

LAW ENFORCEMENT mDL TOOLKIT
DOC-07

Legal & Privacy Considerations

State Acceptance Law, Data Minimization, CJIS Compliance, and Fourth Amendment Guidance

Audience	Legal Counsel, Command Staff, Policy Officers
Purpose	Addresses the legal and privacy landscape governing law enforcement use of mDL technology, including state acceptance law variability, data minimization requirements, CJIS Security Policy obligations, data retention policy guidance, and Fourth Amendment considerations. This document should be reviewed with agency legal counsel before deployment.
Published	April 2026 American Association of Motor Vehicle Administrators (AAMVA)

Legal Counsel Review Required

This document provides general guidance, not legal advice. Agency legal counsel must review all aspects of mDL deployment — including policy development, data retention schedules, procurement contracts, and officer training content — before deployment. State law varies significantly, and the legal landscape is evolving.

State Acceptance Law

Law enforcement authority to accept mDLs as valid credentials is not uniform across states, and the legal landscape is changing rapidly. Agencies must understand their jurisdiction's current legal posture before deploying mDL reader technology.

Legal Posture	Description & Agency Action Required
Mandatory Acceptance Law	Some states (e.g., Georgia via HB 296, 2025) have enacted laws requiring officers to accept mDLs when equipped with a reader, and mandating agency-wide reader deployment by a specified date. Agencies in these states have a statutory obligation to deploy. Confirm effective date and equipment requirements.
Permissive / Authorizing Law	Some states have enacted laws authorizing — but not requiring — officers to accept mDLs. Officers may, but are not required to, accept an mDL as valid identification. Agency policy should clarify officer obligations when a driver presents an mDL.
No Specific Legislation	Many states have no specific mDL legislation. In these jurisdictions, officers may still encounter mDLs issued from other jurisdictions. Because the mDL is an extension of the physical, legitimately-issued driver license or ID card, agencies with mDL verification capabilities are likely permitted to accept the mDL. Engage agency legal counsel and the state DMV for a formal determination.
Adverse or Restrictive Legislation	A small number of jurisdictions may have passed laws restricting relying parties from requiring digital identity presentation. While this should not hinder acceptance of mDL, legal counsel must review before any mDL deployment.

AAMVA's mDL Model Legislation provides a template for jurisdictions seeking to enact clear mDL acceptance law. Agencies in states without clear acceptance authority should engage their legislative affairs contacts and DMV to advocate for legislative clarity.

Physical Credential Requirement Remains

Regardless of state mDL acceptance law, most states currently require drivers to carry their physical credential when operating a motor vehicle. Though mDLs present the same data — from the same data source — as physical driver licenses and ID cards, most relying parties do not yet have the capability of reading and authenticating mDLs. Officers should continue to request physical credentials when an mDL cannot be verified or when the encounter

requires physical credential examination.

Data Minimization and Selective Disclosure

ISO/IEC 18013-5 is built on the principle that relying parties (including law enforcement) should request only the data elements necessary for the specific transaction. AAMVA's Model Legislation codifies this principle, providing that relying parties shall only request data elements necessary to complete the transaction for which the data is being requested.

In the case of law enforcement encounters, it is generally understood Law Enforcement mDL readers will request all available mDL data.

Data Retention Policy

Generally, mDL data should be handled in the manner and retained for the same periods as is data obtained from physical drivers. However, because the proliferation of digital identity credentials has introduced new questions and concerns regarding data privacy, agencies may wish to consider developing and adopting a formal data retention policy governing mDL transaction data before deploying reader technology. Policy considerations should address:

- **Retention Period:** How long is mDL transaction data retained in the CAD/RMS? Is it tied to the incident record, or maintained separately?
- **Non-Incident Retention:** Is mDL data that does not result in a citation, report, or arrest retained at all? If so, under what legal authority, and for how long?
- **Local Device Retention:** Does the reader application retain transaction data locally on the officer's device? If so, confirm the retention period and purge mechanism with the vendor.
- **Compliance with State Records Law:** Retention schedules must comply with applicable state public records retention law. Confirm that mDL transaction data is classified under the appropriate records retention schedule.
- **CJIS Compliance:** Any mDL transaction data commingled with Criminal Justice Information is subject to FBI CJIS Security Policy retention and destruction requirements.

CJIS Security Policy

The FBI Criminal Justice Information Services (CJIS) Security Policy applies to any system that stores, transmits, or interfaces with Criminal Justice Information (CJI). Because mDL data will routinely be used to initiate NCIC/CIC queries — and the results of those queries are CJI — the mDL reader and its integration software may be subject to CJIS requirements.

Key CJIS requirements for mDL deployments:

- **Encryption:** All CJI in transit must be encrypted using FIPS 140-2 compliant algorithms. Verify with all vendors.

- **Multi-Factor Authentication:** Advanced authentication is required for access to systems containing CJI.
- **Audit Logging:** All access to CJI must be logged. Reader software integrated with CJI systems must maintain compliant audit logs.
- **Vendor ISA:** All vendors with access to CJI data must execute a CJIS Information Security Agreement (ISA). This is a mandatory contract requirement.
- **Personnel Security:** Vendor employees with unescorted access to CJI systems must have completed required background checks.

Fourth Amendment Considerations

Agency legal counsel should review the intersection of mDL technology with Fourth Amendment jurisprudence. The following areas warrant specific attention:

Data Minimization and Scope of Request

Requesting mDL data elements beyond what is legally required for a given encounter may raise Fourth Amendment questions. Officers and agencies should establish clear policy on what data elements may be requested for each encounter type and ensure reader applications are configured accordingly.

Plain View During mDL Engagement

During NFC or QR engagement, the officer's proximity to the holder's device may raise questions about whether the contents of the phone visible during the engagement are subject to plain view doctrine. Officers should not examine phone contents beyond what is necessary to initiate the mDL session. Under no circumstances should an officer touch or otherwise handle a subject's mDL device (i.e. mobile phone) solely for the purpose of reading or authenticating an mDL.

Long-Term Surveillance Risk

The ISO/IEC 18013-5 standard's non-tracking design — where no central server logs the transaction — is a significant privacy protection. Agencies should avoid implementing supplemental logging systems that recreate the surveillance risk the standard was designed to prevent, as such systems could be challenged as warrantless tracking.

Policy Development Checklist

Before deploying mDL reader technology, agencies should consider developing policies addressing the following:

- ☐ Officer authority to accept mDLs — defined by reference to applicable state law
- ☐ Data elements authorized for request in each encounter type
- ☐ mDL transaction data retention schedule — compliant with state records law and CJIS Security Policy

- [] Procedures when mDL cannot be verified — fallback to physical credential
- [] Prohibition on accessing phone contents beyond mDL session initiation
- [] Vendor CJIS ISA requirement — standard contract provision
- [] Officer training requirement on legal and privacy obligations

Related Toolkit Documents

- **DOC-01:** Standards Overview — privacy protections built into ISO/IEC 18013-5
- **DOC-05:** Procurement Considerations — CJIS ISA and data ownership contract requirements
- **DOC-08:** Training Plan Framework — officer training on legal and privacy obligations