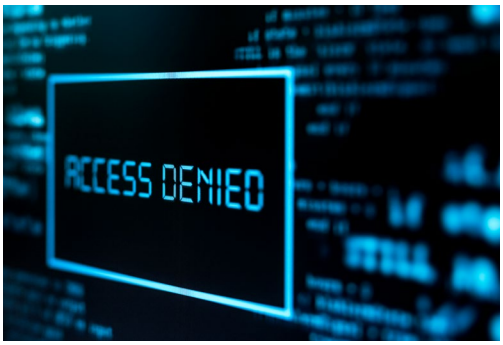
AAMVA

American Association of Motor Vehicle Administrators

SECURITY
Safety Privacy
Data Access
Protection
SHARING PII

Managing Data Privacy and External Access
Best Practice



February 2021

MANAGING DATA PRIVACY AND
EXTERNAL ACCESS WORKING GROUP

Cover photo credits: © iStockphoto.com

Contents

Introduction

This document is a best practice guide for motor vehicle agencies (MVAs) to protect driver and vehicle records, provide access and authorize usage consistent with law, and apply effective and efficient approaches to internal and external audit practices. Specifically, the focus of this document is the protection and management of MVA data that is personally identifiable information (PII), confidential, sensitive, or otherwise restricted.

The demand for privacy protection and data management is an ever-expanding challenge for MVA leaders. The importance of this issue is illustrated by high-profile breaches of government and corporate databases and made more complex by myriad laws governing PII. However, the need to secure this information must be balanced against the interests of the proliferation of entities seeking to obtain driver and vehicle record data under public access laws.

MVAs are custodians of vast amounts of data, much of it specific to individuals. In the wrong hands, this data can be used to cause harm to these individuals and, ultimately, harm to MVAs. The use of MVA data to stalk, harass, and intimidate individuals was the impetus for the passage of the Driver Privacy Protection Act (DPPA) in the United States. Given the volume of data being maintained, MVAs risk breaches of multiple identifying records, events that have befallen other public and private sector entities. In 2015, for example, the U.S. Office of Personnel Management discovered the theft of approximately 20 million records containing PII.* The risk to MVAs, given the nature and amount of data they hold, requires the adoption of safeguards and a comprehensive approach to privacy protection.

Guiding Principles

Data privacy is driven by core principles derived primarily from Fair Information Practices Principles (FIPP).† The FIPPs, established in the 1970s by a U.S. Department of Health, Education & Welfare (HEW) advisory committee study, serve as the basis for a number of information privacy laws, such as the U.S. Privacy Act of 1974. FIPPs established concepts of data privacy that are used today. Principles include disclosing systems of records that use an individual's data, notifying individuals regarding what information about them is kept by an organization, requiring consent before information given for one purpose is used for another purpose, providing the ability for an individual to correct erroneous data, and creating steps to secure data and prevent unauthorized use. These principles include:

- Collection limitation – Collect only data that are necessary to fulfill the mission of the MVA.
- Accountability – MVAs should have knowledge of all access to driver and vehicle data and should be held accountable for complying with laws and procedures for protecting data, providing training about safeguarding data, and auditing the use of data.
- Openness or transparency – Provide notice of practices and policies related to the collection, use, and dissemination of PII.
- Data quality – Data should be accurate, complete, and up to date.

* United States Office of Personnel Management. Cybersecurity Resource Center, available from https://www.opm.gov/cybersecurity/cybersecurity-incidents/

† For background on FIPPS, see United States Department of Justice, Office of Privacy and Civil Liberties, Overview of the Privacy Act of 1974, available from https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction

- Purpose specification – Specify the purpose for which data are collected at the time of collection (establishing justification for collection).
- Security and safeguards – Safeguards and mechanisms to protect data should be in place.
- Use limitation and permissible use – MVA data may only be released on an authorized basis pursuant to applicable law. This principle also includes consent of the individual when applicable.
- Individual participation – This allows individuals to understand or request information on what PII an MVA has about them, the ability to request amendment if such PII is inaccurate or out of date, and the ability to challenge any denial of a request to amend data.

Not a part of FIPPs but important to protection of MVA data is the principle of ownership. MVAs should retain governance authority and ownership of their data within the statutory and regulatory restrictions of their jurisdiction. Data leaving the confines of an MVA are still considered to be owned by the MVA until it is destroyed, subject to any ownership provisions in a data-sharing agreement.

Challenges

Key challenges facing MVAs include balancing disclosure of MVA data, public transparency, and data privacy. Private companies, government, and individuals rely on MVA data to conduct business. MVA data provide a foundation for statistical reporting on public safety and consumer affairs issues, such as crash reporting, law enforcement requests, vehicle recalls, and credit score determinations. PII and data used beyond their permissible purpose creates risk for both MVAs and the individual. Specific challenges faced by MVAs include:

- Data ownership – Comingling of MVA data by data recipients challenges ownership boundaries, because each layer of comingling has the potential to further dilute the source of the data.
- Data governance – Establishing a comprehensive framework for managing data across internal boundaries, rather than in silos, can seem daunting. MVAs can achieve this goal beginning with small steps to improve data governance and data management plans.
- Data residency – The increasingly borderless nature of the world creates opportunities for sharing data but also creates control and data distribution risks.
- Data retention – Advances in technology will compel MVAs to continuously evaluate their means for storing and retrieving data.
- Open records laws – As governmental entities, MVAs are expected to balance protection of data with the public's right to know.

Benefits of MVA Data and PII Sharing

There are several beneficial and permissible reasons why MVAs disclose data. MVA data play an integral role in public safety, traffic safety, federal grant distribution, and consumer protection. The valid uses of MVA data include but are not limited to:

- Vehicle recalls: MVAs provide vehicle owner and registrant data to support vehicle safety recall and owner notifications regarding class action lawsuits.
- Public safety: Law enforcement accesses MVA data to verify driver identification, enforce vehicle and traffic safety laws, and confirm vehicle ownership.
- Individual identification: PII allows MVAs to reduce the chance of false identification. For example, social security numbers (SSNs) provided to MVAs are checked against Social Security Administration (SSA) data to validate that the data provided is correct and that driver's license credentials are not improperly or

fraudulently issued. Validation of data enhances the quality and validity, or integrity, of data.

- Asset identification: Data from MVA records are used in identifying citizens or residents who owe taxes and are subject to vehicle liens.
- Insurance purposes: MVA records identify driver and vehicle data, location of vehicle, and other demographic data that help write insurance policies and prevent fraud.
- Employment verification: MVA records provide verification of employment eligibility, such as obtaining and maintaining employment with a commercial driver's license.
- Federal grant distribution: U.S. law and federal agency regulations factor aggregated MVA data on vehicle or driver counts to calculate distribution of federal infrastructure and highway safety grants to states and local jurisdictions.

