[53] in order to limit the release of PII/PHI and reduce the risk that an individual can be identified.

[52] See 45 CFR 46.114 (b).

[53] 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.

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 laws, 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 whether the law applies to that type of entity (e.g., HIPAA applies only 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)?

Risk Exposure

- Does the agreement include an indemnification clause? If so, who is being indemnified, and by whom? Does it shift the risk entirely to one party (i.e., the data recipient)?
- What is the scope of the indemnification? Does it include legal fees, damages, and costs of investigations and defenses? Are there carve-outs for gross negligence or willful misconduct?
- Is there a limitation of liability clause? Could this limitation reduce accountability for data misuse or breach?

Who bears the financial responsibility for breach-related costs (e.g., credit monitoring, legal defense, regulatory penalties)?

Already have legal agreements in place? Use the following questions to evaluate your legal agreements:

- If there are existing templates/model agreements, how do these documents work together?
- If there are existing templates/model agreements, are they modular or malleable to potential project-specific needs?
- 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 unchartered 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 AISP Network Survey Series: Legal to explore existing efforts.[54]

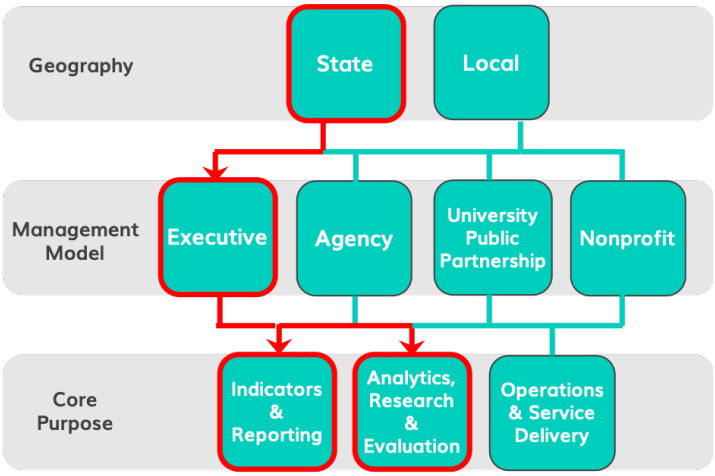
Government leaders of all political affiliations have embraced and encouraged the expansion of IDS to facilitate more effective and efficient government. The creation of the Evidence-Based Policymaking Commission Act of 2016 (HR. 1831) marked a turning point in federal recognition of the value of integrated data. Administrative data reuse is also now an important and commonplace way that states and localities are working to deliver more equitable, responsive, and effective public programs. Organizations interested in integrating data do not have to start from scratch and work in isolation. Across the country, strong legal frameworks, tested agreements, and cross-sector models demonstrate how data can be shared safely and legally to advance public good.

On the next page, 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 to demonstrate how and why legal frameworks differ.

[54] See Berkowitz, E., Kemp, D., Jenkins, D., Hawn Nelson, A. (2025).

Indiana Management Performance Hub (MPH)
Executive, State

The Indiana Management Performance Hub (MPH) governs the enterprise-level integrated data system and drives evidence-based decision-making across Indiana. MPH became the nation's first standalone state data agency in 2017, through executive order.



Learn more about MPH here.

Lead Agency: Indiana Management Performance Hub

Data Partners: All state agencies

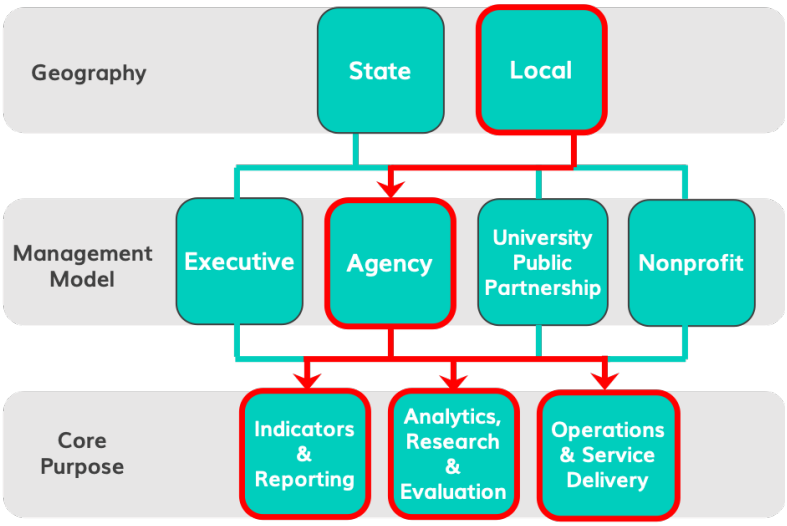
Legal Authority: Executive order, authorizing legislation, contracts

Funding: Federal, state

The Indiana Management Performance Hub (MPH) was initially established by executive order in 2014 and subsequently codified into state law in 2017, affirming its role under the Office of Management and Budget with authority vested in the state's Chief Data Officer. This statute formally designated MPH as a standalone state agency, empowered to act as an official "agent" for executive state agencies, and authorized to receive, link, analyze, and share government data on their behalf. MPH's governance allows it to streamline interagency collaboration, maintain data stewardship across systems, and uphold privacy through standardized agreements and infrastructure such as the Enhanced Research Environment.

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

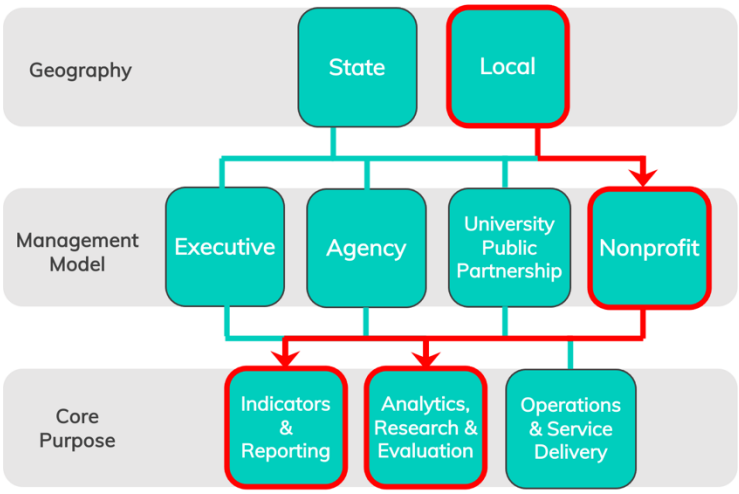
Legal Authority: Authorizing statute, contracts (e.g., Data Sharing Confidentiality Agreement)

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

Allegheny County's integrated data warehouse is built on the legal authority granted to its Department of Human Services (DHS), which operates as a "covered component" under HIPAA and serves as both the payor and oversight entity for human services programs—giving it the ability to require contracted providers to share client information for treatment, payment, and care coordination purposes without additional consent. Because DHS oversees both service delivery and funding, it can mandate data sharing with its providers as a condition of contract, thereby creating a clear legal pathway for comprehensive data integration. Moreover, the warehouse supports public dashboards for aggregated data, and secure access for research or internal operations via data sharing agreements. External research requires board review.

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

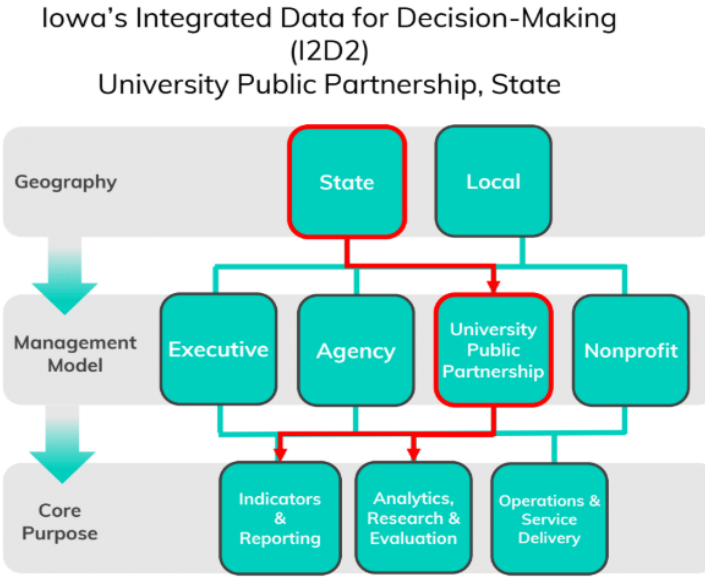
Data Partners: Baltimore City, Baltimore's Promise, and Baltimore City Schools, Baltimore City Health Department, nonprofit organizations

Legal Authority: Authorizing legislation, contracts

Funding: Philanthropic partners, fee for service

The Baltimore City Youth Data Hub was formally established in 2022 through state legislation, which authorized the creation of an integrated data system linking youth data across public and partner organizations including Baltimore City Schools, other city agencies, and Baltimore's Promise (a local collective impact nonprofit). Under the law, an executive committee governs the Youth Data Hub and appoints a manager to oversee operations, with express authority granted for designated entities to provide data, including personally identifiable information, subject to defined privacy and oversight protocols. The Youth Data Hub emphasizes community-centered analysis and governance, ensuring that data use centers equity, transparency, and youth well-being.

