Legal Issues for IDS Use: Finding a Way Forward

Actionable Intelligence for Social Policy, **Expert Panel Report**

Prepared by

John Petrila, Barbara Cohn, Wendell Pritchett,
Paul Stiles, Victoria Stodden, Jeffrey Vagle,
Mark Humowiecki, and Natassia Rozario

MARCH 2017

ACTIONABLE INTELLIGENCE
FOR SOCIAL POLICY

Actionable Intelligence for Social Policy
University of Pennsylvania
3701 Locust Walk, Philadelphia, PA 19104
215.573.5827 | www.aisp.upenn.edu

Table of Contents

Table of Contents

I. Introduction

As our society becomes increasingly diverse and complex and resources become more constrained, there is a strong consensus in favor of using integrated data systems (IDS) to achieve more effective, efficient, and responsive government. IDS link administrative records from multiple agencies to give a broader view of social problems and policy solutions, while providing robust privacy and data security safeguards. IDS are not only appropriate and legal, but can also provide essential capabilities in furthering the core governmental functions of audit, evaluation, research, and evidence-based practice in public programs and policy. *The issue is no longer whether we should integrate data, but how to integrate such that legal barriers and concerns can be addressed.*

This paper offers practical insights to enable governmental agencies and other parties to develop the foundational legal documents for an IDS. The two primary foundational legal documents are the memorandum of understanding (MOU) and data use license (DUL). The MOU is the agreement among the parties that are contributing data to the IDS ("Data Contributors") and the party that is administering the IDS ("Lead IDS Agency"). The DUL is the agreement between the IDS and a researcher, evaluator, or other outside party ("Data Licensee") that sets forth the terms and conditions under which it may gain access to data from the IDS for a specific purpose.

These foundational legal documents can only be developed after the parties have come to a shared understanding of the goals and structure of the IDS they wish to create. *IDS Governance: Setting up for Ethical and Effective Use* (Gibbs et al., 2017) describes processes to engage the myriad stakeholders involved in an IDS, build trust and cooperation among the parties, develop a shared vision, mission, and goal, and then execute that shared goal. The lawyers responsible for drafting the legal agreements should be included as part of this process to build their commitment to the shared goal, to address legal questions along the way, and to ensure that the legal agreements reflect the consensus of all involved parties.

This report is premised on the following propositions:

1. IDS are consistent with federal and state legal principles and can be established without compromising individual privacy.
2. An IDS is designed to maximize appropriate access to data and transparency while protecting privacy.
3. IDS are essential to promoting government efficiency and innovation by improving core government functions, including audit, evaluation, budgeting, effective and efficient provision of services, and informed decision making.
4. Numerous jurisdictions have established IDS and have seen demonstrable improvements in population health, social well-being, and government efficiency.
5. There is a growing federal and public mandate for the establishment of IDS that is closely connected to the promotion of evidence-based practice.

This paper has five sections. The first makes the case for *developing an IDS as a tool to integrate data to drive sound social policy.* The second section underscores the importance of understanding the politics and relationships behind creating MOUs and DULs. The third section outlines some of the components that must be considered when planning an IDS, including advice on getting parties to discuss and agree upon key aspects of an IDS. The fourth section offers guidance on the core components of MOUs and DULs, and provides templates for each with sample language. Finally, specific state and federal laws on privacy and confidentiality that are frequently implicated when establishing an IDS are included for reference.

II. The Decision to Build an IDS: Making the Case for the IDS

The first step is deciding to build an IDS. When making the case for establishing an IDS, it is important to highlight that *integrating data drives sound social policy.* Breaking through data silos and categorical boundaries will result in the transformation of raw data into actionable insight by providing a 360-degree view of data and services across sectors.

1. The collection of massive amounts of data creates opportunity. Government plays multiple roles depending on the jurisdiction and issue. Many departments and agencies already collect large troves of data. This creates an opportunity to link the data already being collected to achieve cross-sector understanding, collaboration, and impact. Government provides services, funds services through private contractors, audits services, and evaluates publicly funded programs. As a result of these multiple activities, every level of government possesses enormous amounts of administrative data in electronic format. In some situations, for example, reimbursement for services provided in a Medicaid program, government *requires* the creation and transfer of electronic data. In other situations, when government provides services such as education, government *generates* electronic data about student performance. In still other situations, through legislation such as the Affordable Care Act, government *stimulates* a rapidly expanding private/public market in generating, storing, and integrating electronic data. And, of course, electronic data are ubiquitous in virtually any sector of the economy that relies on reaching large numbers of people, from marketing to the delivery of goods. These multiple sources of data create unprecedented opportunities for government to significantly improve its core functions.

2. Complexity creates demand. Many citizens interact with multiple public programs (education, health, employment, social services, etc.). This overlap in public programs and services creates a demand for integrating and using data both within and across program boundaries to better understand and meet the needs of distinct populations. The goals of vertical and horizontal integration recognize that human problems and issues are not a series of discrete conditions, each occupying its own silo. A “whole person” approach to program implementation examines all the needs of a target population. A “whole population” approach for the effective and efficient delivery of services looks at the needs of an entire community. Individual and community needs do not fit neatly into compartments; they spill over programmatic lines and established bureaucratic procedures. Real life is complex and nuanced.

3. The imperative for government to ensure quality care and services in the face of rising costs and limited resources creates demand. In an era of shrinking and constrained resources, it is imperative that government act efficiently and effectively in creating, overseeing, and evaluating its investments to ensure that quality services are being delivered. There is a bipartisan consensus that integrated data systems enable both the planning and evaluation necessary to achieve the highest state of community social health for the greatest number of people. Community social health, broadly defined, is fundamental to the economic and social prosperity and health of the individual, family, community, and state.

III. Politics and Relationships

After deciding to establish an IDS, stakeholders must consider issues of politics, trust, and relationships, all of which form the backdrop for the IDS. Ultimately, the IDS requires more than just the executed legal agreements, but also a spirit of cooperation. This section will provide the tools to help lawyers engage in a process of building trust, and posit rebuttals to some of the most common arguments made in opposition to data sharing. We discuss the most frequent objections to developing an IDS in the table and section below.

Table 1: Addressing common legal concerns and myths

Objection	Response
A. This is not legal.	This is legal. All federal (and most state) laws authorize data sharing for appropriate governmental and research purposes. (Section VI provides more specific authority based on the particular data type and governing laws.)
B. This pits individual interests against societal interests.	A well-constructed IDS will balance individual and societal interests in a legal, ethical, and politically feasible manner. While individuals have a strong interest in data privacy, they have an equally strong interest in effective and efficient government programs and policy. An IDS preserves individual privacy through policies and procedures that include de-identification, as appropriate, and data security, while helping to ensure that government carries out its functions in the most effective, appropriate, and high-quality manner possible.
C. This seems like too big of a project and beyond government’s ambit.	Project sponsors should define a clear scope and articulate systems for how the IDS will be and will not be used. IDS can make government more efficient and effective at core functions: · Audit · Evaluation · Research · Operations · Budget and policy making Government continues to own the information it generates or possesses as part of its functions. Government is not giving up control over data; government is simply sharing data to further legitimate governmental purposes. Note: Government can also elect to partner with universities or other non-profit entities to administer an IDS based on a determination of what institution is most capable of performing this function.
D. This is uncharted territory.	Integrated data is happening all over the country and is endorsed at the state and federal level. In 2016, the Evidence-Based Policymaking Commission Act of 2016 (H.R. 1831) became law. Its goal is to “focus on the most basic pre-requisite for evidence-based policy: good data.” The National Conference of State Legislatures has prioritized opening government data for public use, including integrated data. The Conference maintains websites devoted to highlighting states that have prioritized expanded use of government data and data transparency on state expenditures or contracts.

Objection	Response
E. This requires obtaining individual consent to re-disclose data, which is not administratively feasible.	Most data privacy laws allow the agency holding the data to use or share that data, including personal identifiers, for research or policy-making purposes without obtaining individual consent. While some agencies may wish to update their notice of data privacy or equivalent disclosure to mention the integration of data for public purposes, this is not generally a legal requirement.
F. This makes a data security breach likely.	Data security is always an important consideration whenever government collects and stores data. High-quality IDS place a premium on data security. In most cases, the data security provided by the IDS is stronger and more robust than that applied to the data in their original location. The model MOU and DUL contain rigorous data security requirements to ensure that data are protected.
G. This exposes us to too much liability . . . we are going to get sued.	The major data privacy laws (e.g., Health Insurance Portability and Accountability Act [HIPAA] and Federal Education Rights and Privacy Act [FERPA]) not only allow and encourage data sharing for these purposes, but also do not contain a private right of action for individuals to sue over a data breach or misuse of private data.

A. Common Concerns

1. This is not legal.

Legal issues are consistently identified as a significant barrier to creating IDS; however, all federal laws (and most state laws) allow for the sharing of data, even individually identifiable information, for certain purposes.

Certainly, misunderstandings about law have resulted in myriad interpretations about what kind of interagency data sharing is legally allowable, what is restricted, and how law and policy define the roles and responsibilities of each involved agency or entity. These law-based challenges result from a variety of factors, including (a) misinterpretation of laws and policies, (b) inconsistent federal, state, and local laws, (c) ambiguous federal, state, and local laws, (d) absence of clear statutes/regulations/case law, (e) fear of litigation, and (f) long-standing cultural trends, norms, and policies within an organization.

Data sharing is often clouded in confusion that, in the face of ambiguity, gives rise to a culture that is risk averse beyond the actual risks posed by legal rules—where progress and opportunity for improved outcomes is deferred in lieu of the status quo. In effect, this sanctions an environment of paralysis where information silos are maintained, perpetuating a fragmented system of health and human service delivery.

The goal of the IDS is to facilitate data sharing while ensuring that information exchange rests on a solid legal framework. It relies on the presumption that, as long as certain protective structures are in place, restrictions on the sharing of such data should only be observed when there is a clear legal bar to such sharing. The goal is to adopt legal and organizational policies that create a foundation to support the secure exchange of client data while respecting individual privacy and choice *consistent with law*.

No privacy or confidentiality law is absolute in its protections. The challenge is to apply the law *as it exists* rather than as it is assumed to be. Law plays a crucial role not only in protecting privacy, but also in defining governmental powers and jurisdiction, and in establishing the framework within which electronic information is generated, stored, and shared. The law is a tool that can be used effectively to establish standards of practice to help facilitate quality care and positive outcomes.

2. This pits individual interests against societal interests.

Reluctance to set up an IDS can stem from concerns around balancing individual and societal interests. Government is strongly committed to protecting personal information. At the same time, government also has a responsibility to improve the quality, effectiveness, and efficiency of public services. Government has always had to balance individual interests with the public interest (taxation, security/policing, public health, etc.). The inability and reluctance to share information comes at a significant cost on many levels: unavailability of vital information; difficulty in maintaining continuity of care; inefficient use and waste of resources; and inability to understand the "whole person"/ "whole population" and coordinate services to optimize outcomes.

An IDS can appropriately balance both individual and societal interests. Citizens increasingly expect that public services will be more responsive and better tailored to meet their needs and that public funds will be spent efficiently. Similarly, they have high expectations that their personal information will be safeguarded and fully protected from unauthorized disclosure, identification, or misuse. While there is a strong individual interest in privacy, individuals have an equally strong interest in their well-being in addition to their community's well-being, including having access to the most effective, appropriate, and high-quality services in a timely manner.

IDS operate against this backdrop. Well-executed data sharing agreements provide the foundation to facilitate a secure exchange of information that provides meaningful data through an interoperable information network to advance an effective and efficient service delivery system. Foundational requirements are as follows: (a) data sharing must protect confidentiality and security, and operate within the principles established by governing laws and regulations; and (b) data sharing requires participants to operate within a set of clear protocols that govern who, when, how, and why individuals and entities can access and use data, as well as ensure compliance with regulatory and oversight structures.