Glossary of Terms and Acronyms

AA	Advanced Authentication. CJIS Security Policy language that means the same as multifactor authentication. Needed whenever CJI is being accessed from a non-secure location.
Access control	To ensure that access to assets is authorized and restricted based on business and security requirements
Agent	A third-party entity performing title and registration or driver's license and identification card transaction services on behalf of, or directly to, the MVA
American Association of Motor Vehicle Administrators (AAMVA)	Tax-exempt, nonprofit organization that develops model programs in motor vehicle administration, law enforcement, and highway safety. Founded in 1933, AAMVA represents the motor vehicle officials in the United States and Canada who administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the MVAs.
Attack	To attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset
ATPA	Administering Third-Party Agents Working Group, a working group commissioned by AAMVA to develop a best practice related to management and administration of agents
Audit (noun)	Checking processes against standards for compliance is defined as verification activity, such as an inspection or examination, of a process or quality system to ensure compliance with a set of defined requirements. Two types of audit classifications exist: ■ Internal – Audit conducted by agency to ensure processes and personnel are meeting standards ■ External – Audit conducted by agency or outside entity to ensure processes and personnel are meeting standards for use of agency's data
Audit (verb)	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. Also, a review and inspection conducted by authorized MVA employees or official designees of an agent's operations, place of business, and processed motor vehicle titling or registration or driver's license transactions

Audit scope	Extent and boundaries of an audit
Audit trail	An unmodifiable record of all activity related to any data
Authentication	Provision of assurance that a claimed characteristic of an entity is correct
CCPA	California Consumer Privacy Act
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
Cloud computing	A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information
Cloud subscriber	A person or organization that is a customer of a cloud
Consumer grade	Any device, system, or software meant for home, not enterprise or corporate, use
Corrective action	Action to eliminate the cause of a nonconformance, to prevent recurrence, and/or to mitigate or remediate a data loss after the fact
CSA	CJIS Systems Agency
CSP	Criminal Justice Information Services Security Policy
CTA	Control Terminal Agency
DAMA	DAMA International, a not-for-profit, vendor-independent, global association of technical and business professionals dedicated to advancing the concepts and practices of information and data management. DAMA International published the DMBOK®, or Data Management Book of Knowledge.
Data leakage	Any unauthorized access, use, or disclosure of PII or sensitive data
Data recipient	Entity receiving data, especially PII, from an MVA

Data-sharing agreement	A written agreement that recognizes and governs the rights and duties of the parties to the agreement between an MVA and a data recipient
Dealer(ship)	A person or entity engaged in the business of buying, selling, or exchanging vehicles
Department of Motor Vehicles	See Motor Vehicle Agency (MVA)
DPPA	Driver's Privacy Protection Act, a federal (U.S.) law limiting the disclosure of personal information on a motor vehicle record
EU	European Union
Executive management	Person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization
FBI	Federal Bureau of Investigation
Federal Information Processing Standard (FIPS)	Standards developed by the U.S. federal government for use in computer systems by nonmilitary government agencies and government contractors
FIPPs	Fair Information Practice Principle
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation, law enacted in the European Union relating to the protection and movement of personal data
Governing body	Person or group of people who are accountable for the performance and conformance of the organization
HIPAA	Health Information Portability and Protection Act
ID	Identifier
Incident management plan	Instructions for responding to unauthorized use of MVA data. An incident management plan covers staffing, decision making, interactions with stakeholders, immediate steps for securing data, and response options for notifying the extent of unauthorized use and plans for rectifying the incident while planning for future events and how to limit the likelihood of future events.

Information security	Preservation of confidentiality, integrity, and availability of information
Information security event	Identified occurrence of a system, service, or network state indicating a possible unauthorized access of information security policy or failure of controls or a previously unknown situation that might be security relevant
Information security incident	A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information system	Applications, services, information technology assets, or other information-handling components
Integrity	Property of accuracy and completeness
Interested party	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Internal users	Agency employee who has been granted access to data
ISCM	Information Security Continuous Monitoring
ISO	International Organization for Standardization
IT	Information technology
Law enforcement agency (LEA)	Agency providing criminal justice services
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
Local office	Nongovernmental agency providing MVA services
Minimization	Collecting and sharing only what is needed or allowed
Monitoring	Determining the status of a system, process, or activity

Motor vehicle agency (MVA)	In the United States, an MVA is a state- or territory-level government agency that administers vehicle and driver's license laws, regulations, and policies. Similar departments exist in Canada. The acronym "MVA" is not used in every state, province, or territory, nor are the traditional MVA functions handled by a single agency in every jurisdiction, but the generic term is universally understood, particularly in the context of driver's license issuance and renewal. Driver licensing and vehicle registration in the United States are handled by the state or territorial government in all states but Hawaii, where local governments perform MVA functions. In Canada, driver licensing and vehicle registration are handled at the provincial or territorial government level. The Uniform Vehicle Code prefers the name "Department of Motor Vehicles," but it is synonymous with MVA.
MVA data	Any data processed by an MVA in the course of business. MVA data may contain information about individuals or organizations that, if disclosed publicly, would cause harm to the individual, the organization, or the MVA.
Multifactor authentication (MFA)	Using two or three authenticators to allow access to data. The three authenticators are "something you know" (password, PIN), "something you have" (proximity reader card, RSA key fob), and "something you are" (fingerprint, retina, facial)
NIST	National Institute of Standards and Technology
Nlets	International Justice and Public Safety Network. The proper name "Nlets" is derived from the previous acronym Nlets (National Law Enforcement Telecommunications System).
OTP	One-time password
PCI	Payment Card Industry
PIA	Privacy Impact Assessment
PII	Personally identifiable information
Policy	Intentions and direction of an organization as formally expressed by its top management
RAP Back	Record of Arrest and Prosecution Background, an FBI service allowing for the continuous monitoring of arrest records of employees who hold positions of trust (e.g., schoolteachers, daycare workers) or who are under criminal justice related supervision or investigation
Redisclosure	The action of an external user providing MVA data to a subrecipient

Risk	Effect of uncertainty on objectives
Risk acceptance	Informed decision to take a particular risk
Risk assessment	Overall process of risk identification, risk analysis, and risk evaluation
Risk management	Coordinated activities to direct and control an organization regarding risk
Risk management process	Systematic application of management policies, procedures, and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring, and reviewing risk
RBA	Risk-Based Authentication
RMF	Risk management framework
SOC	Service Organization Control, "Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service"*
SSA	Social Security Administration
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Subrecipient	Entity to which MVA data, especially PII, is redisclosed
Suspension	A sanction that temporarily withdraws an agent's access to do business on behalf of an MVA
Threat	Potential cause of an unwanted incident, which might result in harm to a system or organization
TPA WG	Third-Party Agents Working Group
Unauthorized use	Intentional, improper use of MVA data for unauthorized purpose. An example is using access to MVA data to find an ex spouse's address.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled
VPN	Virtual private network
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats

* https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html

Chapter 1 Overview of Privacy Laws and Standards

Privacy, as it pertains to MVAs, is the protection of PII or data provided to the MVAs by an individual. Because MVAs are stewards of a significant amount of personal data, privacy is a primary concern. Privacy regulations balance the needs of government to provide public services with the individual's right to the protection of their personal data.