This state-university partnership supports Iowa's investments in more effective and efficient coordinated systems of care for young children and their families. Building from a legislative mandate through Early Childhood Iowa that commissioned state departments toward collaboration, I2D2 brings together leadership from partners across the state and faculty at Iowa State University.



Learn more about I2D2 here.

Lead Agencies: Iowa State University

Data Partners: Departments of Management, Health and Human Services, Workforce Development, Economic Development, and Education; and Head Start agencies

Legal Authority: Authorizing legislation, contracts

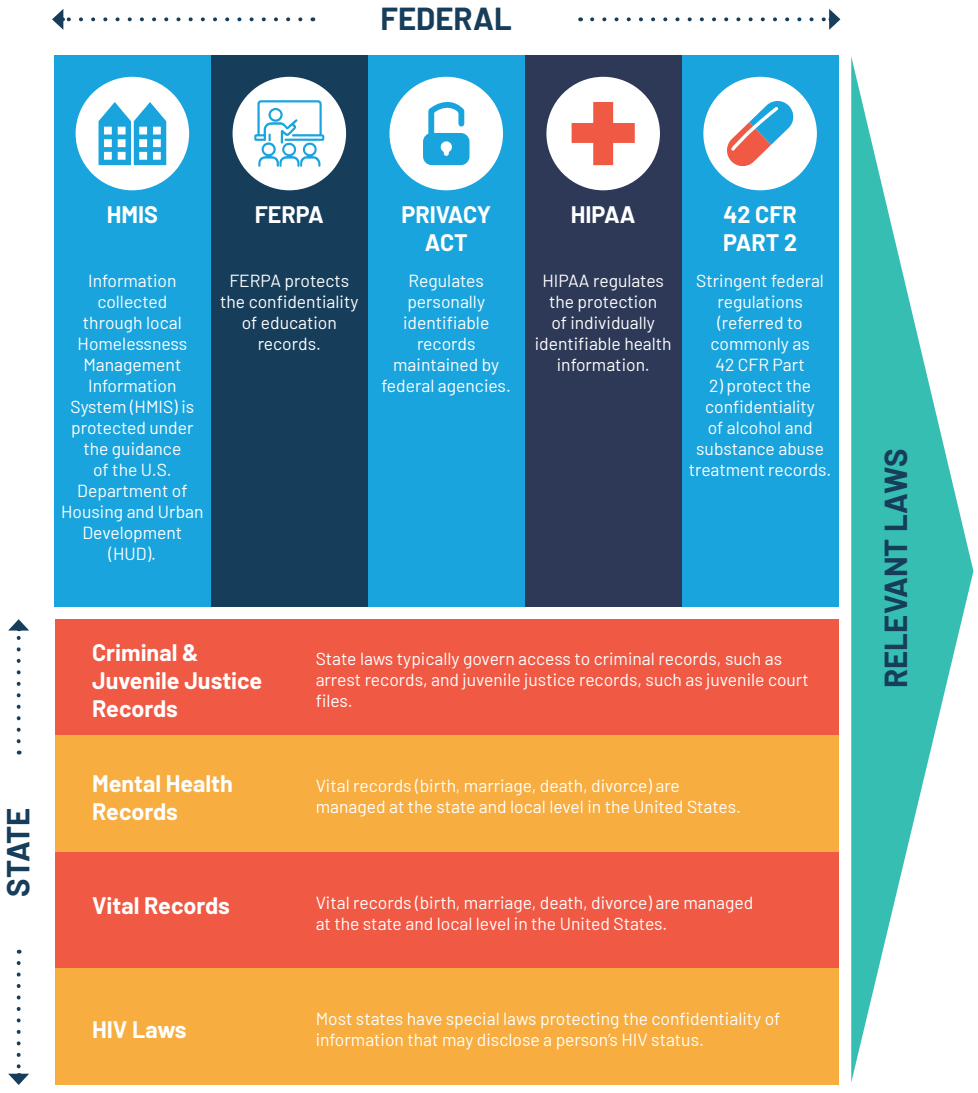
Funding: Individual grants and contracts

In 2018, Iowa's I2D2 system was launched through a collaborative partnership between Iowa State University (a land-grant university) and multiple state agencies and was authorized through state legislation. Their legal framework authorizes the integration of data across early childhood programs and is operationalized through a suite of legal instruments, including Memoranda of Understanding (MOUs) to establish partnership commitments, Data Sharing Agreements (DSAs) to define the terms and safeguards for transferring data, and Data Use Licenses (DULs) to govern the use of datasets for approved projects.

These four examples offer distinct models for legal frameworks that meet the needs of partners, the legal authority of host organizations, and their purposes for sharing data. For more examples, see Appendix O.

Federal and State Laws

Discrete statutes and regulations must be considered when 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. Of particular relevance are state laws governing highly confidential information such as juvenile arrest records, mental health records, and other sensitive types of information. Confusion sometimes arises when there is a perceived or real conflict between federal and state law. While addressing this conflict, keep 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. In some cases, federal law is silent, and states fill in the gaps with their own laws. Significantly, federal laws preempt or displace state law when there is a conflict. Given the above, there are some substantive areas where state laws must be consulted (mental health, HIV, criminal justice).[55] The graphic below identifies some of the laws most likely to be relevant to the discussion. For a more robust offering of pertinent federal laws for commonly accessed data assets, see *Appendix A*. For further legal resources by federal and state statute, see *Appendices B-C*.



[55] See Hodge, J., Kaufman, T., & Jaques, C. (2011).

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to protected health information[56] (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.[57] 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,"[58] 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"[59] (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).

For more on HIPAA, see *HIPAA Decision Matrix*.[60]

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.[61] FERPA also protects PII about the student that is different from 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, in 2011 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."[62]
- 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."[63] Note the specific reference to a "data warehouse."
- 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.[64] The Privacy Technical Assistance Center (2017) has also released guidance specifically addressing concerns around IDS and student privacy.[65]

56 45 CFR § 160.103.
57 See Marron, J. (2024).
58 45 CFR § 160.103.
59 45 CFR § 164.514.
60 See Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023).
61 34 CFR § 99.3.
62 See discussion of the regulation with DOE commentary within the Federal Register (2011, December 2).
63 See Federal Register, 2011, 76 (No. 232), p. 75637.
64 See National Center for Education Statistics (2010).
65 See U.S. Department of Education & Privacy Technical Assistance Center (2017).

- Finally, there may be confusion about 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.[66]

For more on FERPA, see *FERPA Decision Matrix*.[67]

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

Stringent federal regulations (commonly referred to 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."[68] 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).[69]
- Many state laws on substance abuse track (or in some cases may exceed) protections in 42 CFR. When thinking about an IDS, it is important to look at state law as well as the federal regulations.

For more on 42 CFR Part 2, see *Demystifying 42 CFR Part 2: Legal and Ethical Use of SUD Records*.[70]

Federal Regulations Governing the Confidentiality of Information Collected in Homeless Management Information Systems (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).[71] 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 service 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.[72]

66 See U.S. Department of Health and Human Services & U.S. Department of Education, *Joint Guidance on the Application of the FERPA and HIPAA to Student Health Records* (2008, revised 2019).
67 See Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023).
68 42 CFR § 2.11.
69 See Kamoie B. & Borzi P. (2001, August).
70 See Kemp, D. (2024).
71 42 USC § 11360a; 24 CFR § 578.7; 24 CFR § 578.57; 24 CFR § 578.103; 69 FR 45888.
72 42 USC § 11360a; 24 CFR § 578.7; 24 CFR § 578.57; 24 CFR § 578.103; 69 FR 45888.

The Privacy Act

The Privacy Act of 1974 regulates how the federal government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act protects the confidentiality of personally identifiable information of citizens and permanent residents contained in systems of records maintained by federal agencies.[73] The Privacy Act has stringent confidentiality provisions but permits disclosure without the subject's consent under a number of exceptions. Two notable exceptions follow:

- Personally identifiable information can be shared without 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."[74] This definition has been used to permit researcher access even to identifiable data.
- Personally identifiable information can be shared within an agency on a "need to know" basis.[75]

For more on the Privacy Act, see *A Privacy Act Primer*.[76]

State Public Records Acts[77]

State public records laws, also known as sunshine or freedom of information laws, govern public access to government records and are essential tools for promoting transparency. However, these laws can present legal and operational challenges for IDS, particularly when they intersect with the need to protect individual privacy. **A key challenge some IDS initiatives will face is determining whether newly linked datasets qualify as public records and are therefore subject to disclosure**. Most state public records acts include exemptions that protect personally identifiable information (PII), confidential records, or records protected by other laws, which can help shield sensitive data from disclosure. For example, Washington State's Public Records Act (RCW 42.56) includes exemptions for personal data where disclosure would violate an individual's right to privacy, and for records that are protected under other federal or state laws like HIPAA or FERPA.[78]

However, these protections vary by state. The Tennessee Public Records Act (TPRA) (T.C.A. § 10-7-503) presents a unique challenge: It includes a strong presumption of public access and fewer explicit exemptions related to administrative data or data sharing arrangements.[79] In Tennessee, government records, including data sharing agreements and potentially some de-identified datasets, may be subject to disclosure unless a specific exemption is written into statute or clearly applies. This creates legal uncertainty and can have a chilling effect on interagency data collaboration, particularly when sensitive populations are involved or where linked data increases re-identification risk.