3. This seems like too big of a project and beyond government's ambit.

Much of the opposition to an IDS emerges from fears around the scope and complexity of the task. For example, how much of the agency/department's time and money will go into establishing and maintaining the IDS? And will the potential outcomes warrant the investment? It is important to clearly define scope and parameters, articulating very clear principles for how the IDS will be used and for how it will not be used. In addition, it is important to stress that rather than creating additional burdens, the IDS will ultimately serve to streamline and bolster agency/department functions. Many departments, agencies, and public support programs already collect large amounts of data, but lack the infrastructure and resources to use the data effectively. By linking disparate data sets, the IDS would allow these entities to leverage their current data collection efforts without additional burdens.

It is also important to emphasize that the government, as data contributors, still maintains control over the data and will play an important role as gatekeepers to decide how data can be used, and which data can be used in accordance with privacy and security standards. The IDS will be structured under a robust governance structure, which will review its operation and have authority over the ways in which data can be used.[1] A clear governance process ensures the legal and ethical use of this public good.

1 For a discussion of governance approaches and best practices, see Gibbs et al., 2017.

4. This is uncharted territory.

Government hesitation to pursue IDS projects frequently stems from fears that they are entering uncharted territory. Numerous highly functioning IDS, however, already exist. For example, the South Carolina Integrated Data System has been in existence for more than 25 years and collects data from 20 different agencies and programs. The South Carolina program began small and has expanded over time by providing value to government, ensuring the security and integrity of data, and continuously communicating with all of its stakeholders (see *Case Study 1*). Similarly, the IDS in Allegheny County, PA, was established in 1999 and holds over 640 million records (see *Case Study 2*).

Government leaders of all political affiliations have embraced and encouraged the expansion of IDS to facilitate more effective and efficient government. In 2016, U.S. House Speaker Paul Ryan and Senator Patty Murphy drafted the Evidence-Based Policymaking Commission Act of 2016 (H.R. 1831), which passed with bipartisan support and was signed into law by President Barack Obama. The explicit goal of the Commission is to "focus on the most basic pre-requisite for evidence-based policy: good data" (Milner, 2016). The bill creates a 15-person commission to review federal data sources and make recommendations on the optimal structures for data integration, data security, and use of integrated data for "program evaluation, continuous improvement, policy-relevant research, and cost-benefit analyses."

There are also multiple efforts at the state level to encourage greater use of administrative data. For example, the National Conference of State Legislatures has made opening government data for public use, including in combined (that is, integrated) format, a priority. The Conference maintains a website devoted specifically to this topic, which among other things provides links to state legislation addressing the issue.[2] The Conference also maintains a website titled "Statewide Transparency Websites and Legislation" providing links to the 36 states that have tried through legislation or executive action to provide information to the public about state expenditures or contracts.[3] Again, the overarching principle in both federal and state efforts is a commitment to the accessibility and use of public data.

Government is not the only party addressing this issue; for example, the Sunlight Foundation maintains a website that provides links to state efforts to integrate data for public purposes (see Shaw, 2015).

2 See http://www.ncsl.org/research/telecommunications-and-information-technology/open-data-legislation.aspx
3 See http://www.ncsl.org/research/telecommunications-and-information-technology/statewide-transparency-spending-websites-and-legis.aspx

Case Study 1: South Carolina Integrated Data System

The South Carolina Integrated Data System serves as an illustrative example of a statewide IDS with a robust culture for data sharing that ensures compliance with federal, state, and local laws. Nearly 25 years old, the South Carolina Integrated Data System has proven to be an important state resource as evinced by the continued leadership, investment, and commitment to its sustainability and growth.

Established in the early 1990s, the South Carolina Integrated Data System is housed in the Office of Research and Statistics (ORS), which is located in the Budget and Control Board of the State Government. The South Carolina IDS collects data from over twenty state agencies and other organizations, including data from the education department, health department, disease registries, all payer healthcare databases, legal/safety services, social services, claims systems, behavioral health, and other state support agencies. Nearly twenty-five years old, the South Carolina IDS has proven to be a valued state resource, as evidenced by continued leadership, investment, and commitment.

The South Carolina IDS has stringent requirements around FERPA and HIPAA trainings and data transfer protocols, which are stipulated in all MOUs. If interested in using the South Carolina IDS, researchers contact the relevant Office of Research Services (ORS) staff member, who reviews the research proposal. Once the researcher has approval from the appropriate state agency, the researcher must secure permission to use the data. ORS requires external researchers to share their findings with them before they publish any of their results.

Because of the IDS, the state is able to evaluate their programs, identify potential areas for cost savings, devise innovative approaches to enhance program outcomes and policy initiatives, expand the reach of social services to remote parts of the state, and create reimbursement scales that match quality of programs.

The South Carolina IDS attributes its robust culture for data sharing to relationship building. Since its inception, ORS staff have worked tirelessly to maintain their relationships with agency staff and to remain transparent about how data are being stored and used. As ORS Section Chief Dave Patterson articulates, "you have to keep those lines of communication open, otherwise everything breaks down" (Kitzmiller, 2013).

See *Appendix E* for sample South Carolina MOU.

Case Study 2: Allegheny County Data Warehouse

Allegheny is an important example of how integrated data can be used to improve government efficacy. Nearly 17 years old, the Allegheny County Data Warehouse has proven to be a valuable county resource that has only expanded over the years.

Established in l999, the Allegheny County Data Warehouse is housed within Allegheny's Department of Human Services (DHS) and serves as a central repository linking together human services data and other client data to support a wide range of administrative, decision making, and policy activities within and external to DHS. DHS staff members believe that the data warehouse promotes greater transparency, efficiency, and collaboration between DHS caseworkers, clients, and community partners who are vested in the work that DHS does throughout the county.

Expanding over time to include a broad range of data sources, Allegheny County Data Warehouse included 640 million records in 2014 from almost one million individuals that include demographic information (e.g., client name, Social Security number, date of birth and address); service information (past and present services that clients and/or their families receive and service cost); and provider information (e.g., name, location, types of providers, and services delivered).

In terms of research, the Allegheny County Data Warehouse is used to support the internal DHS research agenda as well as the work of external researchers. Before an external research request is approved, DHS requires institutional review board (IRB) approval from both the researcher's institution and DHS to ensure ethical use and practice. DHS staff work closely with external researchers to revise their work so that it includes sound research questions leveraging the strengths of the data housed within their warehouse. DHS also asks external researchers to write policy briefs about their study and findings for a general audience.

Allegheny also serves as a powerful example of how an IDS can overcome seemingly insurmountable barriers. In a project between the Data Warehouse and the Pittsburgh County schools, it seemed that the legal barriers were intractable. Specifically, the School District and DHS attorneys were concerned with issues of confidentiality inherent in sharing student and client data, including the issue of how to legally obtain consent to use student records. The attorneys found a solution in a 2008 FERPA amendment that permitted the release of personally identifiable student data without consent to those organizations interested in conducting research to improve student achievement as long as those organizations had a signed MOU that outlined confidentiality parameters and data use protocol. Ultimately, through developing deep relationships between the school system and DHS, these attorneys were able to tie data to actionable research and found a way to draft a legal agreement that met all of the requirements of FERPA and HIPAA (Kitzmiller, 2014).

See *Appendix F* for sample Allegheny County MOU.

5. Data sharing requires obtaining individual consent to re-disclose data, which is not administratively feasible.

The major data privacy laws generally authorize use of administrative data for public purposes such as evaluation, audit, and research without individual consent under certain conditions. The rationale is that the individual's particular data is not the focus of these inquiries and the risk of disclosure of the individual's information beyond the IDS is extremely low. Although individual identifiers are included in order to link records across data sets, the individual identifiers are protected, and the IDS typically releases only de-identified information to researchers and other Data Licensees.

When research is being performed, the IRB will determine whether individual informed consent is required. The Common Rule[4] allows for waiver of individual consent requirements when:

> The research involves no more than minimal risk to the subjects;
>
> The waiver or alteration will not adversely affect the rights and welfare of the subjects;
>
> The research could not practicably be carried out without the waiver or alteration; and
>
> Whenever appropriate, the subjects will be provided with additional pertinent information after participation (45 CFR § 46.116(d)).

When using existing administrative data in research, the primary risk to individuals is that their confidential information is exposed. The use of de-identified data, the bar on re-disclosure, and the data security protections that are built into the MOUs and DULs usually provide adequate protection to make it a minimal risk. For a more detailed discussion, see *Appendix H*, Memo to Providers on Data Sharing Rules (Allegheny County).

6. This makes a data security breach likely.

Appropriate data security is the best protection against a data breach. A well-designed IDS will include industry-standard data security measures covering administrative, physical, procedural, and technical safeguards.[5] These requirements will include encryption in transit and at rest, to protect electronic data from being intercepted during transfer to or from the IDS or being accessed while stored. Data security within the IDS may be more advanced than the security applied to the original source data. While the risk of a data security event can never be fully eliminated, the Lead IDS Agency can manage these risks through the use of appropriate legal agreements and standard data security and data privacy protections.

7. This exposes us to too much liability . . . we are going to get sued.

The 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.[6] While lawsuits brought by private parties alleging breach of privacy under state law do exist, in general (and particularly with federal laws), government regulators enforce data privacy and security laws. They are principally looking to ensure that entities have the appropriate legal agreements in place and meet the minimum administrative, physical, and technical data security standards. The model legal agreements contained in this paper are designed to help satisfy those legal requirements. Enforcement actions generally focus on patterns and practices of behavior clearly violating legal standards or particularly egregious events.

4 For an explanation of the Common Rule, see https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html#

5 A summary of the administrative, physical, and technical data security safeguards required by the HIPAA Security Rule is available at https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

6 See, e.g., *Abdale v. North Shore-Long Island Jewish Health System, Inc. (Index No. 02367/2013); Dittman et al. v. The University of Pittsburgh Medical Center*, Case No. GD-14-003285 in the Court of Common Pleas of Allegheny County, Pennsylvania.

IV. Planning Tools and Tips

In addition to considering the politics and relationships, the parties must address several core questions to navigate the complexities of creating and sustaining an IDS during the planning process. This section provides some tips and tools for the planning phase of establishing an IDS that will lead to durable legal agreements and ultimately a successful IDS.

A. Stakeholder Group

Before moving to draft and execute legal agreements, the parties should engage in a robust stakeholder engagement and planning process, as outlined in the *IDS Governance: Setting Up For Ethical and Effective Use* (Gibbs et al., 2017).

Through this process, the group can come to consensus on key elements of the proposed IDS that will need to be reflected in the legal agreements. These elements include the specific reasons for creating the IDS, the necessary parties that must be included in the planning process, the organizational structure of the IDS, the data sets required to address the IDS' research priorities, and the legal issues associated with those data sources.

B. MOU Inventory Checklist

It is common for someone within an agency being asked to contribute data to raise legal objections to the formation of the IDS or the sharing of particular fields. Practice has shown the importance of careful review of these objections to address perceived legal barriers and create consensus around the legality of contributing the data. An MOU Inventory Checklist (see *Appendix A*) can enable the planning group or other stakeholders to document, analyze, and resolve legal objections to the sharing of particular data up front. The tool is designed to help promote sharing administrative data by

- enabling agencies to better understand their administrative data elements and characteristics,
- helping evaluate issues relevant to data sharing for current uses, and
- analyzing uses that may differ from the original collection purpose.

V. The Foundational Legal Agreements: The MOU and the DUL

Once the stakeholders have built trust and a shared understanding on some key items, the parties should begin to document these details in formal legal agreements. This section will discuss two such agreements, the memorandum of understanding (MOU) and the data use license (DUL).

A. Parties

For purposes of these foundational legal agreements, there are three major types of parties: Lead IDS Agency, Data Contributor, and Data Licensee.

1. Lead IDS Agency

The Lead IDS Agency is the legal entity that will administer the IDS. Its responsibilities include hosting the technology, employing the IDS staff who support the function and use of the IDS, contracting and working with Data Contributors and Data Licensees, hosting the IDS governance framework, and performing other tasks necessary to maintain a functional IDS.

The Lead IDS Agency may be a governmental agency (e.g., South Carolina Budget and Control Board, Office of Research and Statistics) or an academic or other private institution (e.g., Chapin Hall at the University of Chicago). 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.