In addition to privacy, confidentiality is a standard applicable to the protection of PII or personal data. Examples of confidentiality include data in law enforcement investigations, trooper or officer PII, computer system network topology diagrams, passwords, or access codes. Privacy, by contrast, includes PII such as name, address, driver's license number, SSN, or medical information about an individual. Whereas data privacy relates to information about an individual, confidentiality might relate to programs, actions, the protection of someone working in an official capacity, or protection of vulnerable populations.

Several laws and standards apply to protection of MVA data. The following are detailed descriptions of common MVA compliance obligations.

- Criminal Justice Information System (CJIS): Criminal justice information (CJI) is frequently provided to law enforcement agencies (LEAs) to perform their mission and enforce the law, such as investigations, identity history, person, organization, property, and case or incident history data.
- Payment Card Industry (PCI) Compliance: The technical and operational standards that businesses should follow to ensure that credit card data provided by cardholders is protected
- DPPA: In the United States, personal information, including highly restricted personal information as defined in 18 U.S.C.S. 2725, contained in a motor vehicle record shall or may be withheld pursuant to the federal DPPA.
- Tax information: Information related to property taxes and personal taxes; may also include social security numbers
- Insurance information: Information related to insurance policies for vehicles or individuals
- Medical information: Information related to disability or medical conditions of an individual
- Administrative Adjudication Information: Information related to administrative or civil proceedings, hearings, restrictions, or other matters adjudicated in a noncriminal justice venue

This section provides a foundation for privacy expectations for MVA data. The section also discusses the implications of identifying, tracking, and reporting ongoing privacy compliance requirements.

1.1 DPPA

The DPPA, 18 USC §2721, is a landmark U.S. law designed to prohibit state departments of motor vehicles from disclosing PII without consent of the data subject unless the requester meets an articulated statutory exception. Prior to DPPA enactment, PII contained in MVA records was largely available to the public.

The DPPA defines "personal information" as "information that identifies an individual, including

an individual's photograph, social security number, driver identification number, name, address (but not the five-digit ZIP Code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status."* The DPPA defines "highly restricted personal information" as "an individual's photograph or image, social security number, medical or disability information."† Congress has shown the intent to differentiate types of PII to ensure a higher level of protection for photos, SSNs, and medical information.

If a state Department of Motor Vehicles is found to have "a policy or practice of substantial noncompliance" with the DPPA, the Attorney General may impose a civil penalty against the agency of up to $5,000 per day. In addition, individual states may impose penalties against an MVA for unauthorized use or unauthorized release of PII.

The DPPA provides MVAs with defined "permissible uses," which determine whether PII can be disclosed by the MVAs. Some of these permissible uses are mandatory, but most are permissive.

MVAs must disclose personal information under the DPPA in certain situations. The following is a list of must-disclose reasons pursuant to 18 U.S.C. §2721(b):

1. For use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories
2. For use in performance monitoring of motor vehicles and dealers by motor vehicle manufacturers
3. For use in the removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti-Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321–331 of title 49

MVAs may disclose information for other articulated reasons including the following:

1. For use by any government agency, including any court or law enforcement agency, in carrying out its functions. (18 U.S.C. §2721 (b)(1))
2. For use in connection with motor vehicle market research activities, including survey research. (18 U.S.C. §2721 (b)(2))
3. To verify the accuracy of information provided by a business, or to correct information provided to the business for purposes of preventing fraud by, pursuing legal remedies, or recovering on a debt or security interest. (18 U.S.C. §2721 (b)(3))
4. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to a court order. (18 U.S.C. §2721 (b)(4))
5. For use in research activities and for use in producing statistical reports, so long as the personal information is not published, re-disclosed, or used to contact individuals. (18 U.S.C. §2721 (b)(5))
6. For use by any insurer or insurance support organization, or by a self-insured entity or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating, or underwriting. (18 U.S.C. §2721 (b)(6))

* 18 USC § 2725(3).

† 18 USC §2725(4).

7. For use in providing notice to the owners of towed or impounded vehicles. (18 U.S.C. §2721 (b)(7))
8. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection. (18 U.S.C. §2721 (b)(8))
9. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license. (18 U.S.C. §2721 (b)(9))
10. For use in connection with the operation of private toll transportation facilities. (18 U.S.C. §2721 (b)(10))
11. For any other use in response to requests for individual motor vehicle records with the express consent of the person to whom such personal information pertains. (18 U.S.C. §2721 (b)(11))
12. For bulk distribution for surveys, marketing, or solicitations with the express consent of the person to whom such personal information pertains. (18 U.S.C. §2721 (b)(12))
13. For use by any requester with the express written consent of the person to whom such personal information pertains. (18 U.S.C. §2721 (b)(13))
14. For any other use specifically authorized under the law of the state that holds the record, if such use is related to the operation of a motor vehicle or public safety. (18 U.S.C. §2721 (b)(14))

Although the DPPA or applicable law is quite broad in its permitted uses, it is ultimately up to the MVA to decide which discretionary purposes are appropriate. The MVA can balance the privacy rights of individuals with the potential benefits of disclosing the data responsibly.

1.2 U.S. Privacy Act

The U.S. Privacy Act of 1974, 5 U.S.C. §552a, "attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies."* The U.S. Privacy Act of 1974 only governs executive branch agencies of the federal government and generally does not apply to state agencies, except for very specific provisions. The law requires federal agencies publish notice of any "systems of records" or collection of records that might contain identifying information. The law prohibits the disclosure of an individual's record absent that individual's written consent unless the disclosure meets one of the 12 statutory exceptions. Carving out 12 exceptions is similar to establishing permissible uses or specific instances when personal information can be disclosed by an MVA, as detailed in the DPPA.