To navigate these risks, agencies must work closely with legal counsel to understand how their state's law applies to both source data and outputs, and to identify exemptions that may apply. Data use agreements and governance policies should address public records risks explicitly by defining data ownership, use limitations, and protocols for responding to records requests. Where disclosure is possible or likely, IDS leaders should communicate clearly with interest holders and community partners about the limits of confidentiality and the legal obligations to which agencies are subject.

---

73 Pub Law No. 93-579, 5 U.S.C. § 552a (2018).
74 5 USC § 522a (a)(7).
75 5 USC § 522a (b)(1).
76 See Kemp (2025).
77 While there are federal laws that govern public access to records held by federal agencies, such as the Freedom of Information Act), we have deliberately chosen to focus on state public records acts, because most IDS are housed within state or local agencies and are generally subject to state disclosure requirements.
78 Wash. Rev. Code § 42.56.210.
79 Tenn. Code Ann. § 10-7-503.

Tribal Data Sovereignty

Tribal data sovereignty refers to the inherent right of a Tribal nation to govern the ownership, collection, and use of its own data.[80] Tribes are sovereign jurisdictions with the authority to self-govern and determine their own form of government and laws.[81] As part of this authority, Tribes necessarily have the authority to protect their citizens and provide human services that they elect.[82] It follows then that Tribal nations have the authority to administer the collection, use, and ownership of their own data.[83] Generally, state governments do not have regulatory authority on Tribal lands. As a result, in a data sharing context, Tribes and federal, state, or local governments can enter into data sharing agreements.[84] 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.[85] As a result, the legal frameworks discussed previously may be helpful for Tribes intending to share data with state and local partners as a reference. *Appendix C* provides a sampling of Tribal laws pertinent to data sharing.

Despite their status as sovereign governments, Tribes are often excluded from state and federal data systems or treated as external interest holders rather than equal partners. Challenges include uncertainty about engagement with Indian Tribes, a lack of formal data sharing pathways, restrictive interpretations of privacy laws, failure to disaggregate Tribal data in public reporting, and systems that prioritize agency control over Indigenous data rights.[86] These barriers in turn limit Tribes' ability to further develop their public health systems through funding or collaboration, conduct timely disease surveillance, respond to public health emergencies, and design data-informed health interventions.[87] As a result, many Tribes must rely on incomplete or outdated information to access the data that state and federal agencies routinely share with other government entities.[88] Addressing these inequities requires a shift toward recognizing Tribal sovereignty, honoring Indigenous data governance principles, and building sustained government-to-government relationships that support meaningful data access and use.

Case Study: Tulalip Tribe–Washington State Data DOH Data Sharing Agreement

In January 2025, the Washington State Department of Health (DOH) and the Tulalip Tribe signed a data sharing agreement to advance Tribal data sovereignty.[89] Under the agreement, the Tulalip Tribe will have direct access to state public health datasets, including the Washington Disease Reporting System. Importantly, the Tribe will retain oversight over the use of its members' data, empowering Tribal health authorities to lead outbreak investigations, develop health priorities, and control how Tulalip data are aggregated and shared. Check out the Template Tribal Data Sharing Agreement (TDSA) created in partnership with Tribes and Washington's Governor's Indian Health Advisory Council (GIHAC).[90]

This agreement represents a significant shift toward respecting government-to-government relationships, enhancing Tribal ownership of their data, and setting a model for other Tribes in Washington State and beyond.

For a more robust discussion on working with Tribal data, see A Toolkit for Centering Racial Equity Throughout Data Integration.[91]

80 See *Williams v. Lee*, 358 U.S. 217, 271 (1959) (articulating power of Indian Tribes to regulate affairs on an Indian reservation).
81 Nat'l Farmers Union Ins. Companies v. Crow Tribe of Indians, 471 U.S. 845, 856 (1985).
82 See Tsosie, R. (2019).
83 See Kukutai, T., Taylor, J., Tauli-Corpuz, V., et al. (2016).
84 For information on jurisdictional coordination between states and Tribes, see Tribal Legal Preparedness Project (n.d.).
85 See Milam, S. (2020).
86 See Hassanein, N. (2025, April 3).
87 See U.S. Government Accountability Office (2022, March).
88 Ibid.
89 See Washington State Department of Health (2025, January 21).
90 See Washington State Department of Health (2025, March 17).
91 See Hawn Nelson, A., Zanti, S., Jenkins, D., Algrant, I., Rios Benitez, J., et al. (2025, 2020).

Conclusion

There is no one right path to data sharing and use that is legal, ethical, and a good idea. We began by discussing the threshold question of "Is it legal?" and exploring how governance structures can help ensure that data use is not only legal, but also ethical and a good idea. Clear governance and legal frameworks should work together to mitigate the inevitable risks of data sharing, protect privacy, and guide responsible data use. We examined the role of lawyers and privacy officers in data governance and throughout the data life cycle. Lawyers play a central role in this process, not only as compliance gatekeepers but as strategic partners in shaping agreements, governance documents, and permissible uses. We also highlighted how public records laws, Tribal data sovereignty, and the emerging role of AI all shape the legal and ethical considerations.

The following table offers examples of positive and problematic practices for engaging legal counsel in data integration efforts. They illustrate the difference between treating legal review as a box to check at the end and strengthening data sharing by including lawyers as integral partners from the start.

Positive Practice	Problematic Practice
Ensuring that there is legal representation on the data governance group from the very beginning of planning the data integration effort	Reaching out to the legal team only when a problem has occurred
Engaging legal counsel to conduct an inventory of existing relevant legal agreements	Starting from scratch and drafting new legal agreements without context
Working collaboratively with the legal team to create an MOU, DSA, and DUL for the integration effort	Involving legal counsel at the very end of negotiations, after partners have already reviewed and agreed on a data sharing agreement, just to get "final sign-off"
Seeking the advice and input of legal counsel to ensure that each proposed use of data is legal	Waiting until after the data have already been shared to get legal advice or seeking retroactive approval
Engaging the legal team early and often to help plan fundamental governance documents	Skipping legal review of governance documents in order to "move the project along"

By adopting more of the practices in the left column and avoiding those in the right, agencies can reduce delays, strengthen compliance, and build more durable and trustworthy data systems.

We hope this guide has shown you that, while this task is complex, it is worthwhile. We also want to emphasize that governance and legal frameworks should be iterative; it is necessary to **periodically reassess legal frameworks and data uses** as projects grow and laws change. We suggest using annual legal audits, updated inventories, and governance body reviews to accomplish this task. With the right team asking and considering the right questions, agencies and their partners can "find a way forward" to share and integrate data to improve lives.

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 are 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, social security number), 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.

Interest holders: define term to indicate group that is put together to determine collaborative decision-making—each data integration effort will include a different group of interest holders.

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: an individual right to control how personal information is collected, accessed, and used. Common privacy risks for individuals include:

- Financial risks, such as identity theft or fraud;
- Physical risks, such as stalking or burglary;
- Reputational risks, such as embarrassing rumors or damaging photos; and
- Dignitary risks, such as a loss of autonomy or opportunity when a person is profiled or discriminated against by an automated decision-making system.

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.

References

Actionable Intelligence for Social Policy, Data Quality Campaign, Education Commission for the States, & West Ed's Data Integration Support Center. (2025, May). *Defining Modern, User-Centered State Longitudinal Data System Design*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Asemio. (2021). Unlocking Insights: How Tulsa Built Momentum with Easier, Faster, and Safer Data Sharing.

Berkowitz, E., Jenkins, D., & Hawn Nelson, A. (2025). *Network Survey Brief: Capacity*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Berkowitz, E., Jenkins, D., & Hawn Nelson, A. (2025). *Network Survey Brief: Governance*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Berkowitz, E., Kemp, D., Jenkins, D., & Hawn Nelson, A. (2025). *Network Survey Brief: Legal*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Center for Democracy & Technology & The Leadership Conference's Center for Civil Rights and Technology. (2025, May 9). *Immigration, DOGE, and Data Privacy*.

Center for Regional Economic Competitiveness (CREC). (2018, March). *Data Sharing Toolkit*. State Data Sharing Initiative.

Centers for Disease Control and Prevention & Office for State, Tribal, Local and Territorial Support. (2024, May 16). *Tribal Emergency Preparedness Law*. Public Health Law Program.

Commission on Evidence-Based Policymaking. (2017, September). *The Promise of Evidence-Based Policymaking*.

Connecticut Office of Policy and Management. (2023). *Legal Issues in Interagency Data Sharing*.

Connecticut Office of Policy and Management. (2025). *DataLinkCT Data Governance.*

Connecticut Office of Policy and Management, Data and Policy Analytics. (2025, January 24). *CT High Value Data Inventory*. Connecticut Open Data Portal.