The Lead IDS Agency will be a party to all MOUs by which data are contributed by Data Contributors and integrated within the IDS. It will also be a party to all DULs by which data are shared from the IDS with a Data Licensee.

2. Data Contributors

The Data Contributors are the various entities that possess and agree to share administrative data with the IDS. The Data Contributors may be an entire governmental agency or a subdivision within an agency that is responsible for maintenance of a particular data set. In South Carolina, there are 20 Data Contributors, including the Departments of Health, Education, and Health and Human Services. Each Data Contributor will be party to an MOU with the Lead IDS Agency.

In addition to facilitating data transfer to the IDS on a regular basis, the Data Contributor will provide critical information about the data variables to ensure that the data's limitations and definitions are well understood. The Data Contributor may also participate in the governance of the IDS.

3. Data Licensee

An IDS produces value by making data available for various purposes, including performing audit, evaluation, policy making, and research. The Data Licensees are any private or governmental entity that seeks an extract of data from the IDS to pursue one of these functions. Data Licensees may be academic researchers or governmental agencies. The Data Licensee enters into a DUL that sets the specific terms and conditions of the use of the data for a particular project or purpose, usually after such project has been approved through a formal governance process.

B. MOU (Memorandum of Understanding)

The MOU is the foundational agreement among the Lead IDS Agency and the Data Contributors. Note, however, that 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 Contributors. The specific name does not change the substantive terms required in the agreement.

The MOU sets forth the core features of the IDS structure as well as the respective legal rights and responsibilities of each party within the IDS. In the appendix, we provide a model MOU template (see *Appendix B*) and examples of some exemplary MOUs from South Carolina, Allegheny County (Pittsburgh, PA) and Virginia (see *Appendix E, F, G*).

A good MOU will codify both the legal requirements and the operational structure of the IDS. An MOU should be written in plain, simple language so that anyone involved in the IDS (including agency leadership, operational staff, the public) can understand its terms. The Lead IDS Agency can have separate MOUs with each data contributor or can craft a single MOU that all Data Contributors sign. For example, South Carolina has an MOU template that it uses with each Data Contributor, modifying

it depending on the type of data. Virginia has developed a single MOU that all Data Contributors enter. In either case, it is important to include a mechanism to add parties and amend the MOU to accommodate growth in both size and scope of the IDS.

There is no required structure for an MOU. Agencies may have existing templates or structure they want to deploy. We have developed an IDS template that includes more than two dozen provisions that should be part of any IDS MOU; see *Appendix B*. These sections include (a) standard contract provisions (e.g., parties, term, dispute resolution, notice, termination, amendment), (b) provisions setting forth the IDS operating structure (IDS structure, roles and responsibilities, data to be shared), and (c) provisions relating to the legal use and protection of confidential data (legal authority, confidentiality, data security, breach). For each section, the template also includes principles and practice tips for consideration when drafting.

The MOU will need to establish legal compliance under all applicable state and federal laws. The creation of an IDS requires the sharing of personally identifiable information (PII) at the individual level to enable the correct matching of data at the person level. Most state and federal laws permit the sharing of PII for evaluation, audit, and research purposes. The template is written to be flexible to accommodate an IDS that is subject to multiple state and federal data privacy laws and regulations, including HIPAA, 42 CFR Part 2, FERPA, and COPPA.[7] Section VI discusses each of these major data privacy regimes and some unique requirements and considerations that may apply.

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 don't use legal agreements frequently. For example, Allegheny County does not require legal agreements for data sharing among county agencies (e.g., Health and Human Services) because the County is a single legal entity and does not need to contract with itself. The Allegheny County MOU, *Appendix F*, is the exception because it involves the Pittsburgh School District, which is a separate legal entity from the County. *Appendix B* provides principles and practice recommendations that can be adapted to local organizational culture. Some organizations may choose to forego certain provisions as unnecessary.

C. DUL (Data Use License)

The DUL is the other foundational legal agreement involved in an IDS. The DUL sets forth the terms and conditions under which a researcher, evaluator, or other outside party—Data Licensee—may gain access to data from the IDS for a specific purpose. The parties to the DUL are the IDS and the Data Licensee. In the appendix, we provide a model DUL template.

While these agreements can be called Data Use Agreements, we have chosen to refer to them as Data Use Licenses (DUL), to reflect the spirit of other similar licenses such as the Creative Commons family of licenses. Specifically, the language of license emphasizes the limited nature of the Data Licensee's rights to the data. A DUL grants a Data Licensee the temporary right to use a limited set of data for a specific purpose under certain conditions. The Data Licensee does not gain any ownership interest in the underlying data and is limited by the DUL in terms of data use, sharing of data, and practices such as privacy protections and restrictions on de-identification.

A DUL contains many of the same standard contract provisions, including those related to the legal use and protection of confidential data as the MOU. The DUL also contains provisions regarding the terms of the license itself (the specific data elements, the duration of the license, the handling of the data set, etc.). *Appendix C* provides a DUL template that sets forth model language, principles, and practice tips for each section of the DUL. *Appendix I* also includes a model DUL from the Centers for Medicare and Medicaid Studies.

7 Children's Online Privacy Protection Rule (COPPA). 1999. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

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 will be subject to the review of an IRB.[8] An IDS may elect to provide the Data Licensee a de-identified or limited data set in order to limit the release of PII and reduce the risk that an individual can be identified.[9]

VI. Data-specific legal issues

There are discrete statutes and regulations that must be considered in creating an IDS. Some are federal, some are state. Not all of these laws apply in every situation, and on occasion laws may be in apparent conflict. This section simply notes the laws most likely to be relevant to the discussion. For further legal resources by federal and state statute, see *Appendix D.*

A. Specific Laws

1. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA applies to "protected health information" (PHI) and is likely to arise as an issue whenever any type of health information is considered as part of an IDS. HIPAA also has provisions governing the security of electronic data, and those are considered.[10]

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," defined as a "health plan" (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.
- A question always worth considering is 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 in an IDS). HIPAA provides specific information on the "de-identification" of PHI. In addition, HIPAA provides for creation of a "limited data set" (similar but not identical to a "de-identified data set") as an alternative to the use of PHI.

Note that HIPAA provides broad exceptions to confidentiality to permit public health agencies to carry out their functions, for example in disease prevention or control. A discussion can be found on the U.S. Department of Health & Human Services website.[11] In addition, some categories of health information are particularly subject to state law. An example is information related to HIV status, which many states continue to treat as a separate category of information with specific rules for disclosure. These discrete laws arose because of concerns that disclosure of such information would lead to discrimination against the person so identified. While HIV status is PHI under HIPAA, the manner in which such information can be disclosed is usually governed by state laws that have more stringent privacy protections than HIPAA.

8 Per 45 CFR §46.102, research is defined as "a systematic investigation, including development, testing, and evaluation, designed to develop or contribute to generalizable knowledge." See https://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html#46.102
9 For a discussion of limited data sets, see http://www.hhs.gov/hipaa/for-professionals/faq/limited-data-set.
10 For more information about HIPAA and technology protections, see Patterson et al., 2017.
11 See https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html

2. 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 (34 CFR 99.3). FERPA also protects PII about the student that is different than the PHI covered by HIPAA. Four points about FERPA are worth noting, with much more detail provided in the reference section:

- Because researchers often had difficulty accessing records protected by FERPA, the U.S. Department of Education (DOE) promulgated a rule intended to expand access for research: DOE noted that the restrictive interpretation given FERPA was unwarranted "given Congress' intent in the American Recovery and Reinvestment Act to have states link data across sectors."[12]
- 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." 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 an excellent guide to this subject. The Privacy Technical Assistance Center (2017) has also released guidance specifically addressing concerns around IDS and student privacy.
- Finally, there may be confusion between which parts of a student record are covered by FERPA and which sections may be covered by HIPAA. The federal government has prepared guidance on this issue.[13]

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

Stringent federal regulations (referred to commonly as 42 CFR Part 2) protect the confidentiality of alcohol and substance abuse treatment records. While HIPAA protects PHI in the possession of covered entities, 42 CFR protects information regardless of who has possession, as long as the information was "received or acquired by a federally assisted alcohol or drug program." 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) (Kamoie and Borzi, 2001).
- Many state laws on substance abuse track (or in some cases may exceed) protections in 42 CFR. In thinking about an IDS, it will be important to look at state law as well as the federal regulations.

12 A discussion of the regulation with DOE commentary can be found here: http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
13 See https://www2.ed.gov/policy/gen/guid/fpco/doc/ferpa-hipaa-guidance.pdf

4. The Homeless Management Information System (HMIS)

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

Three points about HMIS are worth noting here.

- PPI can be disclosed externally or used internally by the homeless organization only if the use or disclosure is permitted by law and the use or disclosure 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.[14]
- As with other federal laws, HMIS data can be used in de-identified form (see Sokol and Gutierrez, 2005).

5. The Privacy Act

The Privacy Act (1974) has stringent confidentiality provisions but permits disclosure without the subject's consent for a "routine use," defined as "the use of such record for a purpose which is compatible with the purpose for which it was collected" (5 USC § 522a (a)(7)). This has been used to permit researcher access even to identifiable data. An example of how Medicare data, which is protected by the Privacy Act, can be accessed by researchers is in materials prepared by the Research Data Center.[15]

6. State Law

All states protect the confidentiality of certain types of information. Of particular relevance are state laws governing highly confidential information such as arrest records, mental health records, and other sensitive types of information. The confusion that sometimes arises is when there is a perceived or real conflict between federal and state law. In addressing this conflict, it is worth keeping certain principles in mind:

- Some federal laws, for example HIPAA, create a floor for protecting confidentiality, and states must meet the minimum requirements but are free to set more stringent requirements.
- Given the above, there are some substantive areas (mental health, HIV, criminal justice) where state laws must be consulted in determining applicable confidentiality rules (see Hodge et al., 2011).

7. Law Enforcement and Juvenile Justice Data

Both federal and state agencies maintain arrest records, and different agencies maintain court records such as case files and records of convictions. Access to such records can be difficult. In 2001, the U.S. Department of Justice Bureau of Justice Statistics prepared an overview on the topic, and while there has been no update to this point, it is a valuable resource to begin understanding the myriad laws on the topic (Bureau of Justice Statistics, 2001).

14 Guidelines and a model agreement can be found in Gellman, 2006.
15 Available at https://www.resdac.org/cms-data/request/cms-virtual-research-data-center

In addition, the Department of Justice in 2012 published a document titled *Survey of State Criminal History Information Systems, 2012,* which provides state-by-state descriptions of information captured by the various states on criminal justice records (Bureau of Justice Statistics, 2012).

Juvenile justice records are primarily governed by state law. For a period, the Department of Justice, through its Office of Justice Programs, published comprehensive reports on the privacy of juvenile justice records; however, the last report (which is still useful as a frame of reference) was in 1997 (Bureau of Justice Statistics, 1997). More recently, the Office of Justice Programs in 2006 published a report titled *Guidelines for Juvenile Information Sharing*, which is a good resource for those with interest in the topic at a more global level (Office of Juvenile Justice and Delinquency Prevention, 2006).

VII. Conclusions

Integrated data systems have shown tremendous promise in helping government and its partners maximize the value of existing administrative data to understand and address complex social problems. Lawmakers and citizens are beginning to demand that government make better use of their existing data to maximize the effectiveness of limited resources. Although some government lawyers perceive significant legal obstacles to robust data sharing, most of these barriers are both exaggerated and surmountable. Excellent examples around the country highlight how local, county, and state governments develop and operate IDS in accordance with all relevant state and local laws and in ways that protect the privacy and security of individually identifiable data.

Experience demonstrates the importance of approaching the development of an IDS, especially the creation of the legal agreements, in a collaborative and deliberate way. Lawyers should be involved in all stages of planning, from the first articulation of mission and goals, through a comprehensive assessment of the data to be included, and through the development of policies and procedures for governance and data security.

As the various agencies develop a shared understanding of the goals, structures, and processes for operating an IDS, the lawyers can document the most important components in the two primary legal agreements: the Memorandum of Understanding and the Data Use License. This report provides a rich library of model agreements, templates, and legal resources for lawyers to consult as they work with their colleagues across government to understand systematically the legal requirements and draft agreements that fulfill them.

