AISP

## Network Survey Series

# LEGAL

AISP supports the ethical use of individual-level administrative data for social policy change and advocates for the expansion of resources and infrastructure that makes this possible. We help foster cross-sector collaborations, build the relationships and trust that enable and sustain data sharing, and center racial equity. The following brief shares lessons from a February 2023 survey of 37 state and local data integration efforts in the AISP Network. All sites surveyed have some data governance and data sharing agreements in place, but vary widely in maturity, scope, purpose, and approach. Among the 37 survey respondents (19 states and 18 local efforts), there is representation from every major region of the continental U.S. and high representation of coastal states and cities.

**This brief explores how sites approach legal frameworks for routine sharing and linking of cross-sector data.**

**MAY 2025**

Penn Social Policy & Practice
University of Pennsylvania

# Introduction

## Legal Frameworks for Cross-Sector Data Sharing

**Legal Frameworks:** The rules, regulations, and authority that determine why, when, what, how, and with whom data can be shared.

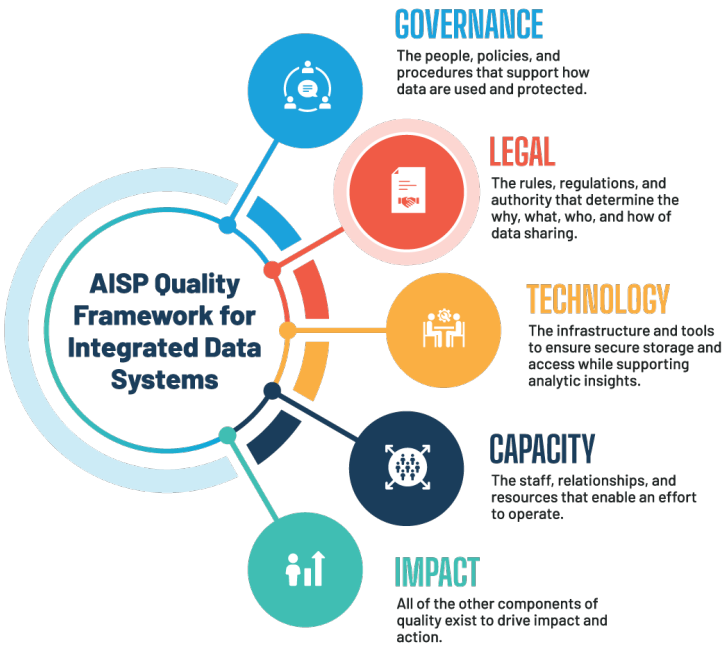
When governments and their partners bring data together safely and responsibly, policymakers and practitioners are better equipped to understand the complex needs of individuals and families and use the resulting information to allocate resources where they're needed most. At the same time, data sharing and integration is not a risk-free endeavor; rather, clear legal frameworks are essential to mitigate potential risks, protect privacy, and guide responsible data use.

As sites in our network know, 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 data (your purpose)**
- **What type of data 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**

In this brief, we will explore the legal authority, legal frameworks and specific agreements that members of the AISP Network use to facilitate data sharing, spelling out the why, what, who, and how.

Legal is the second of five components of quality for integrated data systems (IDS). To learn about the other components of quality IDS, visit **https://aisp.upenn.edu/quality-framework-for-integrated-data-systems/**



# Survey Analysis

## Legal frameworks across the AISP Network

### LEGAL AUTHORITY

Sites in the AISP Network use a variety of forms of legal authority to facilitate interagency and cross-sector data sharing, sometimes employing multiple forms of authority that are mutually reinforcing. Legal authority is often established and memorialized with contracts, covered extensively in the next section. However, legal authority can also rely upon authorizing legislation or executive orders that designate a data integration host, legislation or executive orders that are specific to a priority use case, and agency policies or rules.

A third of sites who responded to our 2023 survey rely on authorizing legislation, while an additional 6 sites (or 16%) rely on legislation specific to a priority use case. Executive orders (EOs) were less common, though they often complemented legislation. We found that EOs are often utilized to jumpstart data sharing efforts or encourage a collaborative planning process, and may precede legislation that then formalizes the effort.