CNN. (2025, July 2). 20 states sue after the Trump administration releases private Medicaid data to deportation officials.

CTData Collaborative: Hartford Data Collaborative. (n.d.). *HDC Governance & Legal Agreements*.

CTData Collaborative: Hartford Data Collaborative. (n.d.). *Request HDC Data: Data Request Process*.

Data Across Sectors for Health & The Network for Public Health Law. (2018, November). *Data Sharing and the Law, Deep Dive on Consent*.

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.

Friedland, J. (2018, January 25). *How ICE Uses Databases and Information-Sharing to Deport Immigrants*. National Immigration Law Center.

Gibbs, L., Hawn Nelson, A., Dalton E., Cantor, J., Shipp, S., & Jenkins, D. (2017). *IDS Governance: Setting Up for Ethical and Effective Use.* Actionable Intelligence for Social Policy, University of Pennsylvania.

Hassanein, N. (2025, April 3). Tribes, long shut out from their own health data, fight for access and sovereignty. *Native News Online*.

Hawn Nelson, A., Algrant, I., Jenkins, D., et al. (2025). *Participatory Governance: Longform Work in Action*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Hawn Nelson, A., Algrant, I., Jenkins, D., Rios Benitez, J., Kemp, D., Burnett, T.C., Zanti, S., & Culhane, D. (2025, 2020). *Introduction to Data Sharing and Integration.* Actionable Intelligence for Social Policy. University of Pennsylvania.

Hawn Nelson, A., Hogle, P., Zanti, S., Proescholdbell, S., & Tenenbaum, J. D. (2024). A governance and legal framework for getting to "yes" with enterprise-level data integration. *Data & Policy*, *6*, e31.

Hawn Nelson, A., Kemp, D., Jenkins, D., Rios Benitez, J., 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.

Hawn Nelson, A., & Zanti, S. (2023). Four Questions to Guide Decision-Making for Data Sharing and Integration. *International Journal of Population Data Science.*

Hawn Nelson, A., Zanti, S., Jenkins, D., Algrant, I., Rios Benitez, J., et al. (2025, 2020). *A Toolkit for Centering Racial Equity Throughout Data Integration*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Hodge, J., Kaufman, T., & 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.

Hofmann, V., Kalluri, P. R., Jurafsky, D., & King, S. (2024, August 28). AI generates covertly racist decisions about people based on their dialect. *Nature, 633*, 147–154.

Indiana Management Performance Hub. (2025, May 29). *State of Indiana Standard: AI Readiness Assessment Methodology (Version 1.0)*.

Iowa's Integrated Data System for Decision-Making. (2021). *Governance*.

Jenkins, D., Berkowitz, E., Burnett, T., Culhane, D., Hawn Nelson, A., Smith, K., & Zanti, S. (2021). *Quality Framework for Integrated Data Systems*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Joffe-Block, J., & Fowler, S. (2025, May 9). *USDA, DOGE Demand States Hand Over Personal Data about food stamp recipients*. NPR.

Kamoie, B., & 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.

Kemp, D. (2025). *A Privacy Act Primer*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Kemp, D. (2024). *Demystifying 42 CFR Part 2: Legal and Ethical Use of SUD Records*. Actionable Intelligence for Social Policy.

Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023). Appendix A, HIPAA Decision Matrix. *Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration*. Actionable Intelligence for Social Policy. University of Pennsylvania.

Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023). Appendix B, FERPA Decision Matrix. *Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration*. Actionable Intelligence for Social Policy. University of Pennsylvania.

Kemp, D., Hawn Nelson, A., & Jenkins, D. (2023). *Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration*. Actionable Intelligence for Social Policy. University of Pennsylvania.

Kukutai, T., Taylor, J., Tauli-Corpuz, V., et al. (2016). *Indigenous Data Sovereignty: Toward an Agenda*. Australian National University Press.

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 Center for Education Statistics. (2010, November). *SLDS Technical Brief: Guidance for Statewide Longitudinal Data Systems* (NCES 2011-601). U.S. Department of Education.

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*. U.S. Department of Health, Education, and Welfare.

National Neighborhood Indicators Partnership. (2025). *Partner Profiles*.

Network for Public Health Law. (n.d.). *Public health authority*. Network for Public Health Law.

North Carolina Department of Health and Human Services. (2025). *NCDHHS Operational Data Request Form*.

North Carolina Department of Health and Human Services (NCDHHS) Data Office, Hawn Nelson, A., et al. (2025, June). *The NCDHHS Data Sharing Guidebook*.

Office of the National Coordinator for Health Information Technology. (2018, September 19). *Meaningful Consent Overview*. HealthIT.gov.

Petrila, J., Cohn, B., Pritchett, W., Stiles, P., Stodden, V., Vagle, J., Humowiecki, M., & Rosario, N. (2017). *Legal Issues for IDS Use: Finding a Way Forward*. Actionable Intelligence for Social Policy, University of Pennsylvania.

Rodriguez, B., El-Amin, A., & Tiderman, L. (2024). *Building a Secure Generative Artificial Intelligence Environment for Research Use*. WestEd.

Scholl, M., Stine, K., Nash, J., Bowen, P., Johnson, L., Smith, S., & Steinberg, D. (2008, under revision 2021). *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. National Institute of Standards and Technology.

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022, March). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (NIST Special Publication No. 1270). National Institute of Standards and Technology.

The Sequoia Project. (2025, April 24). *Moving Toward Computable Consent: A Landscape Review*.

Tribal Legal Preparedness Project. (n.d.). *Home*. 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. (2011, December 2). Family Educational Rights and Privacy; Final Rule. *Federal Register*, 76(232), 75604–75660.

U.S. Department of Education & Privacy Technical Assistance Center. (2017, January). *Integrated Data Systems and Student Privacy*.

U.S. Department of Health and Human Services. (n.d.). *How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule?* National Institutes of Health.

U.S. Department of Health and Human Services. (2025, January 15). *Security Risk Assessment Tool.*

U.S. Department of Health and Human Services & Office for Human Research Protections. (2025, June 6). *Institutional Review Board Written Procedures: Guidance for Institutions and IRBs*.

U.S. Department of Health and Human Services & 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*.

U.S. Government Accountability Office. (2022, March 4). *Tribal Epidemiology Centers: HHS Actions Needed to Enhance Data Access* (GAO Report No. GAO-22-104698).

Washington State Department of Health. (2025, January 21). *DOH and Tulalip Tribe Sign Historic Tribal-Specific Data Sharing Agreement*.

Washington State Department of Health. (2025, March 17). *WA-DOH TDSA template*.

World Economic Forum. (2020, July 30). *Redesigning Data Privacy: Reimagining Notice & Consent for Human Technology Interaction*. World Economic Forum.

Zanti, S., Berkowitz, E., Katz, M., Nelson, A. H., Burnett, T. C., Culhane, D., & Zhou, Y. (2022, August 24). Leveraging integrated data for program evaluation. *Evaluation and Program Planning, 90*, 101967.

Zanti, S., Jenkins, A., Berkowitz, E., Hawn Nelson, A., Burnett, T.C., & Culhane, D. (2021). *Building and Sustaining State Data Integration Efforts: Legislation, Funding, and Strategies*. Actionable Intelligence for Social Policy, University of Pennsylvania.

APPENDIX A:
Survey of Common Federal Legal Authority for Data Sharing & Integration

This table summarizes common federal laws governing relevant permissible uses and disclosures of data assets such as Medicaid, WIC, SNAP, vital records, arrest records, and medical records, among others. This table identifies the relevant statute and/or code and the allowable uses permitted under those legal authorities. As a note, in some cases, whether an asset can be used or disclosed for the purposes below will also depend on the data recipient (or host). *This table focuses on relevant uses and disclosures of identifiable data without consent*. This table is not meant to be exhaustive, and instead summarizes the uses most relevant for sharing and integrating cross-sector administrative data. Of note, federal law generally permits de-identified and aggregate data to be shared freely without limitation and identifiable data can usually be shared with consent.