References

Bureau of Justice Statistics. (1997). *Privacy and Juvenile Justice Records: A Mid-Decade Status Report.* U.S. Department of Justice, Office of Justice Programs. https://www.bjs.gov/content/pub/pdf/PJJR.PDF

Bureau of Justice Statistics. (2001). *Use and Management of Criminal Record History Information: A 2001 Update*. U.S. Department of Justice, Office of Justice Programs. https://www.bjs.gov/content/pub/pdf/umchri01.pdf

Bureau of Justice Statistics. (2012). *Survey of State Criminal History Information Systems, 2012.* U.S. Department of Justice, Office of Justice Programs. https://www.ncjrs.gov/pdffiles1/bjs/grants/244563.pdf

Cornman, Stephen Q. (2009). The unique method for obtaining data: Entering agreements to share administrative records. Federal Committee on Statistical Methodology. Washington, D.C.

Gellman, Bob. (2006). Disclosures for research under the HMIS privacy standard. Paper presented at the 2006 National HMIS Conference. https://www.hudexchange.info/resources/documents/ModelHMISResearchAgreement.pdf

Gibbs, Linda, Amy Hawn Nelson, Erin Dalton, Joel Cantor, Stephanie Shipp, and Della Jenkins. (2017). *IDS Governance: Setting Up For Ethical and Effective Use.* Actionable Intelligence for Social Policy, University of Pennsylvania.

Hodge, James G., Jr., Torrey Kaufman, and Craig Jaques. (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. https://c.ymcdn.com/sites/www.cste.org/resource/resmgr/PDFs/LegalIssuesTribalJuris.pdf

Kamoie, Brian, and Phyllis Borzi. (2001). A crosswalk between the final HIPAA privacy rule and existing federal substance abuse confidentiality requirements. *Behavioral Health Issue Brief Series.* Center for Health Services Research and Policy, The George Washington University School of Public Health and Health Services. publichealth.gwu.edu/departments/healthpolicy/CHPR/downloads/behavioral_health/bhib-18-19.pdf

Kitzmiller, Erika. (2013). *IDS Case Study: The Circle of Love: South Carolina's Integrated Data System.* Actionable Intelligence for Social Policy, University of Pennsylvania. http://www.aisp.upenn.edu/wp-content/uploads/2015/08/SouthCarolina_CaseStudy.pdf

Kitzmiller, Erika. (2014). *IDS Case Study: Allegheny County's Data Warehouse: Leveraging Data to Enhance Human Service Programs and Policies.* Actionable Intelligence for Social Policy, University of Pennsylvania. http://www.aisp.upenn.edu/wp-content/uploads/2015/08/AlleghenyCounty-_CaseStudy.pdf

Milner, Justin. (2016). Everything you need to know about the Commission on Evidence-based Policymaking." Urban Institute, Urban Wire. April 6. http://www.urban.org/urban-wire/everything-you-need-know-about-commission-evidence-based-policymaking

National Center for Education Statistics. (2010). *SLDS Technical Brief: Guidance for Statewide Longitudinal Data Systems (SLDS).* Institute of Education Sciences. https://nces.ed.gov/pubs2011/2011601.pdf

Office of Juvenile Justice and Delinquency Prevention. (2006). *Guidelines for Juvenile Information Sharing.* U.S. Department of Justice, Office of Justice Programs. https://www.ncjrs.gov/pdffiles1/ojjdp/215786.pdf

Patterson, David, Ken Steif, Niall Brennan, Andreas Haeberlen, Aaron Schroeder, and Adam Smith. (2017). *Towards State-of-the-Art IDS Technology and Data Security Solutions.* Actionable Intelligence for Social Policy, University of Pennsylvania.

References

Privacy Technical Assistance Center. (2017). *Integrated Data Systems and Student Privacy.* U.S. Department of Education. http://ptac.ed.gov/sites/default/files/IDS-Final.pdf

Shaw, Emily. (2015). Sharing sensitive data within government. Sunlight Foundation, February 11. https://sunlightfoundation.com/2015/02/11/sharing-sensitive-data-within-government/

Sokol, Brian, and Oscar Gutierrez. (2005). *Technical Guidelines for Unduplicating and De-Identifying HMIS Client Records.* U.S. Department of Housing and Urban Development, Office of Community Planning and Development. https://www.hudexchange.info/resource/1314/guidelines-unduplicating-and-deidentifying-hmis-client-records/

Wulczyn, Fred, Richard Clinch, Claudia Coulton, Sallie Keller, James Moore, Clara Muschkin, Andrew Nicklin, Whitney LeBoeuf, and Katie Barghaus. (2017). *Establishing a Standard Data Model for Large-scale IDS Use.* Actionable Intelligence for Social Policy, University of Pennsylvania.

It is common for an individual within an agency who is asked to contribute data to raise legal objections to the formation of the IDS or the sharing of particular data fields. Practice has shown the importance of careful review of these objections to address perceived legal barriers and create consensus around the legality of contributing data to an IDS. An MOU Inventory Checklist can enable the planning group or other stakeholders to analyze and resolve legal objections to the sharing of particular data up front.

Figure 1 summarizes the process from development of the MOU Inventory Checklist to integrating its elements into a Memorandum of Understanding/Data Use License.

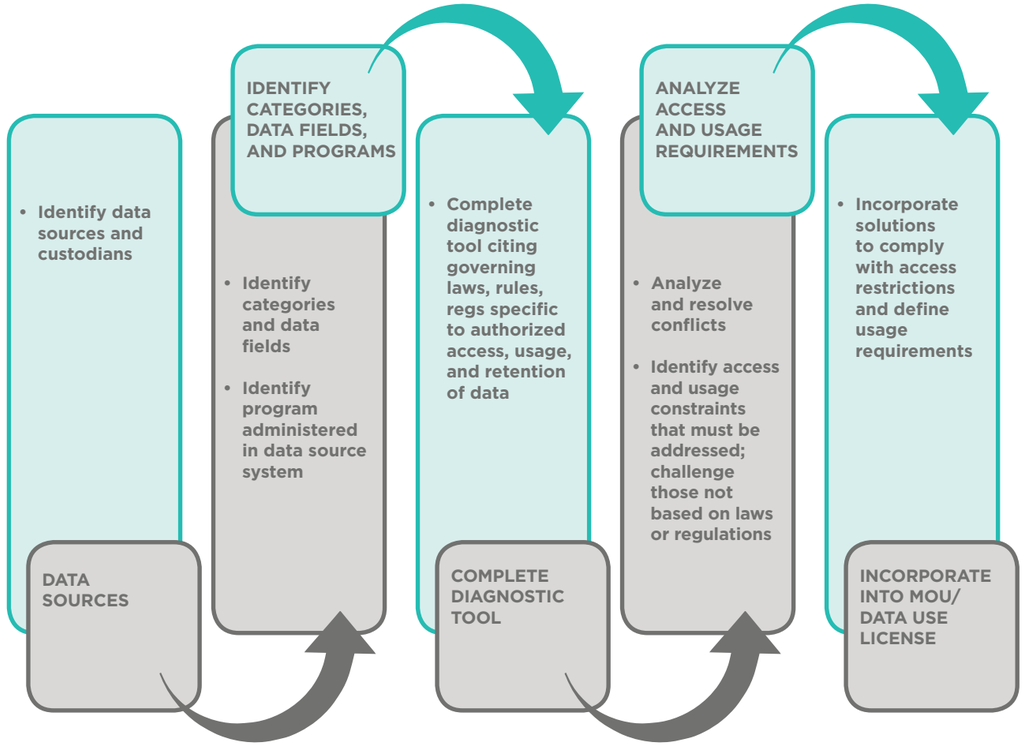

Figure 1: Development framework from creating MOU Inventory Checklist to drafting MOU/DUL.

The MOU Inventory Checklist provides a working framework for documenting and evaluating the governing laws, rules, regulations, and policies related to the data under consideration. Once completed, it can be helpful for creating a Memorandum of Understanding (MOU) or Data Use License. *Table* 2, the MOU Inventory Checklist, is a detailed and comprehensive document, which includes, but is not limited to, answering the following questions:

Table 2: MOU Inventory Checklist.

	Question	Additional Information
1	Agency	
2	Program	The name of the program with custody over the data
3	Data custodian	
4	Related program(s)	E.g., programs related to child care may be: Earned Income Tax Credit, Medicaid, etc.
5	Where are the data stored? (system name)	
6	Is this the original administrative data source? (e.g., for Social Security number (SSN)—the original source is either the Federal Social Security Administration or the local jurisdiction's data collection.)	Yes, No. If no, what is the original administrative data source and cite applicable laws governing allowable uses and data sharing.
7	Data provenance	What is the history/the origin of the data? Where did they originate? Have they been re-purposed since their origin? Are these the original raw data or have they been curated? If curated, by whom and how?
8	Identify if the data are licensed	Yes, No. If licensed, specify the terms of use.
9	Funding streams related to the administrative data	Federal, State, City, other, identify combination
10	What are the contents of the administrative data that are collected and maintained? Identify the units of analysis and associated data elements that are collected by the program. (See Wulczyn et al., 2017, Appendix C, Table 2: Data Elements by Domain and Source.)	Examples of unit of analysis: person, encounter with program, place, time. Examples of elements by units of analysis: Person (age, sex, race), encounter with program (diagnosis, procedure, assessment), place (address, location, type), time (entry and exit dates).
11	Specify time period of the data requested.	Identify specific months/years of data requested.
12	Frequency of data collection and frequency of update of administrative data file	Daily, Weekly, Monthly, Annual, etc.
13	Identify all legal, regulatory, and administrative policies governing the data; provide applicable citations.	Federal Law, Federal Reg, State Law, State Reg, City Law, City, Reg, Court Consent Decree/Order, etc.
14	Provide text of laws referenced above.	
15	Specify the scope of the legal, regulatory, and administrative policies applicable to the data and provide citations.	Identify applicability to data elements, for example: access, legal obligation to share, permitted uses, disclosure and re-disclosure, limitations and restrictions, exceptions, retention requirements, etc.
16	Specify specific categories of data to be shared and with whom (provide text and citation).	Yes, without client consent; Yes, with client consent; Yes, with qualifications (explain).
17	Identify any restrictions (legal, regulatory, administrative, other) regarding who can be an authorized user of the data.	Yes, No, With qualifications (explain).
18	Are their fields within the data file that can be shared while others cannot (i.e., security or confidentiality)?	Yes, No. If yes, list all fields and identify each with a yes, no. Provide citations.
19	Does the scope of the legal, regulatory, administrative policy, or other specifically address release of data with client consent?	Yes, No. If yes, provide cite and requirements.

	Question	Additional Information
20	If consent is specifically addressed in statute, regulation, administrative policy, or other, describe how it applies to the specific data (e.g., categories or type of data to which consent applies, time periods, expiration data, how data collected prior to consent authorization are addressed.)	
21	Does the scope of the legal, regulatory, administrative policy or other specifically address minors?	Yes, No. If yes, provide cite and requirements.
22	Does the scope of the legal, regulatory, administrative policy or other address individuals who are not competent to consent?	Yes, No. If yes, provide cite and requirements.
23	Does the agency have any existing memoranda of understanding (MOUs) with other agencies, contractors, or third parties related to data sharing?	Yes, No. If yes, provide list and attach copies.
24	Does the scope of the legal, regulatory, administrative policy, or other specifically address utilization of data for research and requisite protocols?	Yes, No. If yes, provide citations and specify requirements.

The following template can be used for drafting an MOU between the Lead IDS Agency and the Data Contributor(s). No single paragraph is required in all MOUs. The length, formality, and comprehensiveness of the document and language may vary depending on organizational legal culture. Even the name given to the agreement may vary depending on jurisdiction.

*Note that format/structure and some content are from Cornman (2009).

