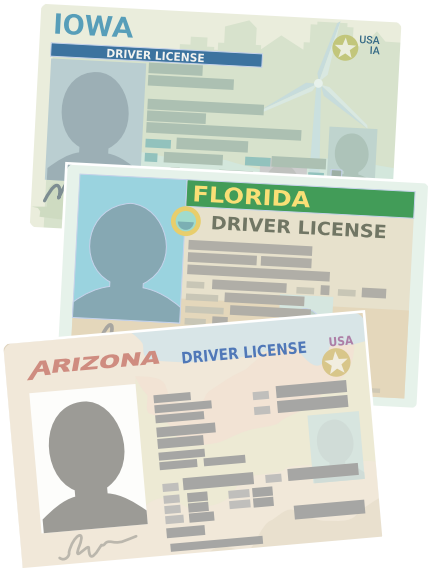
Data Integration Support Center
WestEd

2026
June

Structuring Legal Agreements for Driver's License Data Integration

Overview

This supplement expands on "Driver's License Data Can Help States Better Understand Education and Workforce Pathways" by the Data Integration Support Center (DISC) and the Data Quality Campaign (DQC). That brief aims to help state leaders understand the utility and risk of including driver's license data in their statewide longitudinal data system (SLDS) matching process. This supplement looks at different models for structuring legal agreements when accessing driver's license data.



Why This Matters

Driver's license data held by state motor vehicle agencies (MVAs) can substantially improve the accuracy and completeness of SLDS matching across education and workforce records. However, accessing those data requires a formal legal agreement—and the design of that agreement has direct consequences for privacy protection, operational sustainability, and legal compliance.

This brief helps SLDS directors and their legal and policy staff understand the primary structural models states have used to access driver's license data. It also outlines the components of a sound data-sharing agreement under each model.

Three Structural Models

States have pursued three primary approaches to structuring access to driver's license data for SLDS purposes. Each model has distinct legal, operational, and privacy implications. Choosing a model early will shape nearly every decision that follows—which parties are involved, which data elements are transferred, and what security obligations the receiving party assumes.

Model 1: Direct Agreement—SLDS and MVA

In this model, the SLDS enters into a data-sharing agreement with the MVA and receives driver's license data directly. The SLDS uses the data internally for matching and record enhancement.

Advantages:

- Gives the SLDS direct control over the matching process and timeline.
- Avoids dependence on another agency.
- May simplify governance if the SLDS already has infrastructure for handling personally identifiable information (PII).

Considerations:

- The SLDS becomes a direct custodian of highly restricted personal information, significantly increasing security obligations and breach liability.
- This model requires robust technical infrastructure, PII-trained staff, and strong data governance.
- The SLDS may be required to demonstrate its security posture to the MVA before the agreement is executed.
- States in which the SLDS has statutory authority for the data transfer and an established trust relationship with the MVA are best positioned for this model.

EXAMPLE

MARYLAND

The Maryland Longitudinal Data System (MLDS) Center holds a direct agreement with the Maryland MVA. The MLDS receives specific data elements quarterly, matches the data against its education and workforce records internally, and destroys unmatched records within 60 days. The agreement is grounded in Maryland's MLDS-enabling statute and requires the Center to adhere to its governing board-approved Data Security and Safeguarding Plan.

Model 2: Trusted Third-Party Intermediary

In this model, a trusted third-party agency—typically a state workforce or labor agency—holds its own agreement with the MVA; uses driver's license data to match and enrich its records, such as unemployment insurance (UI) wage data; and shares only the enhanced output with the SLDS under a separate memorandum of understanding (MOU). The third party is the sole recipient of confidential driver's license data; the SLDS never directly receives or handles them.

Advantages:

- Allows the SLDS to avoid direct custodianship of highly restricted personal information, substantially reducing legal exposure and security obligations.
- Leverages an existing MVA relationship rather than requires the SLDS to build one.
- Still benefits the SLDS through improved match rates and enhanced data.

Considerations:

- This model requires two separate legal agreements: one between the third party and the MVA and one between the third party and the SLDS.
- The SLDS cedes some control over the matching process and depends on the third party's capacity and timeline.
- Coordination across three agencies adds governance complexity and requires ongoing relationship management.