Data Asset	United States Code	Code of Federal Regulations	Allowable Uses
Arrest Records	n/a	n/a	*Arrest records are governed by state law*
Child Support Records	42 U.S.C. § 651 42 U.S.C. § 654(26) 42 U.S.C. § 654a(f) 42 U.S.C. § 669	45 C.F.R. §§ 303.21, 307.13	• Establishment, modification and enforcement of child support obligations • Performance of official child support program responsibilities • Paternity establishment • TANF or Medicaid program administration • Pursuant to court order • Approved census or research purposes (with safeguards for confidentiality)
Criminal Justice Information Systems (CJIS)	34 U.S.C. § 41104 34 U.S.C. § 41105 34 U.S.C. § 41106 34 U.S.C. § 41107	28 C.F.R. § 20.21(b) 28 C.F.R. § 20.33 28 C.F.R. § 20.34	• Administration of criminal justice (investigations, prosecutions, corrections) • Research, evaluative, or statistical activities • State sealing or purging obligations • Licensing and employment • Background checks • Data processing/information services
Drivers' License Records/State Identification	18 U.S.C. § 2721(b)	6 C.F.R. § 37.33 6 C.F.R. § 37.41	• Governmental functions • Insurance verification • Research and statistical purposes • Motor vehicle or driver safety and theft • Monitoring emissions • Product recalls and advisories • Enforcement and oversight

Education Records	20 U.S.C. § 1232f 20 U.S.C. § 1232g	34 C.F.R. §§ 99.31-38	• Disclosure to school officials with legitimate educational interests • School enrollment • Government authorities • Financial aid • Audit or evaluation purposes • Studies for educational purposes • Health and safety emergencies • Directory information • Enforcement of or compliance with federal education programs • Disclosure to state or local juvenile justice systems
Homeless Management Information System (HMIS) Records	42 U.S.C. § 11363	24 C.F.R § 576.500(x) 24 C.F.R. § 578.103(b) HMIS Data and Technical Standards, 69 Fed. Reg. 45,888 (July 30, 2004)	• HUD compliance monitoring • Research and analysis of patterns of service use • Reimbursement and funding priorities • Service delivery • De-identification • Collection of unduplicated counts • Analyze patterns of use assistance provided • Project sponsors and applicants
Medicaid	42 U.S.C. § 1396a(a)(7) 42 U.S.C. § 1396b 42 U.S.C. § 1396w-3a	42 C.F.R. §§ 431.301; 431.303; 431.306; 431.307 42 C.F.R. §§ 435.945; 435.948; 435.952 42 C.F.R § 495.346	• Verification of income, eligibility and amount of assistance for other federal programs • Medical assistance eligibility • Service delivery • Investigations related to administration of Medicaid Plan • Program integrity efforts • Prescription drug monitoring • Integration of information into covered provider workflows • State Medicaid program administration
Medical/Health Records	42 U.S.C. § 1306 42 U.S.C. § 1320c-9 42 U.S.C. § 1320d *et al.* 42 U.S.C § 17935	45 C.F.R. § 164 *et seq.*	• Treatment, payment and health care operations • Health care planning and public health activities • Research • Administration of employee benefit plans • Public inspection of certain program evaluations, excluding personal identifiers • Facilitate standardized electronic health care transactions • Law enforcement purposes under specific conditions

Supplemental Nutrition Assistance Program (SNAP)	7 U.S.C. Chapter 51 7 U.S.C. § 2020(e)(8)	7 C.F.R. § 272.1(c)	• Administration of federal and state assistance programs • Recovery of over issuances through tax refund offsets • Administration of the National School Lunch Program or the School Breakfast Program for certifying eligibility • Officials for locating individuals • Program enforcement
Substance Use Disorder Records	42 U.S.C. § 290dd- 2	42 C.F.R. §§ 2.12, 2.31, 2.33, 2.51-2.53	• Medical personnel in a bona fide medical emergency • Scientific research, audits, or program evaluation with conditions • Pursuant to court order • Diagnosis, treatment, or referral for treatment • Disclosure to qualified organizations providing services • Reporting crimes against program personnel • Reporting suspected child abuse and neglect
Supplemental Social Security Income	42 U.S.C. § 405 42 U.S.C. § 1306 42 U.S.C. §§ 1381-1383f	20 C.F.R. § 401.150 20 C.F.R. § 416.101 20 C.F.R. § 416.708 20 C.F.R. § 416.1031	• Verifying and matching information for administration and enforcement of federal laws • Medicare/Medicaid administration or overpayment recovery • Verifying income, resources, or disability status • Fraud investigations or program enforcement, consistent with Privacy Act requirements • Planning or conducting a census or survey • Records management inspections • Statistical research or program evaluation
Tax Return Information	26 U.S.C. § 6103 26 U.S.C. § 7431	26 C.F.R § 301.6103(c)-1 26 C.F.R § 301.7216-2	• Tax preparation • Federal and state tax enforcement and administration • Tax litigation and prosecutions • Disclosure to the President for specified officials' returns • Disclosure to congressional committees (under confidentiality rules) • Statistical analysis and economic research • Pursuant to court order

Temporary Assistance for Needy Families (TANF) Program	42 U.S.C. § 602 42 U.S.C. § 604 42 U.S.C. § 611	45 C.F.R. § 205.50 45 C.F.R. § 263.2 45 C.F.R. § 265.9	• Program administration • Administering federally assisted programs which provide assistance, in cash or in kind, or services, directly to individuals on the basis of need • Promoting self-sufficiency through job preparation and work activities • Employment verification • Audits
Unemployment Insurance Employment Records	26 U.S.C. § 3304 42 U.S.C. § 405 42 U.S.C. § 503	20 C.F.R. § 603.4 20 CFR § 603.5 81 FR 56072	• Eligibility determination • Administration of unemployment compensation programs • Disclosure to public official for use in the performance of official duties • Disclosure to Bureau of Labor Statistics for statistical purposes • Federal oversight & audits • Fraud detection • Program oversight • Pursuant to court order • Evaluation of state programs • Research
Veterans' Affairs Claims	38 U.S.C. § 5701 38 U.S.C. § 5727 38 U.S.C. § 7332	38 C.F.R. § 0.605 38 C.F.R. §§ 1.500-1.527 38 C.F.R. § 1.575	• Medical referrals • Costs recovery • Public health reporting or safety purposes • Credit monitoring after security incident • Claims processing • Benefits administration and verification • Computer matching with federal or state agencies to verify benefits or prevent fraud • Appeals or investigations related to VA claims or benefits • Providing loan or benefit application status to veterans or joint applicants • Collecting SSNs for compensation or pension benefits • Eligibility determination for health benefits plans • Employment decisions • Audits, fraud detection, or program integrity • Research or statistical purposes
Vital Records	n/a	n/a	*Vital records are governed by state law*

Voter Registration Records	52 U.S.C. § 20504 52 U.S.C. § 20505 52 U.S.C. § 20507(i) 52 U.S.C. § 20508 52 U.S.C. § 21082 52 U.S.C. § 21083	n/a	• Public records • Implementation of voter registration programs and activities under the NVRA • Voter registration applications • Ensuring compliance with NVRA requirements • Verifying voter eligibility or coordinating with agencies • Inspection or copying • Oversight, reporting, or enforcement of NVRA compliance • Statistical analysis or election administration purposes
Women, Infants, and Children (WIC) Program	7 U.S.C. § 2018(c) 42 U.S.C. § 1786	7 C.F.R. § 246.26(d)	• Program administration and enforcement • Eligibility determination • Compliance • Program evaluations • WIC-related research • Administration of programs that benefit WIC-eligible persons • Child abuse or neglect reporting • Verification of information for SNAP administration, enforcement, or investigation of federal law violations • Administration of the Food and Nutrition Act or to enforce other federal laws

APPENDIX B:
Selected Additional Resources for Relevant Federal Law and Policy

Authority	Overview	Notable Exceptions and/or Exemptions for Disclosure
Family Educational 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 (34 CFR 99.3). *Note: De-identified data is not a "student record" and therefore not PII.	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))

Additional Resources

Access, Disclosure, and Use of Federal Student Aid (FSA) Data (Data Integration Support Center, 2025)

Federal Privacy Basics Part 1 (FERPA 101 & HIPAA 101) (Video) (AISP & Data Integration Support Center, 2024)

Student Privacy at the U.S. Department of Education (U.S. Department of Education, 2021)

The Family Educational Rights and Privacy Act Guidance on Sharing Information with Community-Based Organizations (U.S. Department of Education, 2021)

Data Transfer in the Larger Education Ecosystem (U.S. Department of Education, 2020)

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)

Webinar on Integrated Data Systems and Student Privacy (U.S. Department of Education, 2017)

Integrated Data Systems and Student Privacy (U.S. Department of Education, 2017)

Responsibilities of Third-Party Service Providers under FERPA (U.S. Department of Education, 2015)

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 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."	Research (42 CFR 2.52)
Additional Resources		
Summary of 42 CFR Part 2, Confidentiality of Substance Use Disorder Patient Records, Final Rule (Network for Public Health Law, 2024) Frequently Asked Questions (FAQs) and Fact Sheets regarding the Substance Abuse Confidentiality Regulations (U.S. Substance Abuse and Mental Health Services Administration, 2022) Substance Abuse and Mental Health Services Administration: Confidentiality of Substance Abuse Disorder Patient Records Snap Shot (Network for Public Health Law, 2020) The Council of State Governments Justice Center. Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (Petrila, J. & Fader-Towe, H., 2010)		
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 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.	Research (Privacy Standard 4.1.3)

Additional Resources		
Federal Privacy Basics Part 2 (Video) (HMIS & Privacy Act) (AISP & Data Integration Support Center, 2024) FY 2022 HMIS Data Standards (Manual) (U.S. Department of Housing and Urban Development, 2021) HMIS Privacy and Security Standards: Emergency Data Sharing for Public Health or Disaster Purposes (U.S. Department of Housing and Urban Development, 2020) Snap Shot: Homeless Management Information Systems (The Network for Public Health Law, 2018)		
Privacy Act of 1974	Regulates personally identifiable records maintained by federal agencies.	Routine Use (5 USC 522a (a) (7))
Additional Resources		
Overview of the Privacy Act of 1974, 2020 Edition (U.S. Department of Justice, 2020) Computer Matching Agreements (U.S. Department of Education, 2007) Department of Justice Privacy, Civil Rights, and Civil Liberties Protection Policy for the Information Sharing Environment (Department of Justice, 2010)		
Health Insurance Portability and Accountability Act (HIPAA) 45 CFR Part 164	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.	Health Care Operations (Business Associates) Research (See, generally, 45 CFR § 164.512)