**Legislation can be designed for a variety of purposes, like granting authority to an office or agency to lead cross-agency data use. In Indiana, the Management Performance Hub (MPH) within the Office of Management and Budget (OMB) is tasked by law to collect, analyze, and exchange government information in carrying out the powers and duties of the OMB and the executive state agency sharing the data.**

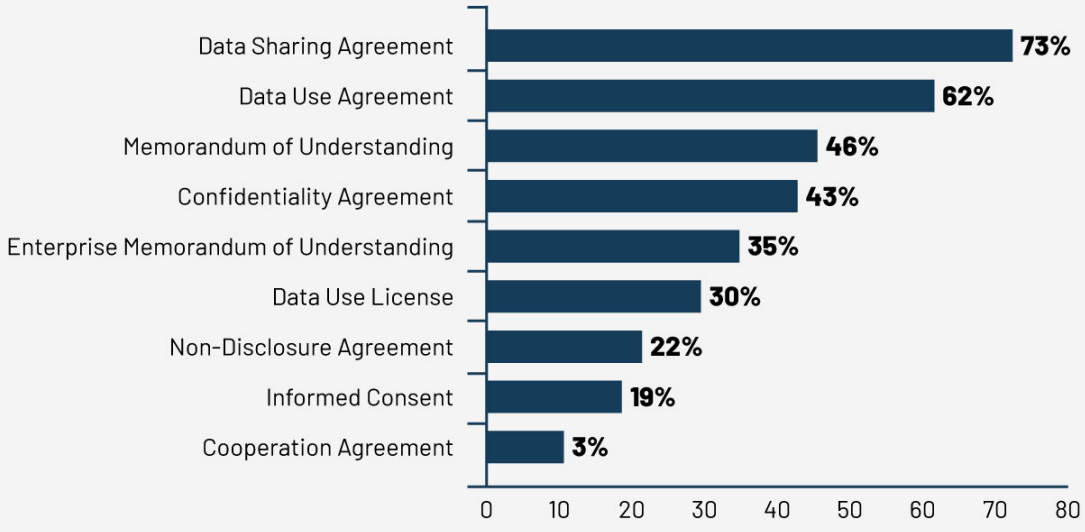
**Legislation can also be used to address a specific state policy priority (for example, Indiana MPH began as an effort to tackle maternal mortality across the state and Massachusetts Chapter 55 legislation kicked off years-long data sharing efforts to monitor and combat the opioid epidemic). Alternatively, legislation can mandate oversight and planning for a state data sharing strategy (like in Connecticut).**

*Learn more about how executive action and different types of legislation enable data sharing and integration in AISP's* **Building + Sustaining State Data Integration Efforts: Legislation, Funding, and Strategies.**

## CONTRACTS

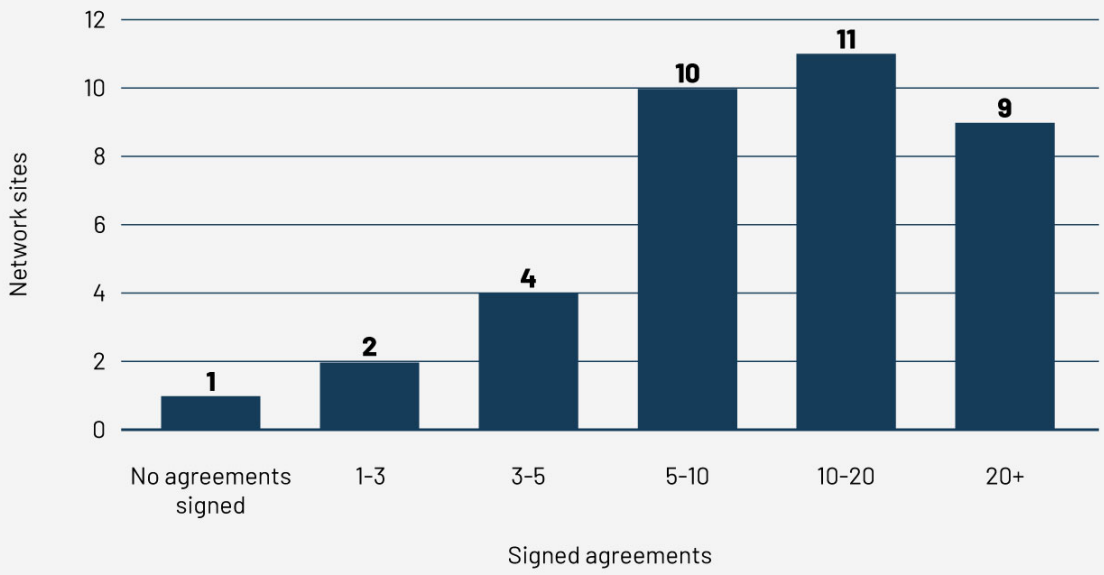
Across the AISP Network, sites have years of experience designing contracts to facilitate data sharing. There are many types of legal agreements used (see graph below) with most sites using a combination of agreements for different purposes.