1.3 Canada's Privacy Act

Canada's Privacy Act (R.S.C., 1985, c. P – 21) is designed to "protect the privacy of individuals with respect to PII about themselves held by a government institution and that provide individuals with a right of access to that information."† Similar to the U.S. Privacy Act, Canada's Privacy Act requires Canadian government agencies to inform individuals why their information is collected and disclose specific instances when it may be disclosed. This act applies only to federal government agencies that process PII and does not control provinces.

1.4 Fair Credit Reporting Act (FCRA)

The FCRA, 15 U.S.C. §1681, was enacted in 1970 to "require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes." The FCRA was an early example of a data protection law.‡

* https://www.justice.gov/opcl/introduction

† https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-397172

‡ https://en.wikipedia.org/wiki/Fair_Credit_Reporting_Act

1.5 General Data Protection Regulation (GDPR)

The GDPR, (EU) 2016/679, became effective in May 2018. The regulation applies to processing and protection of personal data by organizations (called "data controllers") that hold data about European Union (EU) residents. GDPR contains principles that provide a legal basis for processing an EU resident's PII. Similar to the U.S. Privacy Act, the GDPR provides for "filing systems" or systems of records and specific reasons why an individual's personal data might be processed. EU residents' GDPR provisions and principles include:

- The right to protection of (a data subject's) personal data*
- Technical and organizational controls in place
- Use data for its intended purpose
- The right to be forgotten
- Application to all for-profit and not-for-profit organizations
- Permissible use or categories of use

Principles of GDPR may inform the development of privacy best practices for MVAs.

1.6 State, Provincial, and Territorial Privacy Statutes

Many states, provinces and territories have adopted statutes that protect PII and the privacy of individuals. Jurisdictional statutes may extend protections to additional types of data, such as vehicle information or crash data. For an MVA to release any data, the data recipient should be entitled to the information under both the controlling federal or national and jurisdictional law. In other words, an MVA should comply with the strictest protection addressing MVA data.

A recent state privacy law, the California Consumer Privacy Act (CCPA), 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST), became effective January 1, 2020. The law is significant in scope and "creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses."

The CCPA applies to for-profit businesses in California; it does not apply to governments, and thus, it does not apply to MVAs. However, its provisions are important because they reflect evolving privacy expectations and standards.

As of May 29, 2020,† 19 states had introduced comprehensive privacy bills, with three jurisdictions' bills becoming law. There are many common threads to these laws (and prospective laws), in that most include provisions on the following subjects:

- Right of access
- Right of deletion
- Right of portability
- Notice or transparency requirement
- Prohibition on discrimination (exercising rights)

Not all jurisdictions have new or recently amended privacy laws, but it is important to track legislative trends like these to ensure data systems and privacy practices are elastic enough to accommodate new laws.

1.7 Open Records Laws

Many government records are presumed to be public, absent a specific reason to withhold them. This is an underlying basis of open records laws. Specific laws, such as the DPPA, provide exemptions for release of certain MVA records.

The U.S. Freedom of Information Act (FOIA), 5 U.S.C. §552, enacted in 1967, establishes the public's right to request records from federal agencies, and many states have an equivalent law to allow access to MVA records. The presumption articulated in FOIA laws is that public records not protected by specific

* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

† https://iapp.org/resources/article/state-comparison-table

privacy laws, such as the DPPA, will be open to the public.

Canada's Access to Information Act, (R.S.C., 1985, c. A-1), provides the right of access to information contained in records maintained by the federal government and sets out requirements for proactive publication of information.

1.8 National Institute for Standards and Technology (NIST)

Nonstatutory guidance comes from NIST, which publishes a number of standards on privacy and security, many of which are cited by this best practice. NIST Special Publication (SP) 800-53 Revision 4 Appendix J is a Privacy Control Catalog that is applicable to this best practice. The Privacy Control Catalog emphasizes the connection between privacy, security, and risk management.

1.9 International Organization for Standardization (ISO)

ISO is a nongovernmental organization that publishes internationally used standards such as the ISO 27001 information security standard. ISO 27001 is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body after successful completion of an audit.

Chapter 2 Data Strategy and Framework

2.1 Introduction

Good management and governance of data support the protection of MVA data and individual privacy. Development of a strategy and framework for managing and governing data allows the MVA to better understand what data it has, who manages and "owns" the data, and what decision rules are in place to protect and keep the data whole, visible, and protected.

This section reviews principles of data management, data governance, and their relationship to protecting MVA data. Included are high-level concepts and a quick step guide for establishing a framework for protecting data with formal data management and data governance.

Data management is defined by the DMBOK as "the development, execution, and supervision of plans, policies programs, and practices that deliver, control, protect, and enhance the value of data and information assets through their lifecycle."

2.2 What Is Data Management and Data Governance?

Data management and governance are key management practices in the overall health of organizational data. Determining appropriate governance of a data privacy program is challenging and complex. Data management is defined by the Data Management Book of Knowledge (DMBOK®) as "the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets through their lifecycle."* A key output of data management is a data management plan, a document used to relate data to the underlying goals and strategy of an organization. If a strategic goal of an organization is to protect its data, a data management plan will help the organization achieve that goal by outlining steps to take.

Data governance is an approach that addresses many aspects of data management, including information privacy, security ,and compliance. Data governance is the set of processes, rules, responsibilities, and formal decision making to manage MVA data. DMBOK® defines data governance as "the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets."† Data governance adds formal structure to data management by ". . . establish(ing) authority and management and decision-making parameters related to the data produced or managed by the enterprise." Data governance works closely to develop the policies and procedures required to support the organization's data management activities. Data governance emphasizes creation of data owners and data stewards who have responsibility for fulfilling data management concepts and for carrying out the data management plan. The role of the data steward is to manage data in a specific program or area of operation. This includes "integrity, quality and consistency of the organization's data." Data stewardship has not traditionally been a role filled by MVAs but is a key role in the development of an organization-wide data strategy and framework.‡

Both data governance and data management focus on managing the information that improves business outcomes and specific processes while assessing the value the data provides to decision making and

* Data Management Book of Knowledge, © 2017 DAMA International, page 17.

† Data Management Book of Knowledge, © 2017 DAMA International, page 67.