Example Text/Content of MOU Document	Comments*
1. Title Data Sharing MOU establishing the Tri-state Partnership Group	**Principles:** Provide a descriptive title that clarifies purpose of MOU and makes it easily distinguishable from other agreements between the parties.
2. Parties to the MOU Date Source Name: Lead IDS Agency Name: Primary Contact Person: Primary Contact Person: Title: Title: Address: Address: Telephone: Telephone: E-mail Address: E-Mail Address:	**Principles:** This section documents the legal names and contact information of the parties. **Practice Recommendations:** Changes to this information must be made via written notification and amendment. Since there may be multiple agreements between parties, contact information should be as specific as possible and identify principal contact persons at each entity.

(Continued on following 11 pages)

Example Text/Content of MOU Document	Comments*
3. Principles for MOU Basic Principles for this MOU: • Electronic storage of data and information is ubiquitous in today's society and continues to be created, stored, and shared at an expansive pace; • There is a presumption that as long as certain protective structures are in place, restrictions on sharing such data should only be observed when there is a clear legal bar to such sharing; • There is a strong consensus in favor of systematically integrating data and information systems in order to improve the process of policy making and implementation of programs for governmental/public purposes; • Such integrated data systems (IDS) are not only appropriate and legal, but can provide essential capabilities in furthering the core governmental functions of audit, evaluation, and research in public programs and policy; • The IDS supported by this MOU creates clear rules and processes that govern who, when, how and why individuals and entities can access data for public use, as well as ensure compliance with regulatory and oversight structures, and to address any confidentiality and privacy concerns; <Additional principles as desired for specific MOU relationship> With the intent to be legally bound hereby, the parties to this MOU set forth the following as terms and conditions of their understanding.	**Principles:** Should identify specific guiding principles of the interagency data agreement. **Practice Recommendations:** May wish to be more formal using "whereas" statements. May want to also note more generally that an MOU describes the relationships between, and responsibilities of, the parties who have agreed to share data.
4. Background, Purpose, and Scope <Name of Data Contributor> is responsible for providing and administering services for residents of _____. It is dedicated to meeting those needs and most particularly to the state's most vulnerable populations, through an extensive range of prevention, intervention, crisis management, and after care services provided through its program offices. Services include: _____. <Name of Data Contributor> believes that sharing certain data can be beneficial for served populations and improve state programs and services. The goal is to increase data use for policy, evaluation, and research to better serve the vulnerable populations of our state. <Additional Background and definition for scope of agreement as desired>	**Principles:** Provide context for the agreement. Identify specific purpose of the agreement, and define and limit the scope of specific data sharing relationship. **Practice Recommendations:** 1. Briefly describe relationship between the agencies and explain how work described in this agreement will benefit the relationship. Also include short history of the relationship. 2. May include information about the functions of the different parties involved. 3. May include whereas clause information/principles. 4. May want to include structure of IDS here (if not below). 5. May want the purpose and scope in separate section if desired.

Example Text/Content of MOU Document	Comments*
5. Glossary/Definitions of Terms	**Principles:** Define key terms in this agreement. **Practice Recommendations:** Include even standard terms if there is potential for misinterpretation.
6. Legal Authority <Name of Data Contributor> has legal authority to enter into this agreement and share data covered by this MOU with the <Lead IDS Agency>, including disclosure and re-disclosure, under sections _____ of the state of ____ statutes. . . . It is understood that shared data may be re-disclosed with other end users under the terms defined below.	**Principles:** Establish that parties have the legal authority to act, make decisions, enforce decisions, and/or enter into an agreement. Establish that under the terms of this MOU, administrative data will be shared by the parties pursuant to (insert statute). This MOU is intended to facilitate information sharing between the parties **Practice Recommendations:** Should speak to the specific authority that allows for the establishment of the IDS that includes language around 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. May also want to discuss Ownership issues here (if not below).
7. Data to Be Shared <Name of Data Contributor> will provide the following data to the <Lead IDS Agency>: a. Statewide Medicaid enrollment records for 2010-2016; b. Statewide Medicaid Service Claims records for 2010-2016; c. Statewide Medicaid MCO shadow claims 2010-2016; d. Statewide Medicaid Pharmacy claims for 2010-2016; e. Etc.	**Principles:** Describe in detail the data that will be shared by the Data Contributor. **Practice Recommendations:** May wish to just broadly describe the data to be shared and then refer to a separate document or appendix that specifies the databases, elements/items, and formats, as well as other parameters such as geographic boundaries and dates ranges.

Example Text/Content of MOU Document	Comments*
8. Ownership This MOU does not constitute a transfer of any title or interest in the Data, and <Name of Data Contributor> reserves all rights in the Data not expressly granted to <Lead IDS Agency> by this agreement. Any portion of the Data that is modified or merged into another form or merged with other Data shall continue to be subject to the provisions of this agreement. <Name of Data Contributor> makes no guarantee as to the accuracy or currency of the Confidential Information that will be provided as a result of this MOU. The person who will be the data custodian at <Lead IDS Agency>, and will be responsible for ensuring that the provisions of this agreement are carried out, is: Name Title Address Phone E-mail Address Alternate Contact: Name Title Address Phone E-mail Address	**Principles:** Should set forth the ownership rights and responsibilities for the data that are subject to the MOU. Should also specify the custodian of the shared data (including contact information). **Practice Recommendations:** Address: 1. Operational impact questions: a. Who is responsible for veracity? b. Who is responsible for security? c. Who is responsible for updates? d. If there is a HIPAA violation, who is responsible? 2. Structure of IDS may be important here. 3. May want to consider copyright laws, intellectual freedom, and recent SCOTUS rulings around this. Some MOUs contain disclaimer language such as: "Parties to this MOU 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." Or: "Only those representations or warranties made expressly in a data use agreement or in any binding agreements pertaining to the IDS, when, as, and if it is executed, and subject to such limitations and restrictions as may be specified in such agreement, will have any legal effect."

Example Text/Content of MOU Document	Comments*
9. IDS Structure The IDS structure maintained at the <Lead IDS Agency> follows a federated/non-federated model where data are . . .	**Principles:** Describe structure of IDS (if not laid out above). **Practice Recommendations:** Describes federated vs. non-federated models, as well as the governance structure. Use of graphics and schematics can help in the understanding of the structure. This section may also address data security and confidentiality/privacy—if not covered separately below.
10. Roles and Responsibilities In accordance with the provisions of this agreement: A. The <Name of Data Contributor> will be responsible for: a. Compiling the shared data and facilitating its transfer to <Lead IDS Agency> b. Providing ongoing assistance in the integration and analysis of data, as well as interpretation of findings/results c. Etc. B. The <Lead IDS Agency> will be responsible for: a. Securing and using the shared data; b. Informing <Name of Data Contributor> of disclosures, findings, and disposition of the Data; c. Etc.	**Principles:** Clearly describe and delineate the agreed upon roles and responsibilities each organization or agency will be providing to ensure project success. **Practice Recommendations:** The roles and responsibilities should align with project goals, objectives, and target outputs. May want to include specific reference to the databases that will be used and the authorized studies that will be undertaken e.g., refer to the record layout. Some agreements have the record layouts in the appendix. Reference to specific studies may be better included in the Data Use and Permissions section below.
11. Funding Information and Costs of Reimbursement This is a reciprocal data sharing agreement between <Name of Data Contributor> and <Name of Lead IDS Agency>, and both parties acknowledge the benefit of the availability of integrated data via the <Name of Lead IDS Agency> resource. As a result, neither party will charge the other party for the use of and access to data to be exchanged pursuant to this MOU, except as otherwise provided herein.	**Principles:** *Funding*: 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 that makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement. *Costs and reimbursement*: 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. **Practice Recommendations:** May include how downstream revenue is to be handled if there is re-use of data. May also include discussion of how IDS structure impacts funding and reimbursement. May also include differential pricing.

Example Text/Content of MOU Document	Comments*
12. Confidentiality and Privacy Parties understand that disclosure and re-disclosure of the Confidential Information is governed by both federal and state law. For example (and not by way of limitation), federal restrictions on this information are contained in 42 U.S.C. § 503, 26 U.S.C. § 3304, and subpart B of 20 C.F.R. Part 603, and the Family Educational Rights and Privacy Acts Statute ("FERPA") against unauthorized access or re-disclosure. State law restrictions are contained in _____. Pursuant to these requirements, the parties (and each person having access to the data), covenant as follows, and agree that upon their receipt of any Confidential Information, they are representing that they have complied with and/or have accomplished, and will continue to comply with and accomplish each of the following: 1. Confidential Information will be used only for the purposes authorized by law and only for the purposes specified in this MOU; 2. Access to Confidential Information will be provided only to authorized personnel who are required to perform activity required by this MOU and who need to access it for purposes listed in this MOU, who have executed a confidentiality certification. A signed copy of the Certification shall be provided by the individual who signs this MOU; 3. Parties will instruct all Authorized Personnel as to the confidential nature of all Confidential Information, the safeguards required to protect the information, the civil and any criminal sanctions for non-compliance pursuant to state laws. 4. Parties and Authorized Personnel will strictly adhere to the requirements of this MOU and its required procedures, and will report any breaches fully and promptly; 5. Parties will take precautions to ensure that only authorized personnel have access to the computer systems in which the Confidential Information is stored; 6. Parties will implement safeguards and precautions to ensure that only Authorized Personnel have access to the Confidential Information; 7. Parties will ensure that Confidential Information will be stored in a place physically secure from access by unauthorized persons; 8. Parties will ensure that Confidential Information in electronic format is stored and processed in such a way that unauthorized persons cannot retrieve the information by means of computer or otherwise gain access to it; 9. Parties shall immediately terminate an individual's authorized access upon changes in the individual's job duties that no longer require access, unauthorized access to, or use of Confidential Information by the individual, or termination of employment; and 10. Parties shall transmit the Confidential Information by a secure method and encrypt all personally identifiable information (PII) during receipt, transmission, storage, maintenance, and use.	**Principles:** Address how privacy will be ensured and how confidential information will be protected (if not addressed above in IDS description). **Practice Recommendations:** Confidentiality, privacy, and data security are all separate issues. *1. Confidentiality* refers to that which is done in confidence with the expectation of privacy *2. Privacy* means the right to restrict access to private information *3. Data security* is separate section Should identify the relevant statutes on confidentiality. Discuss issues of training, access, and storage and who is responsible for training, access, and storage. Discuss how to address state law and how to deal with pre-emption. May want to require compliance with any oversight boards (e.g., IRB) and stipulate that individuals who are approved to work on joint projects to be trained on safeguard to protect confidential information. Reference relevant statutes: e.g., HIPAA; FERPA; The Common Rule; Privacy Act of 1974; 42 CFR; HMIS; Children's Online Privacy Act; Child Abuse Prevention and Treatment Act.

Example Text/Content of MOU Document	Comments*
13. Data Security <Name of Lead IDS Agency> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Name of Lead IDS Agency> maintains and uses appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of the IDS and to prevent non-permitted use or disclosure of individually identifiable information. <Name of Lead IDS Agency> will ensure that any agent, including a subcontractor, to whom it provides individually identifiable information, received from, or created or received by <Name of Lead IDS Agency>, executes a written agreement obligating the agent or subcontractor to comply with all the terms of the Agreement.	**Principles:** Includes policies and procedures to protect the confidentiality and safety of data. **Practice Recommendations:** Discuss: 1. who is responsible for data security; 2. who is responsible for keeping data-use agreements; what records should be retained; back-up systems; the duration of time that records should be retained 3. 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; 4. how data security changes with industry standards (consider resources such as the SANS Institute [sans.org] and CERT at Carnegie Mellon University [cert.org]) 5. 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.