### Types of Legal Agreements



Altogether, respondents reported more than 445 current, signed data sharing agreements with partners. That number grows exponentially when considering the lifespan of integrated data systems!

### Number of Current Signed Agreements Per Site

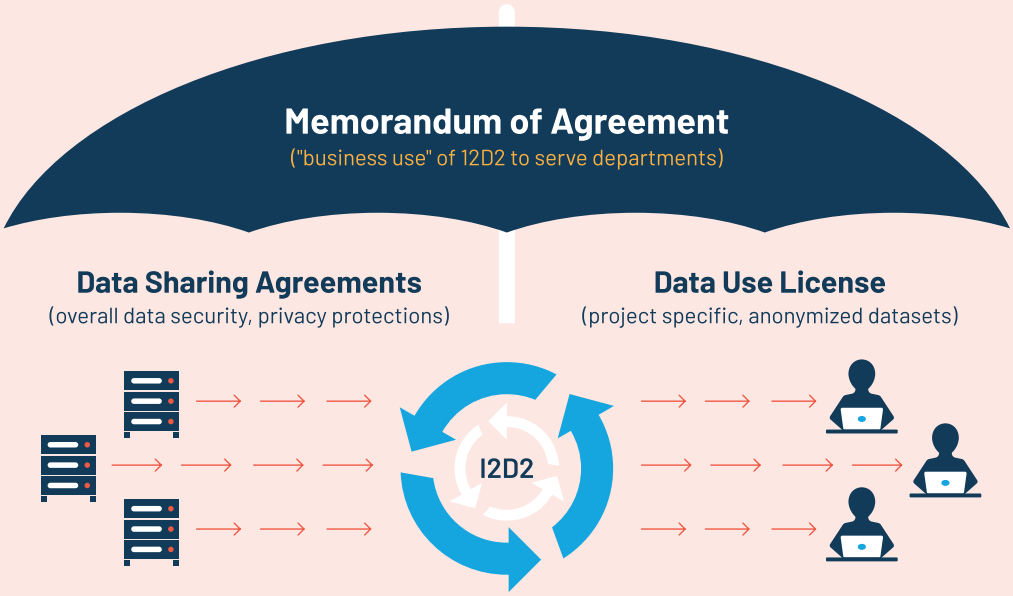



## ONE FRAMEWORK: MULTIPLE CONTRACTS

We recommend a tiered approach to legal agreements, where different types of contracts serve different purposes. A Memorandum of Understanding (MOU) or enterprise MOU (eMOU) is a foundational document that covers the overarching governance process and structure for data access and use, signed by all partners involved. A strong legal framework for cross-sector data sharing should broadly reflect your mission and purpose(s) for sharing, and umbrella documents like MOUs and eMOUs can do just that. This type of document can also clarify the legal authority of the host organization and document data contributing partners' shared commitment to "play in the sandbox." It is important to note, that typically MOUs are not intended to be legally binding.