Additional Resources

Federal Privacy Basics Part 1 (FERPA 101 & HIPAA 101) (Video) (Actionable Intelligence for Social Policy & Data Integration Support Center, 2024)

Direct Liability of Business Associates (U.S. Department of Health and Human Services, 2021)

Covered Entities and Business Associates (U.S. Department of Health and Human Services, 2017)

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)

Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Individual Identifiers (Centers for Medicare & Medicaid Services, 2010)

APPENDIX C:
Selected State & Tribal Laws, Policies, and Rules

The following table compiles illustrative examples from state, Tribes and localities that have implemented data sharing policies, laws and/or rules that extend beyond federal statutes. These samples are meant to show how jurisdictions have regulated other data assets not addressed by federal laws. 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	Toolkit: Data Sharing for Child Welfare Agencies and Medicaid (U.S. Department of Health and Human Services Administration for Children & Families, 2022)	
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	Collecting Data and Sharing Information to Improve School-Justice Partnerships (National Council of Juvenile and Family Court Judges, 2017) The Council of State Governments Justice Center. Information Sharing in Criminal Justice–Mental Health Collaborations: Working with HIPAA and Other Privacy Laws (Petrila, J. & Fader-Towe, H., 2010)	
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: Colville Confederated Tribes Code, Section 3-4-3(c)

Additional Guidance & Resources	Disclosure of Confidential Child Abuse and Neglect Records (Child Welfare Information Gateway, 2022) Data Sharing for Courts and Child Welfare Agencies (Administration for Children & Families, 2018) Reimagining Data at ACF (Administration for Children & Families, 2018) Data Sharing Policy Letter 17-02 (Administration for Children & Families, 2017) Data Sharing Between TANF and Child Welfare Agencies (Office of Family Assistance, 2015) TANF and Child Welfare Programs: Increased Data Sharing Could Improve Access to Benefits and Services (U.S. Government Accountability Office, 2011)	
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	Behavioral Health Data Exchange Consortium, ONC State Health Policy Consortium Project (2014)	
Data Sharing	Some states have passed laws to facilitate data sharing among state agencies.	Indiana: IC 4-3-26 et seq.
Additional Guidance & Resources	UNC School of Government. Internal Sharing of Information Within a County Department of Social Services (Nickodem, K., 2022) Balancing Client Privacy with First Amendment Rights in Local Health Department Clinics (The Network for Public Health Law, 2021) Summary of State Laws that Facilitate Data Sharing Among State Agencies (The Network for Public Health Law, 2019) Data Privacy, Data Use, and Data Use Agreements (DUAs) (Center for Medicare & Medicaid Services, n.d.)	
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: §§ 10-234aa et seq.

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	Improving Data Sharing for Tribal Health: What Public Health Departments Need to Understand About HIPAA Data Privacy Requirements (Milam, S., 2021) Policy Brief: Native Nation Rebuilding for Tribal Research and Data Governance (Hiraldo, K., Russo Carroll, S., David-Chavez, D., Jager, M., Jorgensen, M., 2021) Webinar: Charting a Path Forward for Responsible Data Sharing (National Congress of American Indians, 2019) Tribal Public Health and the Law: Selected Resources (Centers for Disease Control and Prevention, 2016) Tribal Epidemiology Centers Designated as Public Health Authorities Under the Health Insurance Portability and Accountability Act (Centers for Disease Control and Prevention, 2015)	

APPENDIX D:
Sample Executive Orders and Legislation to Facilitate Data Integration

State & Tribal	
Connecticut	Authorizing Legislation establishing a Chief Data Officer: https://cga.ct.gov/current/pub/chap_050.htm#sec_4-67p
Indiana	Executive Order: https://www.in.gov/gov/files/EO_17-09.pdf Authorizing Legislation for Agency to support Data Integration: http://iga.in.gov/legislative/laws/2021/ic/titles/004#4-3-26-1
Massachusetts	Legislation facilitating the exchange of data to understand opioid epidemic: https://malegislature.gov/Laws/SessionLaws/Acts/2015/Chapter55
Michigan	Executive Order: https://www.michigan.gov/documents/snyder/EO_2016-24_546395_7.pdf
Ohio	Executive Order: https://governor.ohio.gov/media/executive-orders/2019-15d
Pennsylvania	Executive Order: https://www.pa.gov/content/dam/copapwp-pagov/en/oa/documents/policies/eo/2016-07.pdf
Tribal	Resolution: https://oneida-nsn.gov/wp-content/uploads/2016/02/01-12-05-A-Open-Records-and-Open-Meetings-Law.pdf
Local	
Baltimore City, MD	Authorizing Legislation: https://mgaleg.maryland.gov/2022RS/bills/hb/hb1276E.pdf
Montgomery County, MD	Authorizing Legislation: https://health.maryland.gov/psych/pdfs/Medicalreports.pdf
Philadelphia, PA	Executive Order: https://www.phila.gov/media/20220330152115/executive-order-2022-02.pdf

APPENDIX E:
Selected Case Law

The following are a sampling of court opinions related to data breaches. This resource is not intended to be exhaustive.

Unauthorized Access and Data Breaches

Clemens v. ExecuPharm Inc., 48 F.4th 146 (2022) (holding that plaintiff had standing to assert claims related to a data breach where a known hacking group intentionally stole and published sensitive personal and financial information on the Dark Web).

AFGE v. OPM (In re United States OPM Data Sec. Breach Litig.), 928 F.3d 42 (2019) (holding that plaintiffs had stated a claim for damages under the Privacy Act and that OPM waived its sovereign immunity by knowingly refusing to establish appropriate information security safeguards).

McCombs v. Delta Grp. Elecs., Inc., 676 F.Supp.3d 1064 (2023) (holding that employee who sued employer for a computer breach failed to allege an injury that was fairly traceable to employer's actions).

Negligence and Breach of Contract Claims

In re Shields Health Care Group, Inc. Data Breach Litigation, 721 F.Supp.3d 152 (2024) (holding that the provider violated contractual obligations implied in law to protect patients' private medical information).

Miller v. Syracuse Univ., 662 F.Supp.3d 338 (2023) (holding that plaintiff had sufficiently alleged an injury-in-fact where data branch exposed his sensitive information to cybercriminals, which is analogous to the common-law tort of public disclosure of private information.)

McKenzie v. Allconnect, Inc., 369 F.Supp.3d 810 (2019) (holding that employer had a duty to prevent foreseeable harm to its employees and to safeguard their sensitive personal information from unauthorized release or theft).

Impact and Consequences of Data Breaches

In re Fotra File Transfer Software Data Security Breach Litig., 749 F.Supp.3d 1240 (2024) (addressing a data breach that exfiltrated protected health information (PHI) and personally identifiable information (PII) of millions of customers).

In re NCB Mgmt. Servs., Inc. Data Breach Litig., 748 F.Supp.3d 262 (2024) (court dismissed complaint by plaintiffs who sued for negligence after PII was compromised in ransomware attack affecting over 1 million individuals).

Toretto v. Donnelley Fin. Sols., Inc., 583 F.Supp.3d 570 (2022) (finding that economic loss doctrine did not bar negligence claim in data breach case where breach exposed sensitive information, including Social Security numbers and financial data, and some plaintiffs experienced fraudulent activity following the breach).

APPENDIX F:
Checklist for Conducting a Data Sharing Agreement (DSA) Inventory

Overview:

Before local governments and organizations can safely and responsibly share data, they must first understand what data they have, where and how the data are stored, and the legal requirements surrounding those data. Importantly, entities need to be aware of and understand the agreements that help to facilitate the use and access of these data. Conducting a data sharing agreement (DSA) inventory is a crucial initial step in this process. DSA inventories can help institutions identify existing agreements, assess their legal and policy implications, and ensure compliance with relevant laws and standards. This checklist provides a structured approach to cataloging agreements, capturing key terms and obligations, and evaluating alignment with current data-sharing practices.

Rationale:

Conducting a thorough audit/review of all existing data sharing agreements is a herculean undertaking for many organizations. Local governments and other institutions charged with collecting administrative data enter into thousands of contracts a year, many of which are owned by different personnel in different departments. Attempting to identify and catalogue these agreements will require significant personnel time. However, the benefits are significant.