‡ AAMVA, "System Modernization Best Practices," May 2017, page 42, available from https://www.aamva.org/SystemModBP/.

strategic planning. Despite their close relationship, however, there is a meaningful difference between data governance and data management. Data governance is the decision-making and rule structure that provides authority over data management.* Data management is the development and application of "plans, polices, program, and practices that deliver, control, protect, and enhance the value of data and information assets throughout lifecycles."† Stated differently, whereas data governance oversees and sets the rules for data management, while data management is the act of managing, controlling, protecting, and deriving value from data. Data governance establishes the frameworks in which data management operates; data management is the plan of action, and the separation between the two creates "an inherent separation between oversight and execution."‡

2.3 Current Adoption of Data Management and Governance by MVAs

Several MVAs have existing data management and governance programs. This section focuses on programs in three states: Florida, Pennsylvania, and Washington. The Florida Highway Safety and Motor Vehicles (FLHSMV) has a formal data management plan and a data governance policy and program.§ FLHSMV's data management and governance plan provides the agency with a structure to manage its data. Its scope covers key roles in the management of data, cataloging of data, security and privacy considerations, retention and storage considerations, audit, and interrelation of data in the agency. The data management plan allows the agency to understand:

- What data it has
- Why the data are collected
- Where the data come from
- Who has access to the data
- Who or what changed the data and for what purpose
- How data should be managed

A 2019 AAMVA survey of MVAs showed that about half the respondents were aware of a data governance program at their MVA. The remainder of respondents indicated there was no data governance program, they were not familiar with data governance, or they were not sure if their jurisdiction governed the use of data.

The FLHSMV data governance policy establishes a means to "catalog, safeguard, and improve the quality of data assets."¶ The data management plan and governance policy work together to govern and manage MVA data. The plans and policies identify the importance of specific MVA roles. This includes identification of data owners and stewards who understand the business processes that require collection of data, what constitutes accurate data, how the data are used, how long the data should be maintained (retention considerations), and how the data can be improved from a usage and quality standpoint.

Pennsylvania requires MVA compliance with an Enterprise Data and Information Management Policy. The policy establishes a Commonwealth-wide standard for managing data. The policy asks agencies to establish a data governance structure, including a master data management plan. The data management plan covers all or nearly all facets of data, including data management processes, creation of data roadmaps, metadata definition, and data integration. The policy covers, in detail, much of the content recommended in the Quick Guide to Data Management and Governance in this section.

Washington State Department of Licensing has developed a data governance board and structure. The following figures** show the operational areas covered by a data governance program.

* Spacey, John, "Data Governance vs Data Management," November 2016, available from https://simplicable.com/new/data-governance-vs-data-management

† Data Management Book of Knowledge, © 2017 DAMA International, page 17.

‡ Data Management Book of Knowledge, © 2017 DAMA International, page 72.

§ Florida HSMV Data Governance Policy, https://www.flhsmv.gov/pdf/policies/1202.pdf and Florida Highway Safety and Motor Vehicles Data Management Plan

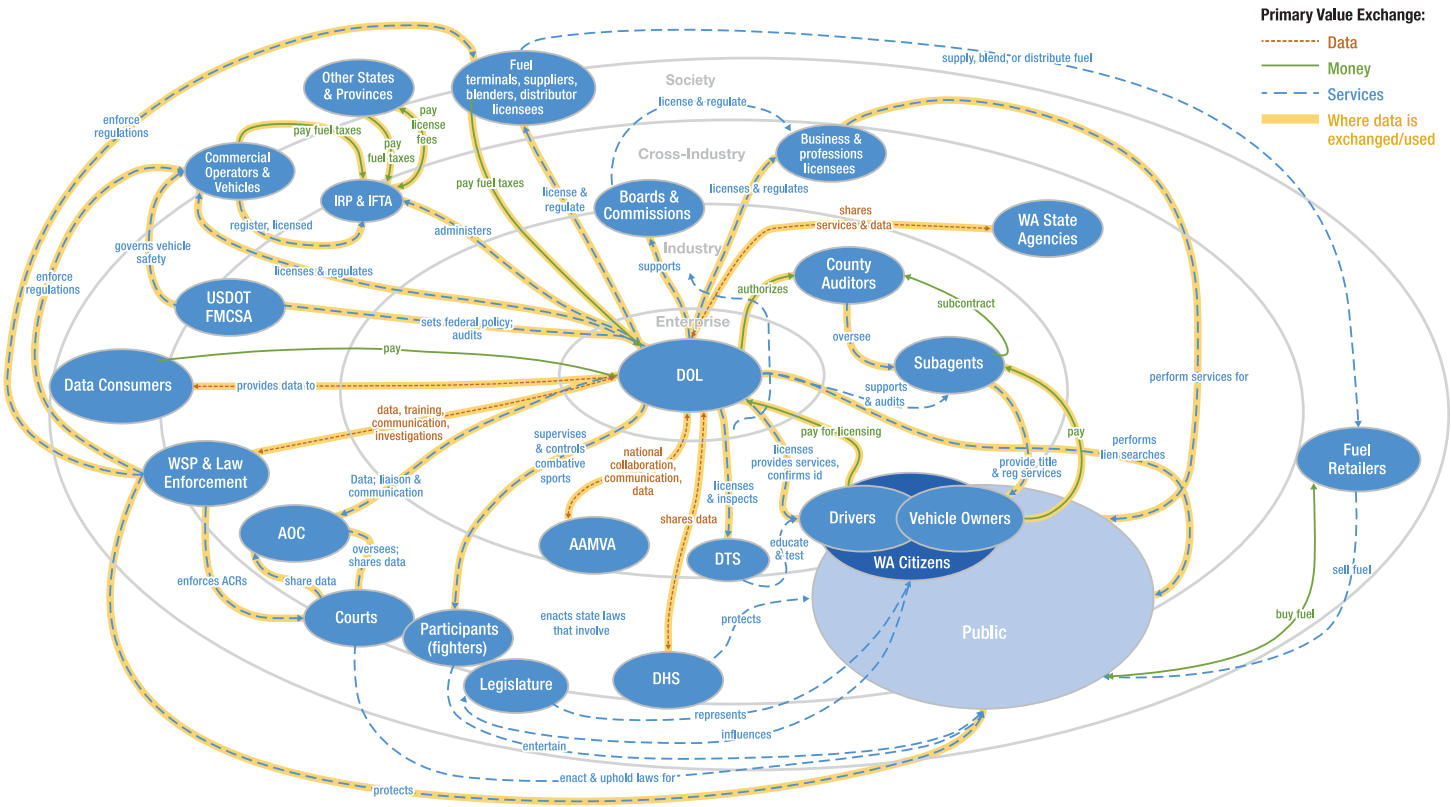
¶ https://www.flhsmv.gov/pdf/policies/1202.pdf, page 3.