Data Sharing Agreements (DSAs) usually make up the second tier and are signed by each data-contributing partner and the host agency to specify the general permitted purposes for the data sharing and how data will be transferred, managed and protected. The DSA will also typically outline the legal basis that permits the exchange. The third tier is generally a Data Use License (DUL) that is put into place after a data request is approved to specify how integrated data will be used and outlines the responsibilities of the data user or recipient. The DUL is signed by each data user or recipient. Not all efforts use this exact structure or these specific terms (for example, some sites use a DSA as their foundational agreement instead of an MOU or eMOU, especially places beginning data modernization efforts); however, we find some type of tiered approach to be important to provide appropriate levels of protection and flexibility for routine, ongoing data sharing. Over two-thirds of respondents reported that they currently use a tiered approach, while others are still working in a more ad hoc way.

**Iowa's Integrated Data System for Decision Making (I2D2) utilizes a tiered approach, beginning with an umbrella agreement—a Memorandum of Agreement (MOA)—that authorizes I2D2 to exist in service of the mission of Early Childhood Iowa. Iowa State University, I2D2's host organization, also signs a DSA with each data-contributing agency that references the MOA to detail how data will be securely moved, managed, integrated, and used. Then, for each approved project, a DUL is negotiated between data requestors and the host to specify project parameters, including datasets, variables, research questions, and timeline. Read more in I2D2's governance plan here.**

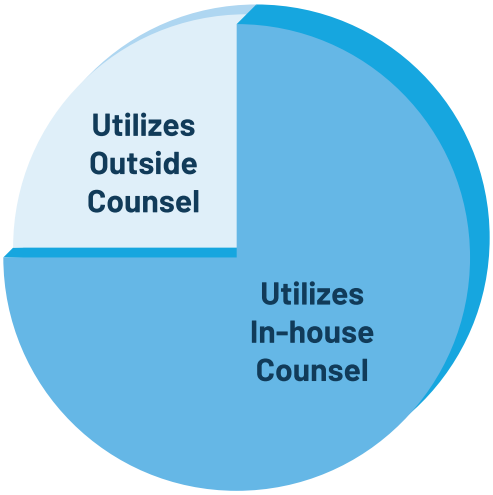


A smaller number of sites are also using supportive ancillary documents—like confidentiality agreements or non-disclosure agreements for staff—to add additional layers of protection and support to their agreement structure for specific use cases. Some sites require informed consent for specific use cases, particularly where client contact is involved. AISP has extensive guidance on this topic, as how consent is collected is often just as important as whether it is required. For more, check out **Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration.**

Finally, it is worth noting that the use of multiple types of contracts across many partners in a data sharing effort can get complicated. Standardizing terms and conditions of access can improve workflow, support insights, and reduce costs. Using standard but modular documents can also increase the flexibility of legal agreements. Two-thirds of sites surveyed use a standard template or model for their data sharing agreements. One in five respondents do not have a legal framework that utilizes tiered agreements. Many of these sites are using standard agreements for some partners or use cases while still developing ad hoc contracts to facilitate sharing and integration.

## The people behind the agreements

Lawyers are essential partners in data sharing efforts and may be housed within an effort or brought in as needed. Lawyers help to determine the legality of use cases, draft and negotiate agreements and mitigate risk for data sharing efforts. According to respondents, three-quarters utilize in-house counsel, while the other quarter utilize outside counsel. In addition, some efforts rely on counsel from partner agencies, university counsel, or legal consultants.




Many lawyers who provide support to data integration efforts are generalists, trained to support a wide range of agency needs and initiatives. As a result, it is not uncommon for legal counsel tasked with supporting state and local data sharing efforts to lack substantive knowledge about legal requirements or secure models for data sharing. Among survey respondents, FERPA was cited as one of the most common barriers to data sharing, alongside interpretations of SNAP, Medicaid and 42 CFR Part 2. Without clear guidance and understanding, counsel may reject data use requests due to perceived (and often misunderstood) legal barriers.