Example Text/Content of MOU Document	Comments*
14. Data Use, Permissions, and Retention A. Data will be transferred to/accessed by <Name of Lead IDS Agency> using the following secure procedures: . . . B. Permissions and consents to use the data will be provided by the <Name of Data Contributor> or obtained by <Name of Lead IDS Agency> to comply with any applicable state or federal laws and/or regulations prior to <Name of Data Contributor> furnishing individually identifiable information pertaining to an individual. C. <Name of Lead IDS Agency> shall use or disclose the shared data only for the purposes of: D. <Name of Lead IDS Agency> will not use or disclose individually identifiable information other than as permitted or required by this Agreement, or as required by state and federal law, or as otherwise authorized by data owners. E. <Name of Lead IDS Agency> agrees not to perform any of the following actions: a. Attempting to identify any individual whose health information is included in a de-identified Limited Data Set. b. Using or further disclosing any data for any purpose other than the purpose specified above or as otherwise permitted by law. c. Publishing or otherwise disclosing information that identifies the individuals whose health information is included in shared data. F. <Name of Lead IDS Agency> agrees not to use or permit others to use shared data that identify an entity or individual health care provider for any of the following purposes: a. To compete commercially against an entity. b. To determine the rights, benefits, or privileges of an entity or individual health care provider. c. To report, through any medium, information that identifies an entity or individual health care provider. G. <Name of Lead IDS Agency> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Name of Lead IDS Agency> will develop, implement, maintain, and/or use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of and to prevent non-permitted use or disclosure of individually identifiable information. These safeguards are required regardless of the mechanism used to transmit the information. <Name of Lead IDS Agency> will document and keep these safeguards current. H. Shared data will be retained by <Name of Lead IDS Agency> for the duration of this agreement and any renewals of this agreement. Back-up systems will be implemented according to industry standards to appropriately secure the back-up media/files. Upon termination of this agreement, shared data and back-up files will be permanently deleted (e.g., using overwrite protocols) within 90 days of the termination date. This requirement applies to all end users with whom data was shared by <Name of Lead IDS Agency>. <Name of Lead IDS Agency> is responsible for providing confirmation of such data destruction.	**Principles:** Define the scope and process of using data, as well as data transfer protocols. **Practice Recommendations:** Describe issues such as: 1. How the data will be securely transferred (or accessed if a federated structure). 2. 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? 3. Use of administrative data for other projects: specify the project and/or uses which the other agency can use administrative records. 4. Data available for researchers: 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. Describe any required statutory firewalls. 6. Data retention—including what records shall be retained for the project contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained.

Example Text/Content of MOU Document	Comments*
15. Notification of results, dissemination of results, and dissemination of end products. <Lead IDS Agency> will notify and provide draft copies of results and findings derived from analyses of contributed data produced by <Name of Lead IDS Agency>, its employees, subcontractors, agents, or end Data Licensees. Such results and end product must be provided to the <Name of Data Contributor> no less than 30 days prior to the dissemination of such results or products. Such notice should be provided to the following individuals at <Name of Data Contributor>: Name Title Address Phone E-mail Address Alternate Contact: Name Title Address Phone E-mail Address <Name of Data Contributor> will then have 30 days to offer relevant review for accuracy, appropriate citations, etc., and acknowledgment of the results or products. <Name of Lead IDS Agency> may presume acknowledgment if none is forthcoming within the 30-day review period.	**Principles:** Describe protocols for providing notice of dissemination of findings from data analyses. **Practice Recommendations:** 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 Lead IDS Agency process and use of the shared data, if desired.
16. Notification if signatories are deleted from or added to the agreement <Name of Lead IDS Agency> is responsible for notifying <Name of Data Contributor> and all signatories to this agreement of any additional signatories, deleted signatories, or other data contributors no more than 30 days after the final execution of relevant documents.	**Principles:** Define who is responsible for notifying the original signatories about additional/deleted signatories or data contributors.
17. Term of Agreement This MOU will be effective on the date that the last Party has executed it (the "Effective Date"), and shall terminate on the date that is five (5) years from the Effective Date, unless such term is extended by mutual agreement.	**Principles:** State specific start and end dates of MOU. **Practice Recommendations:** 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.

Example Text/Content of MOU Document	Comments*
18. Performance Standards and Review Procedures <Name of Lead IDS Agency> understands that <Name of Data Contributor> and other statutory authorities have the right to audit <Name of Lead IDS Agency>'s policies, procedures, and implementation of those policies and procedures for safeguarding the shared data and preserving the confidentiality of information. In addition, <Name of Data Contributor> shall be permitted to audit and monitor <Name of Lead IDS Agency>'s and its employees' access to and use of the Confidential Information on a periodic and "as needed" basis, including on-site inspections, to determine compliance with this MOU. <Name of Lead IDS Agency> agrees to cooperate fully with any auditing or on-site inspections. All reasonable costs of the auditing authority for such auditing and inspection shall be the sole expense of <Name of Data Contributor>. <Name of Lead IDS Agency> shall create and maintain a system sufficient to allow an audit of compliance with the requirements of this MOU.	**Principles:** If the agreement is extended for an indefinite period of time, it should contain a provision for review, at least every three years, to determine the continuing need and whether the agreement should be revised, renewed, or cancelled. **Practice Recommendations:** Should include provisions for audits: 1. Should specify who is responsible for audit 2. Should specify the components of the audit report (citing strengths, deficiencies, and any corrective actions that need to be taken)
19. Resolution of Conflicts In the event a party to the MOU believes that a provision of the MOU has been breached, or if there is a disagreement regarding implementation of the MOU or any of its provisions, the parties agree to attempt to resolve the conflict in the following manner:	**Principles:** Set forth the method for settling disputes. **Practice Recommendations:** 1. Describe process that will occur if a party to the agreement breaches the agreement 2. Issues/events that give rise to a breach of the agreement, at least in general detail.

Example Text/Content of MOU Document	Comments*
20. Unauthorized disclosure of information or other breach <Name of Lead IDS Agency> will report to <Name of Data Contributor>, in writing, any use and/or disclosure of individually identifiable information that is not permitted or required by this Agreement of which <Name of Lead IDS Agency> becomes aware. Such report shall be made as soon as reasonably possible but in no event more than ten (10) business days after discovery by <Name of Lead IDS Agency> of such unauthorized use or disclosure. This reporting obligation shall include breaches by <Name of Lead IDS Agency>, its employees, subcontractors, agents, or end Data Licensees. Each such report of a breach will: a. identify the nature of the non-permitted use or disclosure; b. identify the individually identifiable information used or disclosed; c. identify who made the non-permitted use or disclosure; d. identify who received the non-permitted use or disclosure; e. identify what corrective action <Name of Lead IDS Agency> took or will take to prevent further non-permitted uses or disclosures; f. identify what <Name of Lead IDS Agency> did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and g. provide such other information as <Name of Data Contributor>, or the data owners, may reasonably request. <Add indemnification and/or liquidated damages language>	**Principles:** Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data. **Practice Recommendations:** Describe: 1. the responsibilities for notification by points of contact of each party the MOUs. 2. any criminal/civil penalties that may apply for unauthorized disclosure of information. 3. indemnification language and limitations of liability. 4. 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.
21. Supersedes This MOU supersedes any previous understandings, representations, or agreements, whether written or oral, that may have been made or entered into by the parties relating to the subject matter hereof. OR This MOU does not supersede, replace, or render invalid any other agreement. The Participants mutually agree to promote and advance the purpose of this MOU to enhance information sharing, when necessary, beyond any existing understandings or agreements, including this one.	**Principles:** Establish relationship of this agreement with other understandings or agreements between the parties.
22. Severability Nothing in this MOU is intended to conflict with the current laws, regulations, or policies applicable to each Party. If a term of this MOU is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOU shall remain in full force and effect.	**Principles:** Establish severability of terms of the MOU.

Example Text/Content of MOU Document	Comments*
23. No Private Right of Action This agreement does not create any private cause of action for enforcement or damages.	**Principles:** Clarify that the MOU does not create a private right of action.
24. Modification/Amendment of the MOU Modifications or Amendments to this MOU must be in writing and formally agreed to/executed by all Parties. Concurrence provisions below apply. OR There shall be no modifications or amendments of this MOU, except in writing, executed with the same formalities as this instrument.	**Principles:** Set forth the process for amending the MOU. **Practice Recommendations:** Amendments should be with consent of all parties to the MOU and in writing.
25. Termination of the MOU. Either party may, with or without cause, terminate this MOU by giving a ninety (90) day written notice of its intent to do so. In the event changes in either state or federal law or regulations occur which render performance hereunder illegal, void, impracticable, or impossible, this MOU shall terminate immediately; however, obligations with respect to the treatment and security of Confidential Information and shall survive any termination of this MOU.	**Principles:** Set forth process for termination of the MOU. **Practice Recommendations:** Should contain a provision whereby each party may terminate the agreement within a specified time frame
26. Concurrence	**Principles:** In order to be a valid agreement, there must be concurrence by all parties to the agreement. **Practice Recommendations:** Identify the agency signatories. Agency signatories agree that they have the authority to sign for the agency or participating entity and denote their acceptance of the agreement terms by affixing their signature and the date.

* Note that format/structure and some content of comments is taken from "The Unique Method for Obtaining Data: Model Agreement to Share Administrative Records," published by the *Federal Committee on Statistical Methodology*, July 2009.

Example Text/Content of DUL Document	Comments*
1. Title Data Use License for the Smith Research Group	**Principles:** Provide a descriptive title that clarifies purpose of DUL and makes it easily distinguishable from other agreements between the parties.
2. Parties to the DUL Lead IDS Agency Name: Data Licensee Name: Primary Contact Person: Primary Contact Person: Title: Title: Address: Address: Telephone: Telephone: E-mail Address: E-Mail Address:	**Principles:** This section documents the legal names and contact information of the parties. **Practice Recommendations:** Changes to this information must be made via written notification and amendment. Note as there may be multiple agreements between parties, contact information should be as specific as possible and identify principle contact persons at each entity.

(Continued on following 11 pages)

Example Text/Content of DUL Document	Comments*
3. Principles for Data Use License (DUL) Basic Principles for this DUL: • Electronic storage of data and information is ubiquitous in today's society and continues to be created, stored, and shared at an expansive pace; • There is presumption that as long as certain protective structures are in place, restrictions on sharing such data should only be observed when there is a clear legal bar to such sharing; • There is a strong consensus in favor of systematically integrating data and information systems in order to improve the process of policy making and implementation of programs for governmental/public purposes; • Such integrated data systems (IDS) are not only appropriate and legal, but can provide essential capabilities in furthering the core governmental functions of audit, evaluation, and research in public programs and policy; • This Data Use License Agreement (DUL) is intended to allow limited use of specific IDS data and creates clear rules and processes that govern who, when, how, and why individuals and entities can access data for specified uses, as well as ensure compliance with regulatory and oversight structures, and to address any confidentiality and privacy concerns; <Additional principles as desired for specific DUL Relationship> With the intent to be legally bound hereby, the parties to this DUL set forth the following as terms and conditions of their understanding.	**Principles:** Should identify specific guiding principles of the interagency data use license. **Practice Recommendations:** May wish to be more formal using "WHEREAS" statements. May want to also note more generally that an DUL describes the relationships between, and responsibilities of, the parties who have agreed to share data.
4. Background, Purpose, and Scope <Name of Lead IDS Agency> has entered into MOUs with data owners, and compiled and linked several data systems into an organized IDS. It is dedicated to encouraging access and use of the IDS for policy, evaluation, research, and audit purposes while protecting the rights of individuals whose data is contained in the IDS under all applicable state and federal laws. <Name of Lead IDS Agency> accomplishes this by providing access to limited data sets and/or de-identified data to responsible and credible entities through execution of legally binding data use license agreements. <Data Licensee> conducts evaluations and research in the areas of _____ and desires to continue such work through accessing data contained in the <Name of Lead IDS Agency> IDS. The specific objectives and purpose of the proposed access and analyses are: _____. Anticipated analyses of the data and products will include _____. No additional analyses or products (other than those explicitly outlined above) will be pursued without explicit written permission of <Name of Lead IDS Agency>. <Additional Background and definition for scope of agreement as desired>	**Principles:** Provide context for the agreement. Identify specific purpose of the agreement, and define and limit the scope of specific data sharing relationship. **Practice Recommendations:** 1. Briefly describe relationship between the agencies and explains how work described in this agreement will benefit the relationship. Also include short history of the relationship. 2. May include information about the functions of the different parties involved. 3. May include whereas clause information/principles 4. May want to include structure of IDS and data to be accessed here (if not below) May want the Purpose and scope in separate section if desired.