EXAMPLE

CONNECTICUT

In Connecticut's arrangement, the state Department of Labor (DOL) serves as the intermediary. The DOL holds the agreement with the MVA, uses the data for UI enforcement and labor market statistics, and provides enhanced data to the SLDS. This model reflects a broader approach: Any trusted state agency with an established MVA relationship and appropriate security infrastructure can serve this function, not only workforce agencies.

EXAMPLE

MINNESOTA

Minnesota's Department of Employment and Economic Development (DEED) submits Social Security numbers (SSNs) from its wage records to the Department of Public Safety (DPS), which matches them to driver's license records internally. DPS returns gender, date of birth, zip code, and a unique random identifier—never the raw SSN. DEED relinks the results to its wage data and is authorized to share the enhanced output downstream to the Minnesota Statewide Longitudinal Education Data System.

Model 3: MVA as Matching Agent

In this model, the SLDS or a partner agency provides a set of identifiers to the MVA, which matches them against its own records internally and returns only the matched and enriched output. Raw driver's license data never leaves the MVA's custody.

Advantages:

- Provides maximum privacy protection: No driver's license PII is transferred to any external entity.
- Reduces the legal and security burden on both the SLDS and any intermediary agency.
- May be the most acceptable model for MVAs that are reluctant to transfer highly restricted personal information at all.

Considerations:

- This model requires the MVA to have the internal capacity and willingness to perform matching as a service function.
- The SLDS has limited visibility into and control over the matching methodology.
- Contractual terms must still be established to govern the inputs the SLDS provides, the outputs the MVA returns, and the permissible uses of both.
- This model works best if the MVA has existing data services infrastructure and if concerns about external data transfer make direct transfer impractical.

EXAMPLE

NEW JERSEY

New Jersey's MVA entered into an agreement with the John J. Heldrich Center for Workforce Development at Rutgers University to support the New Jersey Statewide Longitudinal Education Data System.

EXAMPLE

RHODE ISLAND

Similarly, Rhode Island's MVA entered into an agreement with the University of Rhode Island DataSpark, which operated the Rhode Island DataHUB. In both cases, the MVA performed matching in house and returned only matched output, keeping the most sensitive data within the MVA.

Core Components of a Legal Agreement

Regardless of which structural model a state pursues, any agreement will need to address the same six components. The specific content of each component will vary depending on the model—most significantly, which parties are involved, which data elements are transferred, and what security obligations the receiving party assumes—but the framework applies across all three approaches. This section explains key recommendations for each component and suggests implementation approaches.

1. How does the use of the data align with the SLDS's function?

The agreement should open with a clear statement of *why* the SLDS needs driver's license data and *how* that use connects to the system's statutory purpose. This statement is the legal foundation for the entire agreement. It must satisfy the permissible use requirements of the Driver's Privacy Protection Act (DPPA) and give both parties a clear, unambiguous account of why the data are being shared and what they will be used for.

KEY RECOMMENDATION: Ground the purpose statement in the SLDS's enabling statute, enumerate the specific activities the data will support, and describe only uses authorized under the agreement—not potential future uses.

IMPLEMENTATION: Purpose statements typically identify the SLDS's statutory mandate, name the specific matching or analytical functions the driver's license data will enable, and cite the DPPA permissible use provision that authorizes the transfer. Maryland's agreement illustrates this component well: It grounds the data transfer directly in the MLDS's enabling statute and enumerates four authorized uses—identity matching per documented protocol, demographic enrichment of student records, census tract assignment, and workforce training outcome analysis using commercial driver's license and endorsement data.

2. Which laws govern the agreement, and how does the agreement ensure compliance?

The agreement must explicitly identify the federal and state legal authorities that permit the data transfer and establish how the SLDS's use of the data complies with each. At the federal level, the primary governing statute is the DPPA, which restricts what MVA data can be disclosed and to whom.

KEY RECOMMENDATION: Engage legal counsel to assist in identifying federal and state statutes that apply to the specific data elements being shared and the uses being proposed. Enumerate those authorities explicitly in the agreement.