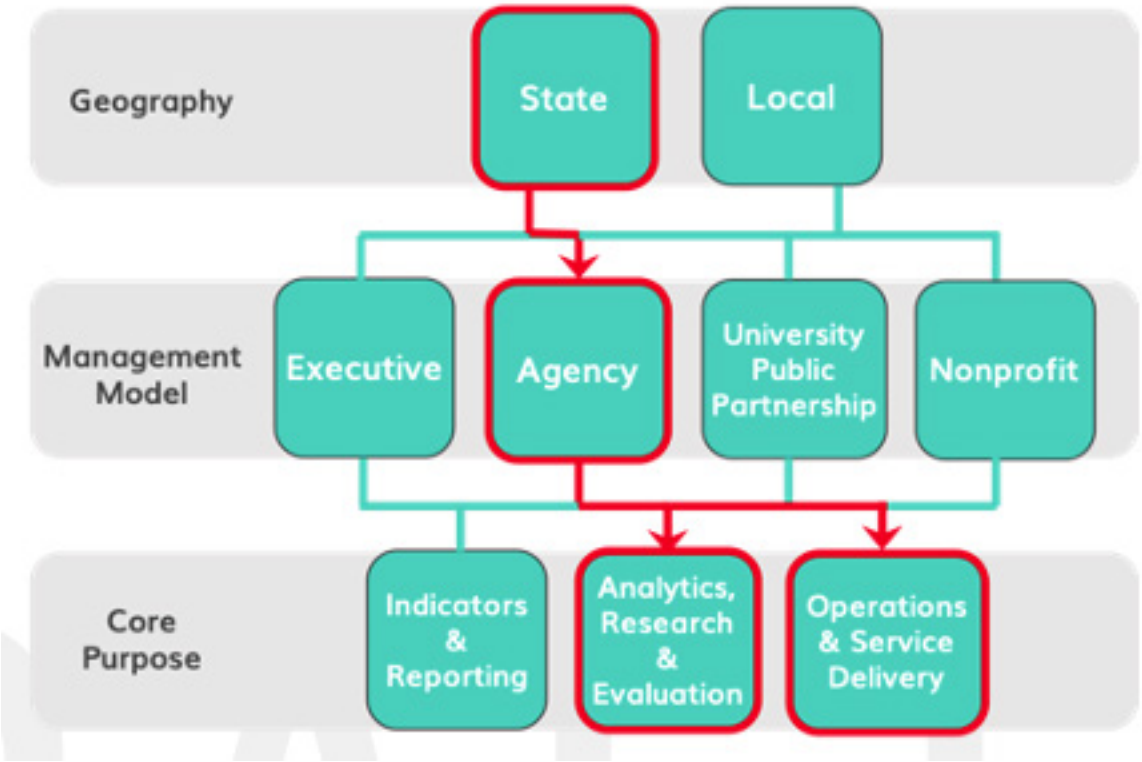
Conducting a DSA inventory can help mitigate legal and compliance risks by ensuring that your organization can quickly respond to legal inquiries, audits, or public records requests. Because DSA inventories provide visibility into who has access to what data, organizations can craft better data governance and security protocols that reduce the risk of breaches or misuse. DSA inventories support operational efficiency over time by saving on the time it takes to locate agreements and assess terms. DSA inventories also reduce the reliance on institutional memory and ensure continuity during staff turnover. Finally, DSA inventories help to support more accurate reporting by providing better documentation to demonstrate how shared data supports outcomes and impacts.

Steps	Considerations & Questions
Locate and catalogue agreements.	· Who generated the contract? · Where does this contract live? · Are there data-sharing terms nestled in other contracts? (SaaS, software, clinical agreements, etc.) · Is there a searchable database for agreements?
Identify key terms.	· Who are the parties? · What data is involved? · How is data being shared? Stored? Maintained? · What are the data elements? · Is the data HIPAA-covered? · Who maintains ownership of the data? · What rights (if any) exist regarding redisclosure? · What are the means of destruction? · What is the term of the contract?

Assess risks and gaps.	· When was this contract signed? · Who was the signatory? · Did the signatory have the legal authority to bind the organization? · Who is personally liable in the event of a breach?
Take action and prioritize.	· Are the agreements aligned with current organization priorities and strategies? · Are there any agreements we need to terminate or modify? · What departments should we follow up with? · What internal processes and controls should we implement?

APPENDIX G:
Sample Legal Definitions for Legal Framework for State IDS

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.

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 H:
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	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.
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 I:
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

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

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.

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.

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.

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.

3. Definitions

See APPENDIX E

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

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.

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.

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.

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.

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.

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 be _____, 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 J:
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	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. 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.
8	Modification; Assignment; Entire Agreement	Establish relationship of this agreement with other understandings or agreements between the parties. Set forth the process for amending the DUL.
9	No Further Obligations	Clarify that there are no additional obligations created by the Agreement—namely, the obligation to enter into future agreements or furnish future data.
10	Compliance with Law, Applicable Law	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.
11	Term of Agreement	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.
12	Use of Name	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.
13	Definitions	Define key terms in this agreement. Include even standard terms if there is potential for misinterpretation.
14	Indemnification	Specify whether the parties will indemnify or defend one another for breach or loss.
	High Value Data Asset Inventory	Compile list of data that have been identified by Data Provider as a strategic asset.
	Confidentiality Agreement	Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description).
	Approved Data Use Priorities	Enumerate the specific uses and priorities to support IDS data access and use.

APPENDIX K:
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:

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

Attachment B:
State's Office of Data Integration

Confidentiality Agreement

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: _____

Telephone: _____ Email: _____

Attachment C:
Approved Data Use Priorities

Approved Data Use Priorities: Enumerate the specific uses and priorities to support IDS data access and use.

1. State's Office of Data Integration (OODI) 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.

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 L:
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	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.). 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."

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?
9	Accountability: Unauthorized Access, Use, or Disclosure	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. 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.
10	Data Use License Reporting Requirements	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. May also wish to include provisions for an evaluation of the Data Licensee process and use of the shared data, if desired.
11	Data Retention and Destruction	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.

12	Term & Termination	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.
13	Indemnification	Specify whether the parties will indemnify or defend one another for breach or loss. *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.
	Data Use License Request Form	Form by which Data Recipient requests a DUL. Form specifies requested data, data output, purpose and use.
	Certification of Data Use License Completion & Destruction of Data	Certification that confirms that access to data has been rescinded and confirms data has been destroyed.

APPENDIX M:
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 ("OODI") in its capacity as the Integrated Data System of the State (StateIDS) Lead Agency and _____("Data Recipient").

This DUL addresses the conditions under which OODI 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 OODI 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. OODI 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. OODI 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-dentification 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.

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 6/15/25)

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: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

Name: _____ Role: _____

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 _____ 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:

A

APPENDIX N:
Sample Consent Form

Template for Universal Consent & Authorization to Share Data

Client/Child/Student Name: _____

Date of Birth: _____

Organization/Agency/Institution: _____

Relationship to Individual (if signing for someone else):

❏ Self ❏ Parent/Guardian ❏ Legal Representative ❏ Other: _____

To provide effective services, support research efforts, and improve coordination among partner agencies, we request your permission to share and receive information about you and/or your child with trusted service providers, organizations, and researchers.

What You Are Agreeing To

By signing this form, you give us permission to:

- ❏ **Collect information** from you, your child's school, healthcare providers, and/or other agencies involved in providing services.
- ❏ **Share relevant information**, such as name, date of birth, demographic information, service enrollment, or progress updates, with participating partners.
- ❏ **Use your information** to improve services provided to you and/or your family; to coordinate services provided to you and/or your family, including referrals; and to evaluate how to better serve you and/or your family.
- ❏ **Use de-identified or aggregate information** (information with no names or identifying details) for evaluation, research, reporting to funders, and continuous improvement of services.

Information That May Be Shared

I agree that the following information can be shared:

- ❏ Demographic information (e.g., name, age, contact information)
- ❏ Education Records (grades, attendance, dates of enrollment)
- ❏ Health and Mental Health Information
- ❏ Admission and Discharge Information
- ❏ Service Enrollment and Participation Details
- ❏ Program Referrals, Eligibility, and Outcome Tracking
- ❏ Family or Household Information Relevant to Services

Participating Partners

(Please check each category you authorize us to share information with.)

Partner Type	Example Services	Check to Consent
Local Schools and Educational Institutions	Academic support, special education	❑
Health Clinics and Public Health Agencies	Screenings, immunizations, check-ups	❑
Mental Health Providers	Counseling, behavioral services	❑
Nutrition and Food Access Programs	Food distribution, nutrition education	❑
Legal and Immigration Support Services	Legal aid, documentation assistance	❑
Early Childhood or Family Support Programs	Parenting education, early intervention	❑
Other:		❑

What Will NOT Be Shared Without Further Consent

- No personal information will be sold or used for marketing or fundraising.
- We will never sell your data.
- No information will be shared with immigration or law enforcement unless required by a valid court order or subpoena.
- No identifiable information will be publicly disclosed.
- If information must be shared with a partner not named in this agreement, **[Insert Organization Name]** will request additional consent.

Your Rights

- You may **refuse to sign** this form. Refusing will not affect your eligibility for services.
- You may **revoke consent at any time** by providing written notice to **[Insert Organization Name]** or the referring agency.
- You have a **right to correct** a record that has errors.
- You have the right to inspect or **request a copy** of shared information or ask how it is being used.
- You **retain rights** under federal and state laws, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) (for health data) (45 C.F.R. Part 164) and Family and Educational Rights and Privacy Act (FERPA) (for education records) (20 U.S.C. § 1232g; 34 CFR Part 99), where applicable.