Example Text/Content of DUL Document	Comments*
5. Glossary/Definitions of Terms Lead IDS Agency – Data License – Custodian – Etc.	**Principles:** Define key terms in this agreement. **Practice Recommendations:** Include even standard terms if there is potential for misinterpretation.
6. Legal Authority <Name of Lead IDS Agency> has legal authority to enter into this agreement and share data covered by this DUL with the <Data Licensee>, including disclosure and re-disclosure, under legally binding Memoranda of Understanding with Data Owners and under applicable sections of state and federal laws. . . . It is understood that shared or accessed data may not be re-disclosed by <Data Licensee> with other end users without explicit written permission of <Name of Lead IDS Agency>.	**Principles:** Establish that parties have the legal authority to act, make decisions, to enforce decisions, and/or enter into an agreement. Establish that under the terms of this DUL, administrative data will be shared by the parties pursuant to (insert statute) This DUL is intended to facilitate information sharing between the parties for the specific purposes outlined in the agreement only. **Practice Recommendations:** Should address 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. May also want to discuss ownership issues here (if not below).
7. Data to Be Shared <Name of Lead IDS Agency> will provide access to the following data to <Data Licensee>: a. Integrated school, Medicaid, and human services data for all children aged 6-12 in the _____ School District from 2010-2016. All data are to be indexed (linked by unique dummy identifiers) at the individual student/person level. b. Etc.	**Principles:** Describe in detail the data that will be shared by the Lead IDS Agency, including structure of files, calculated variables, etc. **Practice Recommendations:** May wish to just broadly describe the data to be shared and then refer to a separate document or appendix that specifies the databases, elements/items, and formats, as well as other parameters such as geographic boundaries and dates ranges. May wish to provide a formal data dictionary for data licensee so that data parameters are clear.

Example Text/Content of DUL Document	Comments*
8. Ownership This DUL does not constitute a transfer of any title or interest in the Data, and <Name of Lead IDS Agency> reserves all rights in the Data not expressly granted to <Data Licensee> by this agreement. Any portion of the Data that is modified or merged into another form or merged with other Data shall continue to be subject to the provisions of this agreement. <Name of Lead IDS Agency> makes no guarantee as to the accuracy or currency of the Confidential Information that will be provided as a result of this DUL. The person who will be the data custodian or control access to the data at <Data Licensee>, and will be responsible for ensuring the provisions of this agreement are carried out, is: Name Title Address Phone E-mail Address	**Principles:** Should set forth the ownership rights and responsibilities for the data that is subject to the DUL. 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.). **Practice Recommendations:** Address: 1. Operational impact questions: a. Who is responsible for veracity? b. Who is responsible for security? c. Who is responsible for updates? d. If there is a HIPAA violation, who is responsible? 2. Structure of IDS and data extract may be important here. 3. May want to consider copyright laws, intellectual freedom, and recent SCOTUS rulings around this. 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."

Example Text/Content of DUL Document	Comments*
9. Data Access Protocol Access to the requested data by <Data Licensee> will occur as follows: <Data Licensee> will contact _____ at <Lead IDS Agency> to review protocols for securely logging in and accessing the requested data sets. Data are not to leave the secure servers of the <Lead IDS Agency> and all analyses will occur on such servers. . . . OR <Lead IDS Agency> will coordinate the secure transfer of the requested data either through secure electronic protocols, or through exchange using appropriate physical media and following strong encryption procedures.	**Principles:** Describe the protocol for accessing and using the data extracts or data sets. **Practice Recommendations:** Describe process and security for direct access (VPN, remote login, etc.) or for data set transfer to Data Licensee. Use of graphics and schematics can help in the understanding of the protocols. This section may also address data security and confidentiality/privacy—if not covered separately below.
10. Roles and Responsibilities In accordance with the provisions of this agreement: A. The <Lead IDS Agency> will be responsible for: a. Compiling the shared data and facilitating access or transfer with <Data Licensee> b. Providing ongoing assistance in the use of the data and interpretation of findings/results c. Etc. B. The <Data Licensee> will be responsible for: a. Securing and using the shared data according to provisions of this agreement b. Informing <Lead IDS Agency> of findings, dissemination of results, and disposition of the Data c. Etc.	**Principles:** Clearly describe and delineate the agreed upon roles and responsibilities each organization or agency will be providing to ensure project success. **Practice Recommendations:** The roles and responsibilities should align with project goals, objectives, and target outputs. May want to include specific reference to the databases that will be used and the authorized studies that will be undertaken e.g., refer to the record layout. Some agreements have the record layouts in the appendix. Reference to specific studies may be better included in the Data Use and Permissions section below.

Example Text/Content of DUL Document	Comments*
11. Funding Information and Costs of Reimbursement This is a reciprocal data sharing agreement between <Lead IDS Agency> and <Data Licensee> and both parties acknowledge the benefit of the availability of integrated data via the <Lead IDS Agency> resource. As a result, neither party will charge the other party for the use of and access to data to be exchanged pursuant to this DUL, except as otherwise provided herein. OR <Data Licensee> agrees to compensate <Lead IDS Agency> for the costs of compiling and providing access to the shared data. <Lead IDS Agency> will clarify such costs in a separate letter of engagement. OR <Data Licensee> agrees to compensate <Lead IDS Agency> for the costs of compiling and providing access to the shared data. <Lead IDS Agency> will charge $80 per hour for analyst time and $5/GB per month for space on the <Lead IDS Agency> secure server. . . .	**Principles:** *Funding*: 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 that makes it clear that the agreement is not an instrument that obligates funds of any party to the agreement. *Costs and reimbursement*: If the agreement result in the exchange of money between parties, state the estimated cost or costs not to exceed, terms of payments, and dispute resolution conditions. **Practice Recommendations:** May include differential pricing.

Example Text/Content of DUL Document	Comments*
12. Confidentiality and Privacy Parties understand that disclosure and re-disclosure of the Confidential Information is governed by both federal and state law. For example (and not by way of limitation), federal restrictions on this information are contained in 42 U.S.C. § 503, 26 U.S.C. § 3304, and subpart B of 20 C.F.R. Part 603, and the Family Educational Rights and Privacy Acts Statute ("FERPA") against unauthorized access or re-disclosure. State law restrictions are contained in _____. Pursuant to these requirements, the parties (and each person having access to the data), covenant as follows, and agree that upon their receipt of any Confidential Information, they are representing that they have complied with and/or have accomplished, and will continue to comply with and accomplish, each of the following: 1. Confidential Information will be used only for the purposes authorized by law and only for the purposes specified in this DUL; 2. Access to Confidential Information will be provided only to authorized personnel who are required to perform activity required by this DUL and who need to access it for purposes listed in this DUL, who have executed a confidentiality certification. A signed copy of the Certification shall be provided by the individuals who sign this DUL; 3. Parties will instruct all Authorized Personnel as to the confidential nature of all Confidential Information, the safeguards required to protect the information, the civil and any criminal sanctions for non-compliance pursuant to state laws. 4. Parties and Authorized Personnel will strictly adhere to the requirements of this DUL and its required procedures, and will report any breaches fully and promptly; 5. Parties will take precautions to ensure that only authorized personnel have access to the computer systems in which the Confidential Information is stored; 6. Parties will implement safeguards and precautions to ensure that only Authorized Personnel have access to the Confidential Information; 7. Parties will ensure that Confidential Information will be stored in a place physically secure from access by unauthorized persons; 8. Parties will ensure that Confidential Information in electronic format is stored and processed in such a way that unauthorized persons cannot retrieve the information by means of computer or otherwise gain access to it; 9. Parties shall immediately terminate an individual's authorized access upon changes in the individual's job duties that no longer require access, unauthorized access to, or use of Confidential Information by the individual, or termination of employment; and 10. Parties shall transmit the Confidential Information by a secure method and encrypt all personally identifiable information (PII) during receipt, transmission, storage, maintenance, and use.	**Principles:** Address how privacy will be ensured and how confidential information will be protected (if not addressed above in data description). **Practice Recommendations:** Confidentiality, privacy, and data security are all separate issues. *1. Confidentiality* refers to that which is done in confidence with the expectation of privacy *2. Privacy* means the right to restrict access to private information *3. Data security* is separate section Should identify the relevant statutes on confidentiality. Discuss issues of training, access, and storage and who is responsible for training, access, and storage. Discuss how to address state law and how to deal with pre-emption. May want to require compliance with any oversight boards (e.g., IRB) and stipulate that individuals who are approved to work on joint projects to be trained on safeguard to protect confidential information. Reference relevant statutes: e.g., HIPAA; FERPA; The Common Rule Privacy Act of 1974; 42 CFR; HMIS Children's Online Privacy Act; Child Abuse Prevention and Treatment Act

Example Text/Content of DUL Document	Comments*
13. Data Security <Data Licensee> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Data Licensee> will maintain and use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of the IDS and to prevent non-permitted use or disclosure of individually identifiable information. <Lead IDS Agency> will ensure that any agent, including a subcontractor, to whom it provides individually identifiable information, received from, or created or received by <Lead IDS Agency>, executes a written agreement obligating the agent or subcontractor to comply with all the terms of the Agreement.	**Principles:** Includes policies and procedures to protect the confidentiality and safety of data. **Practice Recommendations:** Discuss: 1. who is responsible for data security; 2. who is responsible for keeping data-use agreements; what records should be retained; back-up systems; the duration of time that records should be retained; 3. 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; 4. how data security changes with industry standards (consider resources such as the SANS Institute [sans.org] and CERT at Carnegie Mellon University [cert.org]); 5. 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.

Example Text/Content of DUL Document	Comments*
14. Data Use, Permissions, and Retention A. Data will be transferred to/accessed by <Data Licensee> using the following secure protocols outlined in Section 9 above. B. If applicable, permissions and consents to use the data will be provided by the <Lead IDS Agency> to comply with any applicable state or federal laws and/or regulations. C. <Data Licensee> will not disclose or re-disclose any shared or accessed data with any other entities or persons without explicit written permission of <Lead IDS Agency>. D. <Data Licensee> will not use or disclose individually identifiable information other than as permitted or required by this Agreement, or as required by state and federal law, or as otherwise authorized by data owners. E. <Data Licensee> agrees <u>not</u> to perform any of the following actions: a. Attempting to identify any individual whose health information is included in a de-identified Limited Data Set. b. Using or further disclosing any data for any purpose other than the purpose specified above or as otherwise permitted by law. c. Publishing or otherwise disclosing information that identifies the individuals whose health information is included in shared data. F. <Data Licensee> agrees not to use or permit others to use shared data that identify an entity or individual health care provider for any of the following purposes: a. To compete commercially against an entity. b. To determine the rights, benefits, or privileges of an entity or individual health care provider. c. To report, through any medium, information that identifies an entity or individual health care provider. G. <Data Licensee> will use appropriate safeguards to prevent use or disclosure of the individually identifiable information other than as provided for by this Agreement. <Data Licensee> will develop, implement, maintain, and/or use appropriate administrative, technical, and physical safeguards to preserve the integrity and confidentiality of and to prevent non-permitted use or disclosure of individually identifiable information (see section 13 above). These safeguards are required regardless of the mechanism used to transmit the information. <Data Licensee> will document and keep these safeguards current. H. Shared data will be retained by <Data Licensee> for the duration of this agreement and any renewals of this agreement. Back-up systems will be implemented according to industry standards to appropriately secure the back-up media/files. Upon termination of this agreement, shared data and back-up files will be permanently deleted (e.g., using overwrite protocols) within 80 days of the termination date. <Data Licensee> is responsible for providing confirmation of such data destruction.	**Principles:** Define the scope and process of using data, as well as data transfer protocols. **Practice Recommendations:** Describe issues such as: 1. How the data will be securely transferred or accessed. 2. 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? 3. Use of administrative data for other projects: specify the project and/or uses for which the other agency can use the administrative records described by the DUL. 4. Data available for researchers: 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. Describe any required statutory firewalls. 6. Data retention—including what records shall be retained for the project contemplated by the agreement and for a back-up system. Specify the duration of time that records should be retained.