IMPLEMENTATION: Agreements typically cite the DPPA and identify which permissible use provision applies; then they enumerate applicable state statutes governing MVA data disclosure, state privacy law, and data security standards. Maryland's agreement cites eight separate federal laws and five categories of state statutes, requires the MLDS Center to warrant that all authorized staff are familiar with both, and requires the Center to adhere to subsequent changes in law throughout the agreement's duration. Kentucky's agreement similarly enumerates applicable laws, references the Family Educational Rights and Privacy Act alongside the DPPA, and requires encrypted file transfers as a baseline security measure. Most agreements also specify the governing law and venue for any legal disputes.

3. Who will have access to the data?

Access must be defined narrowly and specifically. An agreement that simply names an agency as the recipient without specifying who within that agency can access the data—and under what conditions—leaves the MVA with little assurance that sensitive information will be handled appropriately.

KEY RECOMMENDATION: Define authorized users by category or job title rather than by name, establish a process for designating and revoking access, require signed acknowledgments from all individuals with access, and address contractors and subcontractors explicitly. The MVA will want assurance that the SLDS cannot pass data to third parties without written agreement and accountability.

IMPLEMENTATION: Agreements commonly define authorized users by job title or role, require annual updates to the authorized personnel list, and require prompt notification to the MVA when individuals are no longer authorized. Maryland's agreement defines "authorized staff" to include state employees, information technology contractors, and researchers authorized by the executive director under state regulation. It also requires the MLDS Center to assume full responsibility for contractor and subcontractor compliance. Idaho's agreement is even more specific: Only the research supervisor and research analyst principal may access identified driver's license data. In addition, a written list of authorized individuals must be provided to the Transportation Department within two weeks of execution and updated annually. Nebraska requires a signed confidentiality acknowledgment—cosigned by the employee's supervisor—on file for everyone with access.

4. Which data elements will be shared?

The data elements transferred under the agreement should be no broader than those necessary for the stated purpose. This data minimization requirement is part of both the DPPA and general privacy law principles, and it provides practical protection against scope creep over time.

KEY RECOMMENDATION: Build the data element list from the purpose statement, not the other way around. For each element, ask: What specific matching or analytical activity requires this element? If the answer is not clear, the element should not be in the agreement. Revisit the element list as part of each agreement renewal.

IMPLEMENTATION: Agreements typically enumerate data elements in a table or an attachment, categorized by type. Some agreements attach a separate data specification document to make future updates easier without requiring a full amendment. Across states with existing agreements, practice varies considerably, reflecting differences in statutory authority, SLDS architecture, and the specific matching and enrichment purposes being served. Table 1 on the following page illustrates the range.

TABLE 1: DATA ELEMENTS COMPARISON

	Data Element	CT	ID	KY	MD	MN	NE	SD	WY
IDENTIFYING INFORMATION	First Name	✓	✓	✓	✓	✓	✓		✓
	Middle Name/Initial		✓	✓	✓	✓	✓		✓
	Last Name	✓	✓	✓	✓	✓	✓		✓
	Generational Code/Suffix				✓				✓
	Also Known As (AKA)		✓						
	Social Security Number	✓	✓	✓	✓	✓	✓	✓	✓
DEMOGRAPHICS	Date of Birth	✓	✓	✓	✓	✓	✓	✓	✓
	Age							✓	
	Gender/Sex	✓	✓	✓	✓	✓	✓	✓	✓
	Race				✓		✓		
ADDRESS (Mailing or Residence)	Street Address	✓	✓	✓			✓	✓	✓
	City	✓	✓	✓			✓	✓	✓
	State	✓	✓	✓			✓	✓	✓
	Zip Code	✓	✓	✓		✓	✓	✓	✓
LICENSE INFORMATION	License Number/State Identification	✓		✓					✓
	License Status	✓		✓					✓
	License Issue Date				✓				✓
	License Renewal Date	✓			✓				✓
	Vehicle Information								
METADATA	Last Record Update Date		✓				✓		✓

5. How will the data be stored and used?

Storage and use provisions establish the activities both parties must do to store, use, secure, and protect the data. The MVA gains confidence that its data will be handled appropriately; the SLDS gains a clear operational framework that reduces compliance risk.