** AAMVA, "Data Privacy: Is It Really Private?" Washington Department of Licensing, AAMVA Region 4 Conference, July 2019, available from https://www.aamva.org/workarea/downloadasset.aspx?id=12975


CREATION
CAPTURE
SYNTHESIS
AGGREGATION
STORAGE
SECURITY
ACCESS
ANALYZE
SHARE
ARCHIVE
PURGE


Business Units
Collect Data
Create Data
Manage Data
Use Data
Research & Analysis Office
Data Analysis
Data Reporting
Data Science
Data Requests
I.T. Office
Data Storage
Data Architecture
Database Admins.
Data Security
Records & Disclosure Offices
Records Mgmt.
Records Retention
Public Disclosure
Data Sharing Contracts
ata Contracts Mgmt
Compliance Audits
Data Governance Board


TOP SECRET
CONFIDENTIAL
TOP SECRET
DATA INTEGRITY
Data Confidentiality
• Privacy
• Sensitivity
• Security
Data Integrity
• Quality
• Ethics
• Standards
Data Availability
• Timeliness
• Retention
DATA GOVERNANCE POLICIES



The above diagram shows the Washington State Department of Licensing Data Ecosystem. The ecosystem provides a good visual representation of data processing and data sharing and exchange, as well as where revenue is generated from data exchange. Mapping data flow allows the MVA to understand what data it has and where the data are sent so that data privacy can be better accomplished.

2.4 Relationship Between Data Governance and Managing Data Privacy

Data governance and management provide broad organizational benefits but particularly support privacy protection. The DMBOK® definition of governance ("the exercise of authority and control [planning, monitoring, and enforcement] over the management of data assets") also applies specifically to privacy. A governance program can be applied to identify or establish privacy-specific policies, such as policies on the appropriate use of specific data. To establish a data privacy program, organizational structure should be determined and include strategy, operations, and management for responsibilities and reporting. A data governance and management plan identifies MVA roles for the management of privacy. This includes data stewards, data owners, and a data governance board or committee that creates a cross-functional team to govern the use of data and management of privacy within the MVA. A strong governance model includes the legal framework that protects data and also provides guiding principles for MVAs to follow. In other words, laws that guard against an unwarranted invasion of personal privacy (e.g., disclosure of an address without a specific, permissible use) also provide guiding principles for privacy protection.

2.5 Quick Guide to Data Management and Governance Adoption

A data governance program requires broad participation throughout an MVA. Outreach and education should include identification of data governance stakeholders (from data stewards to executives), identification of stakeholder goals and

needs or concerns for use of data, communication about goals of data governance, creation and execution of awareness, and education campaigns.

It is important to note that data governance and management take time to develop. Data management plans and governance policies may become detailed and require sustained effort for development and maintenance by MVAs.* †

An incremental approach is recommended. The following provides some initial guidance on adoption of data management and governance plans and policies for consideration in an MVA:

- Establish a data governance policy to create the governing body that will develop and execute data management plans. Steps to develop data governance policies and data management plans include:
  - Develop data governance policy and charter: Define what data governance will mean to the organization. What value does MVA data have, and how do they support the organizational strategy and goals?
  - Establish current state: Assess current data management, identify areas of risk, and develop a roadmap to future state. This includes establishing data governance program metrics, such as categorizing assets, data assets discovery, and data steward identification.
  - Make data governance updates to project management documentation: Incorporate data management practices into project management practices so that any new project enhances or protects the management of MVA data. This is the "privacy by design" concept, or the adopted discipline of collecting and processing data with privacy in mind at each step.
  - Determine data asset value: Define the operational value and risk potential of their data assets.
  - Prioritize business data: A data governance plan should identify data assets in priority order and plans for improving or correcting data sets so that the data is more reliable.
- Identify data owners and data stewards. Data owners and stewards are accountable and responsible for the specifications and quality of data sets.
- Create a data catalog. A data catalog is a detailed analysis and listing of all data received by the MVA. A data catalog accounts for all MVA records and data, including the means by which it comes to the MVA. Most data come to MVAs from formal channels, such as the submission of a driver's license or vehicle registration application, but some data come in from less formal channels, such as texts (SMS, or short message service), instant messaging, and social media feeds. All might contain PII.

A catalog of data and records may include a list of records considered public. This type of catalog can help an MVA understand the full scope of records and data for which it is the custodian. The catalog can also provide clarity about which data are considered public (e.g., contracts, maps, organization charts, and other nonconfidential records) and therefore not subject to as rigorous protections as nonpublic data.

- Establish data security (accessibility, protection, and sharing) protocols. These are the standards by which data will be protected. See the Impact Risk and Security sections for more detail.
- Identify data privacy and regulatory compliance considerations, as established in the Overview of Privacy Laws and Standards section.

* Common standards for development of these plans include the DMBOK®, Control Objectives for Information Technologies (COBIT)©, and the Data Governance Institute (DGI). Use of other jurisdictions plans as a best practice is recommended.

† Florida Department of Highway Safety and Motor Vehicles, "Data Governance Roadmap," 2019.

- Establish data storage, retention, and purge policies. These are records management best practices and are defined in a data management plan.
- Establish data quality policies (completeness, timeliness, and accuracy of data), a key area for consultation with data stewards and owners.
- Identify data integration or relationships (connecting multiple data sources). This includes data mapping and how, or with whom, data are shared, both internally and externally. A relational map is a helpful outcome of this exercise. See the Washington State Department of Licensing Data Ecosystem in the appendices for guidance.
- Establish references and master data based on industry standards, such as SSN length, VIN, or ZIP Code. Standards allow data to be entered consistently and ensure data integrity.
- Create a data dictionary. A data dictionary is repository of metadata, or "data about data." It includes data about data elements, such as a description, date the data element was created, when the element was last modified, its file size, timestamp, and so on.
- Establish reporting and business intelligence. This is a process for developing data sets, reports, and other data visualizations that help an MVA make decisions.
- Establish data audit considerations (changes, movement, or deletion of the data). This step establishes what should be audited and which supporting documents are necessary for tracking compliance.
- Establish agreements, policies, and provisions for reuse or redistribution. See the Data-Sharing Agreement section.

"Protecting data privacy is an endeavor that is the responsibility of the department and our partners. We must know what data we have, why the data is collected, where the data comes from, track who or what has access to it, who or what changed it and for what purpose. A Data Management plan and Data Governance policy are the foundation of identifying and managing private and confidential data that must be protected and secured." —**SCOTT LINDSAY, Chief Data Officer, Florida Highway Safety and Motor Vehicle Division**

The steps provided above can be modified to meet the unique needs of each MVA. Recognizing that data are valuable organizational assets is a key driver of data governance and data management. Without that support, data governance and data management will be difficult to implement. Data governance should be driven by organizational mission and vision rather than by technology.