**AISP and the Data Integration Support Center (DISC) offer free, virtual workshops for legal and privacy professionals designed to enhance individual and institutional capacity for data sharing. Recordings and slides from the workshop series are available online, on topics ranging from FERPA and other federal privacy basics to more advanced topics like de-identification and privacy enhancing technologies.**
**See workshop recordings and register for future workshops here.**

Legal counsel spend significant time and effort maintaining relationships with partners and amending agreements. This process can also entail renegotiating and revising agreements to update the framework for new data assets or process needs, to account for improved security or privacy structures, to ensure all partners are happy with the underlying terms, and more. We asked sites if they have a standard renegotiation term, and about half responded yes. Among efforts that have a regular cadence for renegotiating legal agreements, the most common term is 5 years (38%), followed by 19% for both 1- and 3-year terms.

Getting clarity on the roles and responsibilities of all parties involved is an important part of designing legal frameworks and can save lawyers and other agency staff time during later negotiations. Data owners, data stewards, and data custodians each play a different role in the data sharing process. Data owners hold decision making authority over access and use, making their signature on DSAs crucial to data flow and project progression. And yet, reaching an agreement about who qualifies as a "data owner" and keeping track of those designations, can sometimes be difficult. Over 60% of efforts surveyed said they maintain metadata to identify data owners—those with signatory authority—for each partner agreement.

## TRANSPARENCY AND ACCESSIBILITY

While legal frameworks for data sharing are complex and lawyers will need to attend to many details to ensure data sharing complies with all federal, state, and local statutes, AISP urges lawyers to simplify contracts whenever possible. Agreements should be written in plain language so that non-lawyers (including data sharing partners and members of the public) can understand them and more readily engage in conversation and decision making about data use. Survey results show that the use of plain language in legal agreements is increasing but remains a point of growth for the field overall: 44% of sites have legal agreements written in plain language for non-lawyers. Another measure of transparency and accessibility is whether agreements are publicly available. Currently, just over 1 in 3 sites surveyed post their agreement templates or contracts online.

**North Carolina DHHS identifies all three roles—owners, stewards, and custodians— in their data asset inventory. This information is maintained by the NCDHHS Data Office in an internal dashboard and is also made available in the department's public Data Sharing Guidebook. Data stewards are required to update the inventory and Guidebook annually.**

**Connecticut P20 WIN provides a detailed overview of their system and legal agreements on their agency website. Not only are the effort's eMOU and DSA templates available with a supporting map of exhibits and the responsibilities of signatories, but they also provide a data dictionary, learning agenda, annual legal report, "playbook" to guide successful data requests, and more. Explore the webpage here.**

# Looking Ahead

**Clear legal frameworks are essential to mitigate potential risks, protect privacy, and guide responsible data use. Approaches should be tailored to site context and reflect your legal authority and purpose for data sharing.**

By understanding the current landscape of legal frameworks for data sharing across the AISP Network, we hope to inform and inspire all those with an interest in ethical cross-sector data use.

## WONDERING WHERE TO GO NEXT?

- If you'd like to learn more about how legal frameworks fit into an overall strategy for ethical data use, see **Four Questions to Guide Decision-Making for Data Sharing and Integration.**
- For examples and templates for data sharing agreements, see **Finding a Way Forward: How to Create a Strong Legal Framework for Data Integration.**
- Wondering about the role of informed consent in your legal approach? See **Yes, No, Maybe? Legal & Ethical Considerations for Informed Consent in Data Sharing and Integration.**
- Looking to learn more about the federal rules and regulations that govern data access and use? AISP offers the following resources on federal privacy basics:
  - **HIPAA Decision Matrix**
  - **FERPA Decision Matrix**
  - **Demystifying 42 CFR Part 2**

## A NOTE ON THE DATA

To improve data quality, initial survey results have been supplemented with document review and qualitative research. Some responses have been omitted since we first presented on these findings to better represent the current state of the field. If you have questions about any of these changes, please reach out to the AISP team at **aisp@sp2.upenn.edu**.

**Suggested citation:** Berkowitz, E., Kemp, D., Jenkins, D., Hawn Nelson, A. (2025). Network Survey Brief: Legal. Actionable Intelligence for Social Policy, University of Pennsylvania. **www.aisp.upenn.edu**