KEY RECOMMENDATION: Reference the SLDS's existing Data Security and Safeguarding Plan or equivalent governance document in the agreement rather than attempt to replicate technical requirements in legal language. Ensure that breach notification timelines in the agreement are consistent with any state breach notification statutes that may set independent requirements.

IMPLEMENTATION: Security provisions typically require encrypted storage and transmission. They also require alignment with a recognized industry standard (NIST 800 series) or a state framework. Permissible use provisions prohibit use beyond the enumerated purposes and restrict or prohibit redisclosure. Breach notification clauses define what constitutes a breach, establish notification timelines, and assign responsibility for corrective action. Maryland's agreement references its Data Security and Safeguarding Plan, allowing technical requirements to be updated without a formal amendment. Washington state's agreement template goes further in technical specificity, requiring quarterly vulnerability assessments, annual penetration testing, and cyber liability insurance scaled to the number of records held.

6. What records will be kept and for how long?

Retention requirements operate at two levels: retention of the driver's license data and retention of administrative records about how those data were used. Getting both sets of requirements right is essential—retaining data longer than necessary creates risk, while inadequate administrative recordkeeping undermines accountability.

KEY RECOMMENDATION: Treat data retention and administrative recordkeeping as separate obligations in the agreement. Ensure that data protection provisions remain enforceable after the agreement ends.

IMPLEMENTATION: Data retention provisions specify how long driver's license data may be retained and require secure destruction at end of retention, with written confirmation to the MVA. Maryland requires destruction of unmatched records within 60 days and written notification upon completion; Rhode Island requires a signed Certificate of Destruction from a designated custodian and specifies the destruction standard (NIST SP 800-88), with destruction obligations surviving termination of the agreement.

Administrative recordkeeping provisions require logs of who accessed the data and for what purpose, typically available for MVA inspection for five to six years. Annual compliance attestations are common and provide a low-burden accountability mechanism. Washington state extends the recordkeeping period to six years beyond agreement termination and covers breach response, subrecipient communications, and audit documentation.

Recommendations

1. **Assess technical readiness and governance before choosing a model.** The direct agreement model requires significant investment in security infrastructure, access controls, and PII-trained staff. If the SLDS does not currently have sufficient resources to support the in-house matching, consider another model to reduce both risk and the time needed to establish an agreement.
2. **Engage with the MVA early and at the right level.** MVAs vary considerably in their experience with data-sharing agreements and their comfort with different partner types. Executive-level support—from a governor's office or cabinet official—is often a prerequisite for any agreement, regardless of model.
3. **Update data governance structures concurrently.** Incorporating driver's license data changes the SLDS's risk profile. Data governance policies, privacy notices, staff training, and security assessments should be updated to reflect the new data type and its sensitivity.
4. **Plan for sustainability.** MOUs can lapse, and agency priorities shift. Consider whether having statutory authorization for the data-sharing relationship—rather than relying solely on administrative agreements—would provide greater durability over time.

Additional Resources

- "Access and Use of Drivers' License Files by State Labor Market Information Offices; Advancing the Cause," including Connecticut, Idaho, Minnesota, Nebraska, South Dakota, Virginia, and Wyoming
- "Driver's License Data Can Help States Better Understand Education and Workforce Pathways," a March 2025 brief by DQC and DISC
- "Texas Motor Vehicle Records Data Contract Data Use Agreement"
- Privacy Protection Policy between the MLDS Center and the Maryland MVA

HOW DISC CAN HELP

DISC can facilitate productive conversations and assist your agency's legal counsel as they navigate the complex requirements for data sharing and integration. DISC offers technical assistance to public agencies free of cost. For more information on DISC's external legal support services, visit https://disc.wested.org/focus-areas/external-legal-supports/.

A project of WestEd
WestEd.org

Suggested citation: WestEd. (2026, June). *Structuring legal agreements for driver's license data integration.*