2.6 Recommendation

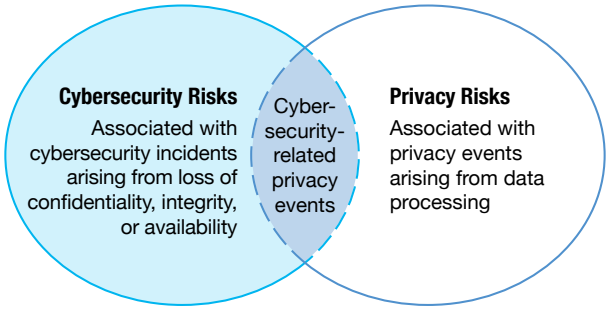
MVAs should adopt a data governance policy and data management plan.

Chapter 3 Impact and Risk Mitigation

3.1 Introduction

This section outlines a common risk management framework (RMF), which MVAs can use to recognize and mitigate the likelihood of adverse data processing, including unauthorized PII access, disclosure, or use.

The recommended RMF is derived from NIST and specifically, but not exclusively, the NIST Privacy Framework. The NIST Privacy Framework Version 1.0 was published in January 2020 and provides a tool for evaluating privacy risk and selecting controls to hedge against risk.* Within the NIST Privacy Framework is Appendix D: Privacy Risk Management Practices. Privacy Risk Management Practices includes a narrative about conducting privacy risk assessments. Also referenced in the Privacy Framework and Appendix D is a Privacy Risk Assessment Methodology (PRAM). The PRAM provides a means to evaluate how data are received by MVAs in each of their business services or systems, what risk is identified in doing so, the impact of the risk being realized, and what controls are in place to mitigate that risk. MVAs can use PRAM to conduct an analysis for each system, product, or service (e.g., a driver's license system, crash reporting system, or vehicle safety inspection station system).† Privacy risk, from the standpoint of the Privacy Framework, is concerned with data processing and data processing issues, or "problematic data actions." Privacy risk is not solely about cybersecurity risk. Cybersecurity risk, as defined by NIST, is "risks associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability," whereas privacy risks are associated with events arising from data processing. The following figure, as used in the NIST Privacy Framework, shows the intersection of cybersecurity and privacy risk.



Cataloging data privacy risks for each MVA system, product, or service consumes significant time. The process provided in this best practice is designed to be an abbreviated approach. Prior to beginning the steps outlined below, the MVA should prepare for a risk assessment, including

- Ensuring that a proper data governance structure is in place
- Dedicating appropriate resources to information security, privacy, and risk management
- Gathering, collecting, and documenting existing risk management information, mission, and objectives of the organization and affected business units, related business processes, related information systems, existing security and privacy controls and policies, and other relevant data

There are two main organizational levels at which RMF preparation occurs: executive and operational.

* National Institute of Standards and Technology (2020), The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, available from https://www.nist.gov/privacy-framework/privacy-framework

† National Institute of Standards and Technology (2019), NIST Privacy Risk Assessment Methodology (PRAM). (National Institute of Standards and Technology, Gaithersburg, MD), available from https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

Both levels have specific roles defined that participate in the process throughout its lifecycle.

The PRAM provides worksheets that an MVA can use to evaluate privacy risks for each system or service, in effect conducting a privacy risk assessment for each core system that fulfills business processes at the MVA. The following narrative provides steps for conducting PRAM-based privacy assessments.

3.2 Framing Business Objectives and Organizational Privacy Governance

Prior to implementing or changing privacy program aspects, MVAs should obtain executive authorization of the risk management plan developed through the PRAM. Authorizing a risk management plan creates organizational accountability by requiring a senior management official to determine if the plan is acceptable to the organization and reduces risk of wasted resources. A baseline plan is also created so that updates and plan version may be maintained.

The first step is to determine MVA organizational objectives for each MVA system, product, or service. A system, product, or service could be, for example, a driver's license system, a crash reporting system, or vehicle safety inspection station system. The following is an abbreviated list of steps to fulfill this activity:

- Conduct an as-is assessment of system, product, or service to determine current privacy posture.
- Define how the system, product, or service fulfills the MVA's mission or business need.
- Describe functional needs or capabilities of the service.
- Define MVA privacy standards.
- Describe the legal requirements surrounding the system, product, or service (e.g., DPPA, FCRA, or other statute or legal frameworks that must be observed).
- Conduct a gap analysis of legal requirements.
- Describe any privacy-related principles (e.g., FIPPs).
- Identify MVA privacy standards that impact the system, product, or service and any privacy-related policies or statements within the MVA or a division or unit of the MVA.

3.3 Determine System, Product, or Service Design

After the development of business objectives and privacy governance, the MVA should assess the system, product, or service design. This step involves mapping the process and data used by the system, product, or service. Mapping should follow the data lifecycle: the business process (including human actors or individual), data intake, processing, disposition (data storage or destruction), and any data recipients. A crash records system, for example, has multiple data transfer points, such as between LEAs, the MVA, and federal or national reporting databases. Crash report retention periods are established by statute and should also be documented. The following steps are taken to complete this activity:

- Determine system, product, or service privacy capabilities.
- Identify the system, product, or service, its purpose and features (e.g., which organizations use data from the system, product, or service; which privacy rules govern the use of the system, product, or service [e.g., DPPA, PCI, FCRA]; how individuals interact with the system; and the privacy interests individuals have with the system).
- Create data map and accompanying system, product, or service flow.
- Conduct data action analysis that identifies data collection actions in each system, context of each, and any summary issues associated with the data action.

During this step and related to system, product, or service identification, conducting data categorization will help determine the adverse impact to the MVA should there be a compromise or loss of organizational assets. In the case of driver and vehicle data, there are laws and regulations that apply, such as the federal DPPA and related jurisdictional laws. DPPA distinguishes between personal information and highly personal information because not all data have the same degree of sensitivity and threshold for disclosure.

3.4 Prioritize Risk

In risk prioritization, identify the likelihood of a data action creating problems or issues. Following the crash reporting system example, an MVA might identify that PII, such as a driver's license number or address, is collected and processed, and even sensitive PII, such as medical condition, is also processed. A problematic data action could be inclusion of sensitive PII in a crash reporting database in which the PII is not completely anonymized. This might result in loss of expected privacy for the individual with a medical condition. Potential risk impact should be assessed in terms of loss or cost to the MVA, such as reputational loss, costs of noncompliance, or other impact. It is important to note that compliance risk is different than privacy risk: an MVA may be in full compliance with, for example, the federal or jurisdictional law but still incur risk by data actions. The following steps are taken to complete this activity:

- Assess the likelihood of problematic data action.
- Determine the impact of problematic data action.
- Calculate the risk based on problematic data action likelihood and impact.
- Prioritize identified risks.