Example Text/Content of DUL Document	Comments*
15. Notification of results, dissemination of results, and dissemination of end products <Data Licensee> will notify and provide draft copies of results and findings derived from analyses of contributed data produced by <Data Licensee>, its employees, subcontractors, or other Authorized Personnel. Such results and end products must be provided to the <Lead IDS Agency> no less than 45 days prior to the dissemination of such results or products. Such notice should be provided to the following individuals at <Lead IDS Agency>: Name Title Address Phone E-mail Address Alternate Contact: Name Title Address Phone E-mail Address <Lead IDS Agency> and original data owners will then have 45 days to offer relevant review for accuracy, appropriate citations, etc., and acknowledgment of the results or products. <Data Licensee> may presume acknowledgment if none is forthcoming within the 45-day review period.	**Principles:** Describe protocols for providing notice of dissemination of findings from data analyses. **Practice Recommendations:** 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.
16. Term of Agreement This DUL will be effective on the date that the last Party has executed it (the "Effective Date"), and shall terminate on the date that is _____ years from the Effective Date, unless such term is extended by mutual agreement. This term of agreement is subject to the termination provisions in section 24 below.	**Principles:** State specific start and end dates of DUL. **Practice Recommendations:** 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.

Example Text/Content of DUL Document	Comments*
17. Performance Standards and Review Procedures <Data Licensee> understands that <Lead IDS Agency> and other statutory authorities have the right to audit <Data Licensee>'s policies, procedures, and implementation of those policies and procedures for safeguarding the shared data and preserving the confidentiality of information. In addition, <Lead IDS Agency> shall be permitted to audit and monitor <Data Licensee>'s and its employees' access to and use of the Confidential Information on a periodic and "as needed" basis, including on-site inspections, to determine compliance with this DUL. <Data Licensee> agrees to cooperate fully with any auditing or on-site inspections. All reasonable costs of the auditing authority for such auditing and inspection shall be the sole expense of <Lead IDS Agency>. <Data Licensee> shall create and maintain a system sufficient to allow an audit of compliance with the requirements of this DUL.	**Principles:** If the agreement is extended for an indefinite period of time, it should contain a provision for review at least every three years to determine the continuing need and whether the agreement should be revised, renewed, or cancelled. **Practice Recommendations:** Should include provisions for audits: 1. Should specify who is responsible for audit 2. Should specify the components of the audit report (citing strengths, deficiencies, and any corrective actions that need to be taken).
18. Resolution of Conflicts In the event a party to the DUL believes that a provision of the DUL has been breached, or if there is a disagreement regarding implementation of the DUL or any of its provisions, the parties agree to attempt to resolve the conflict in the following manner:	**Principles:** Set forth the method for settling disputes short of termination of agreement. **Practice Recommendations:** Steps may include: 1. Notice of dispute and good faith attempt to resolve through negotiation 2. Mediation 3. Arbitration

Example Text/Content of DUL Document	Comments*
19. Unauthorized disclosure of information or other breach <Data Licensee> will report to <Lead IDS Agency>, in writing, any use and/or disclosure of individually identifiable information that is not permitted or required by this Agreement of which <Data Licensee> becomes aware. Such report shall be made as soon as reasonably possible but in no event more than ten (10) business days after discovery by <Data Licensee> of such unauthorized use or disclosure. This reporting obligation shall include breaches by <Data Licensee>, its employees, subcontractors, agents, or Data Licensees. Each such report of a breach will: a. identify the nature of the non-permitted use or disclosure; b. identify the individually identifiable information used or disclosed; c. identify who made the non-permitted use or disclosure; d. identify who received the non-permitted use or disclosure; e. identify what corrective action <Data Licensee> took or will take to prevent further non-permitted uses or disclosures; f. identify what <Data Licensee> did or will do to mitigate any deleterious effect of the non-permitted use or disclosure; and g. provide such other information as <Lead IDS Agency>, or the data owners, may reasonably request. <Add indemnification and/or liquidated damages language>	**Principles:** Specify the remedies and damages in the event of a breach of contract by any party to the agreement or unauthorized disclosure of data. **Practice Recommendations:** Describe: 1. the responsibilities for notification by points of contact of each party to the DUL. 2. any criminal/civil penalties that may apply for unauthorized disclosure of information. 3. indemnification language and limitations of liability. 4. 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.
20. Supersedes This DUL supersedes any previous understandings, representations or agreements, whether written or oral, that may have been made or entered into by the parties relating to the subject matter hereof. OR This DUL does not supersede, replace or render invalid any other agreement. . . . The Participants mutually agree to promote and advance the purpose of this DUL to enhance information sharing, when necessary, beyond any existing understandings or agreements, including this one.	**Principles:** Establish relationship of this agreement with other understandings or agreements between the parties.
21. Severability Nothing in this DUL is intended to conflict with the current laws, regulations, or policies applicable to each Party. If a term of this DUL is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this DUL shall remain in full force and effect.	**Principles:** Establish severability of terms of the DUL.

Example Text/Content of DUL Document	Comments*
22. No Private Right of Action This agreement does not create any private cause of action for enforcement or damages.	**Principles:** Clarify that the DUL does not create a private right of action.
23. Modification/Amendment of the DUL Modifications or Amendments to this DUL must be in writing and formally agreed to/executed by all Parties. Concurrence provisions below apply. OR There shall be no modifications or amendments of this DUL, except in writing, executed with the same formalities as this instrument.	**Principles:** Set forth the process for amending the DUL. **Practice Recommendations:** Amendments should be with consent of all parties to the DUL and in writing.
24. Termination of the DUL Either party may, with or without cause, terminate this DUL by giving an eighty (80) day written notice of its intent to do so. In the event changes in either state or federal law or regulations occur which render performance hereunder illegal, void, impracticable, or impossible, this DUL shall terminate immediately; However, obligations with respect to the treatment and security of Confidential Information and shall survive any termination of this DUL.	**Principles:** Set forth process for termination of the DUL. **Practice Recommendations:** Should contain a provision whereby each party may terminate the agreement with a specified time frame. Note: The MOU template between original data owners and Lead IDS Agency have a 90-day termination notice requirement; thus if original data owners provide such termination notice, the Lead IDS Agency should promptly (within 10 days) give all Data Licensees using the data their 80-day notice of termination.
25. Concurrence	**Principles:** In order to be a valid agreement, there must be concurrence by all parties to the agreement. **Practice Recommendations:** Identify the agency signatories. Agency signatories agree that they have the authority to sign for the agency or participating entity and denote their acceptance of the agreement terms by affixing their signature and the date.

HIPAA Resources

- HIPAA (Protected Health Information) HHS guidance to covered entities: https://www.resdac.org/cms-data/request/cms-virtual-research-data-center
- HHS/Department of Education guidance to relationship between FERPA and HIPAA: http://www.cumc.columbia.edu/hipaa/docs/ferpa-hippa-guidance.pdf
- National Institutes of Health discussion of clinical research and Privacy Rule: http://privacyruleandresearch.nih.gov/pr_02.asp
- Office for Civil Rights discussion of HIPAA and research: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/research.html
- HHS discussion of de-identification of health information: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/
- Centers for Medicare and Medicaid Services data use agreement: https://www.cms.gov/cmsforms/downloads/cms-r-0235.pdf
- North Carolina Department of Health and Human Services data use agreement for a limited data set: https://www2.ncdhhs.gov/info/olm/manuals/dhs/pol-80/man/DHHS_Data_Use_Agreement_Template.pdf
- University of Buffalo's explanation for why business associate agreements are not required for researchers: http://www.hpitp.buffalo.edu/hipaa/Research/DataExtraction.htm

HHS discussion of business associates, noting that researchers are not required to enter business associate agreements for the purpose of accessing protected health information for research: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=es

FERPA Resources

- U.S. Department of Education guidance on FERPA and resources: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- HHS/Department of Education guidance to relationship between FERPA and HIPAA: http://www.cumc.columbia.edu/hipaa/docs/ferpa-hippa-guidance.pdf
- U.S. Department of Education guidance on protection of human subjects: http://www2.ed.gov/about/offices/list/ocfo/humansub.html
- U.S. Department of Education sample agreement between educational institution and authorized representative: http://www2.ed.gov/about/offices/list/ovae/pi/cte/uiferpa.html
- Amended FERPA regulation permitting data sharing agreements with entities not under "direct control" of the educational institution: http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- National Center for Educational Statistics guide to privacy and confidentiality of educational records: http://nces.ed.gov/pubs2011/2011601.pdf
- Privacy Technical Assistance Center guidance on IDS and student privacy: http://ptac.ed.gov/sites/default/files/IDS-Final.pdf

42 CFR Part 2 (based on version prior to January 13, 2017)

- Discussion of the relationship between the HIPAA Privacy Rule and 42 CFR: http://publichealth.gwu.edu/departments/healthpolicy/CHPR/downloads/behavioral_health/bhib-18-19.pdf
- FAQs on the regulation maintained by the U.S. Substance Abuse and Mental Health Services Administration: http://www.samhsa.gov/about-us/who-we-are/laws/confidentiality-regulations-faqs
- National Center for State Courts: Future Trends in State Courts: 42 CFR Part 2: http://www.ncsc.org/sitecore/content/microsites/futuretrends2012/home/PrivacyandTechnology/~/media/Microsites/Files/Future%20Trends%202012/PDFs/SubstanceAbuse_Kunkel.ashx

HMIS (Homeless Management Information System)

- Overview of the HMIS prepared by the U.S. Department of Housing and Urban Development: https://www.hudexchange.info/programs/hmis/
- Overview of data elements that must be collected by HMIS programs: https://www.hudexchange.info/resource/3826/hmis-data-standards-manual/
- Discussion with example of HMIS research agreements: https://www.hudexchange.info/resources/documents/ModelHMISResearchAgreement.pdf
- Discussion of de-identified protected personal information (PPI) in the HMIS system: https://www.hudexchange.info/resource/1314/guidelines-unduplicating-and-deidentifying-hmis-client-records/

Privacy Act of 1974

- U.S. Department of Education requirements for Privacy Act matching agreements: http://www2.ed.gov/policy/gen/leg/foia/acsom6105.pdf

Law enforcement data and criminal justice settings

- Analysis of use of arrest and related records prepared by the U.S. Department of Justice Bureau of Justice Statistics: https://www.bjs.gov/content/pub/pdf/umchri01.pdf
- State laws on juvenile interagency information sharing: https://www.ncjrs.gov/pdffiles1/ojjdp/215786.pdf
- Guide to Michigan law and court rules on accessing court records and filings: http://courts.mi.gov/administration/admin/op/pages/records-management.aspx
- An overview of information sharing in court-related projects: https://www.bja.gov/publications/csg_cjmh_info_sharing.pdf

Enforcement of Privacy and Confidentiality Laws

- The HHS Office of Civil Rights is primarily responsible for enforcing HIPAA. It maintains a website on its enforcement activities here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
- The U.S. Department of Education's Family Compliance Office has primary responsibility for enforcing FERPA violations. Its website is here: https://www2.ed.gov/policy/gen/guid/fpco/index.html?exp=0

Appendix E: Sample MOU, South Carolina

See https://www.aisp.upenn.edu/wp-content/uploads/2017/02/AppE-SC_State_Agency_MOU-non-HIPAA_072014.pdf

Appendix F: Sample MOU, Allegheny County Department of Human Services (DHS)

See https://www.aisp.upenn.edu/wp-content/uploads/2017/02/AppF_Sample_MOU_ALL_DHS.pdf

Appendix G: Sample MOU, Virginia

See https://www.aisp.upenn.edu/wp-content/uploads/2017/02/AppG_Virginia-eHHR-Enhanced-MOU-2015-draft-v4b.pdf

Appendix H: Memo to Providers on Data Sharing Rules (Allegheny County, PA)

See https://www.aisp.upenn.edu/wp-content/uploads/2017/02/ProviderLetterFinalVersion.pdf

Appendix I: Sample DUL, Centers for Medicare and Medicaid Studies

See https://www.aisp.upenn.edu/wp-content/uploads/2017/02/DUA-CMS-model.pdf

Actionable Intelligence for Social Policy
University of Pennsylvania
3701 Locust Walk, Philadelphia, PA 19104
215.573.5827 | www.aisp.upenn.edu