Duration of Consent

This authorization remains valid for one (1) year from the date of signature unless otherwise specified below or revoked in writing earlier.

❑ I wish to set a different expiration date: _____

Security

Your information will be kept confidential and secure through **[Insert Organization Name]**'s data protection practices and those of our participating partners.

Acknowledgements and Signature

- I have read and understand the terms of this consent form. I voluntarily authorize **[Insert Organization Name]** and its partners to collect, use, and share information as described above.
- I understand that if information is shared with an organization not covered by federal privacy regulations (e.g., HIPAA or FERPA), it may no longer be protected and could be subject to re-disclosure.
- I understand that I have the right to inspect the information to be released.

Signature of Client or Legal Guardian: _____

Printed Name: _____

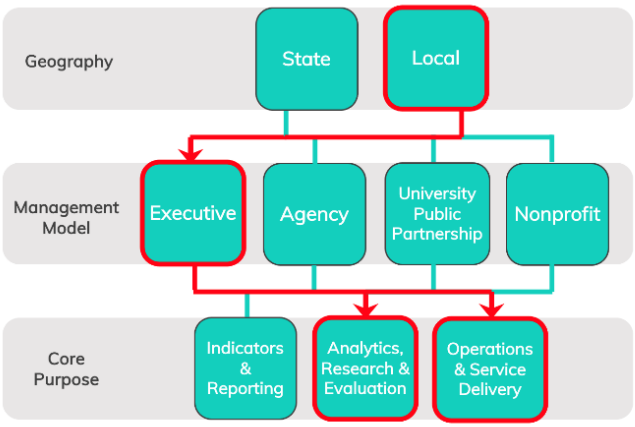
Date: _____

APPENDIX O:
Additional Management Models

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.

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

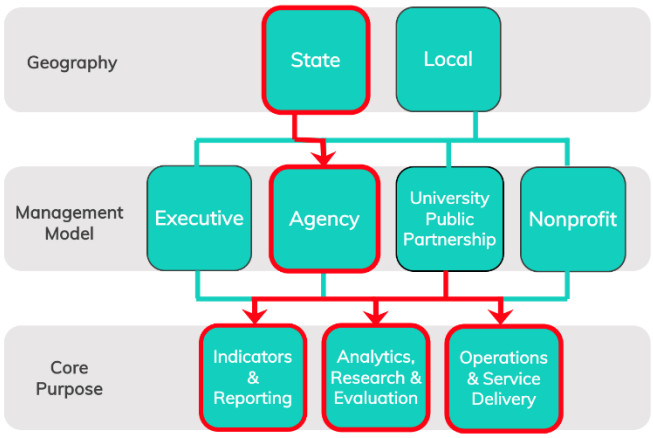
Data Partners: City agencies and service providers

Legal Authority: Executive Order 114, contracts

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

The Rhode Island EOHHS Data Ecosystem uses 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 comprises a team of personnel responsible for the leadership, management, and technical and operational oversight of the program. An inter-agency MOU is in place, which outlines the data sharing process and permissible uses for cross-agency data. Inquiry projects are prioritized through the Learning Agenda and the governance process. Several high-impact uses have been conducted, including projects focused on substance use disorder, fatal overdoses, and child maltreatment prevention.

Rhode Island EOHHS
State, Agency



Learn more about Rhode Island EOHHS here.

Lead Agency: Executive Office of Health and Human Services

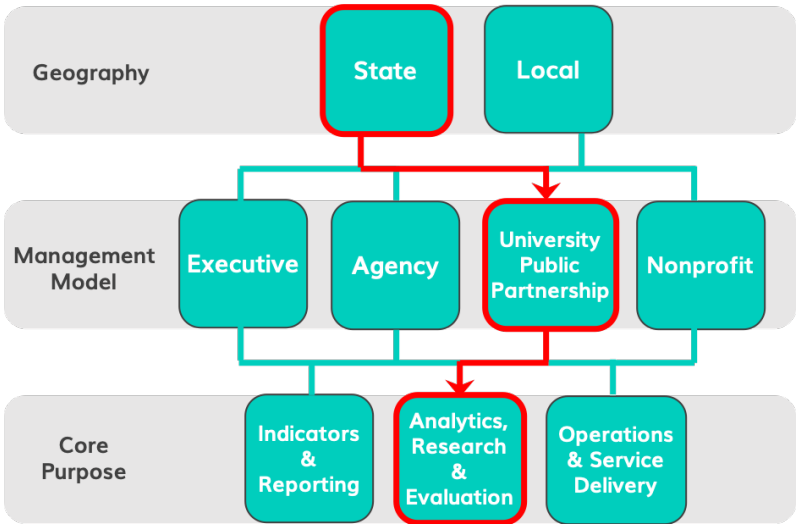
Data Partners: Department of Human Services; Department of Labor and Training; Department of Health; Department of Behavioral Healthcare, Developmental Disabilities, and Hospitals; Department of Youth, Children, and Families; Department of Corrections; and the RI Coalition to End Homelessness

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

The Institute for Research on Poverty (IRP) is a multi-disciplinary research center at the University of Wisconsin–Madison. IRP affiliates examine poverty causes, consequences, and relevant social policy. IRP has assembled linked data resources in the Wisconsin Administrative Data Core (WADC) to support this research.



Learn more about IRP here.

Learn more about WADC here.

Lead Agency: University of Wisconsin–Madison

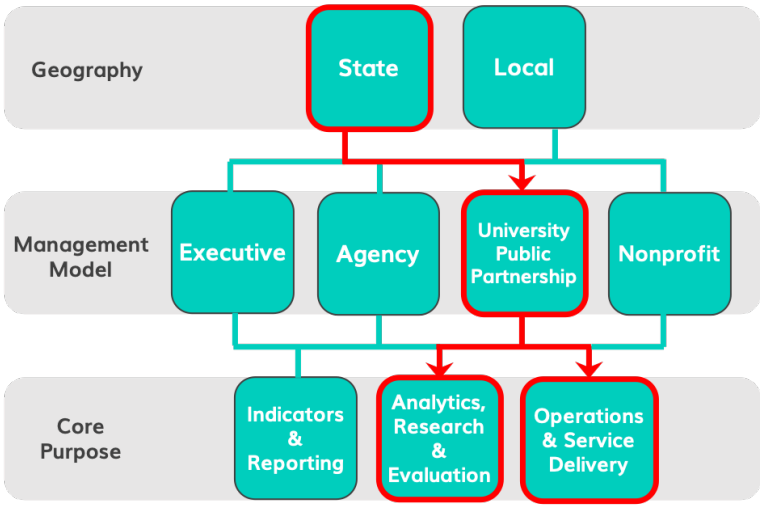
Data Partners: Department of Children and Families, Department of Health Services, Department of Workforce Development, Department of Corrections, Department of Public Instruction, Milwaukee County, Wisconsin Court System, and the Wisconsin Homeless Management Information System

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

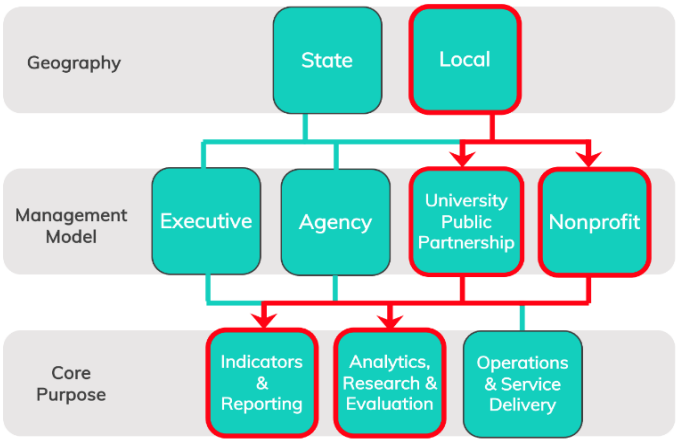
Data Partners: Birth and Death Records (CDPHE), Child Welfare (CDHS), Early Intervention (CDHS), Childcare subsidies (CDHS), EC Workforce Data (CDHS), Postsecondary Education (CDHE), Juvenile Justice Services (CDHS), Juvenile Courts (Judicial), Adult Court (Judicial), Denver Police Department (DPD), 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

Charlotte Regional Data Trust
Local, Nonprofit & University Public Partnership

The Charlotte Regional Data Trust (Data Trust) is located within the University of North Carolina at Charlotte. It houses an integrated data system created to increase the community's capacity for data-informed decision-making and foster university research that impacts the community and deepens understanding of complex community issues. The Data Trust serves as a resource to benefit the greater community. By linking data across siloes, the Data Trust allows researchers and agencies to better describe, understand, and serve the community, particularly groups overrepresented in administrative data.



Learn more about the Charlotte Regional Data Trust here.

Lead Agencies: Charlotte Regional Data Trust + 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

Actionable Intelligence for Social Policy
University of Pennsylvania
3701 Locust Walk, Philadelphia, PA 19104
www.aisp.upenn.edu