3.5 Select Controls

The final step of the process is to define risk mitigation controls. This step entails identifying system, product, or service requirements to reduce privacy risk followed by selecting controls. Controls may be found in publications such as NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems. NIST SP 800-53 (800-53) is a well-known and a broadly used standard that catalogs security and privacy controls for information systems and information and provides a process for selecting these controls. In conjunction with FIPS 200, it provides a clear selection process and list of controls that will be applicable to most information and information systems. 800-53 includes Appendix J: Privacy Control Catalog. The Privacy Control Catalog provides "families" of privacy controls and has linkage to the FIPPs, which form the basis for principles used throughout this best practice.

Using the PRAM, the following steps are taken to complete this activity:

- Identify system or service requirements.
- Select controls to mitigate risk.

3.6 Additional Steps and Guidance

After selection of controls, an MVA needs to implement them. The process of implementing controls is time consuming, but it provides a foundation for privacy protection. MVAs need time to complete this iterative process and conduct periodic, externally sourced audits of their controls. A Service Organization Control (SOC) audit may be one such avenue. Regular internal assessments are important to ensure the proper application of controls and to adjust assessment requirements in a controlled and documented way as requirements change or are updated.

When developing a privacy program, MVAs might find it useful to establish both a baseline understanding of privacy compliance and a future privacy state, or "target profile." A future privacy state allows the MVA to evolve its current privacy posture to one with more stringent privacy requirements via a gap analysis. The gap analysis can provide the foundation for a plan or roadmap between current and future state. The roadmap can detail the budget, staffing, and other resources needed to realize an improved future privacy profile and program.

For more information, please consult the NIST Privacy Engineering Program and the Privacy Risk Assessment Methodology (PRAM), available from https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources. This link provides access to worksheets that MVAs can use to complete the steps outlined above.

3.7 Recommendations

- Conduct a risk assessment using an established protocol, such as NIST.
- Include an evaluation of current state and future state in a risk assessment.

Chapter 4 Analysis of Request

4.1 Introduction

MVAs receive different types of requests for the release of motor vehicle and driver data. This section provides best practices for analyzing these requests to assist jurisdictions in deciding whether to release the information and how to provide it to the requester.

4.2 The Application Process

The DPPA, Canada's Privacy Act, and individual state, provincial, and territorial laws protect the PII in driver and vehicle databases maintained by jurisdictions. The DPPA creates an independent cause of action for the individual to whom the information pertains against anyone who knowingly obtains, discloses, or uses such information without a permissible purpose under the law. Because of the significant consequences of improperly releasing customer data, MVAs should ensure that entities requesting customer information are properly vetted and documented.

"It is critically important for DMVs to have knowledge of the entities that are accessing driver and vehicle data and the intended use." —MIKE DIXON, Senior Director, Division of Motor Vehicles, Colorado Department of Revenue

Developing and implementing an application process for requesting MVA data will help balance the public's interest in governmental transparency and statutory and regulatory compliance with individuals' need for privacy. The application process should account for one-time, ongoing, or bulk requests. The application must collect sufficient information to determine if data should be released to the requester, information the requester is entitled to receive, and the appropriate method of data transmission. The application step should be a separate process from the execution of a data-sharing agreement, which will ultimately define the controlling terms and conditions of use. Bulk data requests require a more substantive application and agreement. For individual or nonbulk data requests, MVAs should have an abbreviated application or data-sharing agreement template.

At a minimum, the application should cover the following topics:

- Identity of the requesting individual or organization
- History of unauthorized use or data-sharing agreement violations from previous data uses
- Type of data requested
- Purpose of the request
- Volume and frequency of the requests
- Data usage
- Method of data transfer
- Security standards and data storage
- Fees for records or data

The application should also require supporting documentation to verify the information provided by the requester as well as an attestation that all the information provided by the requester is accurate. Each of the bullets above is further addressed in detail in the following sections.

The application itself is a public record to be maintained and destroyed in accordance with the MVA's record retention policies. Thus, MVAs should be careful not to request documentation or information that is not necessary for the application review process and should ensure the information provided by the requester on the application is properly protected.

4.3 Review of the Application

MVAs may offer a universal application to cover all data requests or individual applications that reflect factors such as type of data requested, volume of requests, or category of requester. This could be determined by whether the MVA maintains driver and vehicle data in separate databases or if the MVA wishes to offer an application for each type of data. MVAs may also choose to have an application available for one-time requests and a separate application for recurring disclosures or system access requests. MVAs may also make a distinction between government and commercial data requesters. Although the minimum requirements should be included in every application, the number and format of the applications may be adjusted to fit individual business models.

MVAs might consider the following guidance for application workflow:

- Review of individual applications by business, legal, information technology (IT), and information security personnel is optimal. This level of review helps ensure that subject matter experts in all relevant areas are reviewing the information submitted by a requester. After the application is approved by all necessary parties, the request can advance to the data-sharing agreement and implementation processes.
- If individual review is impractical by each professional mentioned earlier, then the MVA can create agreed-upon criteria to help identify which applications should be elevated for further scrutiny. For instance, the business area reviewing each application could have a checklist of applications that would require follow-up (e.g., insurance company requester did not provide proof of incorporation) and of applications that would be sent to another work area for review (e.g., employer does not have antivirus protection on the system that will access MVA records).
- Use templates for application review to mitigate risk. Establishing minimum standards with which all internal groups are comfortable can also help expedite the application process and mitigate the need for individual application scrutiny.

Identity of the Requester: Who Is Asking?

External entities requesting data can vary widely, including government entities, the public, law enforcement, insurance companies, licensed private investigation agencies, employers, toll authority companies, commercial entities, driver training schools, court systems, and other data recipients. Prior to releasing a record or an individual piece of data, the MVA must ensure that the requester is entitled to the information under law. If the law states the MVA shall release the information to the requester, then disclosure is mandatory, and the jurisdiction may not choose to withhold the information. In most cases, however, the release of the data to certain parties is permissive rather than mandatory. As a matter of policy, MVAs should ensure consistency and fairness in exercising discretion to release information. A best practice for permissive release of data is to treat all similarly situated requesters consistently. For example, if an MVA has decided to permit release of certain data to a toll authority, then all toll authorities that request such data should receive the same information, all other factors being equal.

History of Unauthorized Use or Significant Data-Sharing Agreement Violations from Previous Data Requests: What Has the Requester Done Before?

MVAs might wish to require information relating to the requester's history of data usage and business practices in any jurisdiction as a determining factor when deciding if sensitive data should be released. Responses to questions such as whether the entity has ever been subject to MVA administrative action, has been found to have violated federal or jurisdictional privacy laws, or has been convicted of a crime relating to computer fraud or unauthorized access to data may be used in an analysis of whether to release the requested data.

Type of Data Requested: What Are They Asking For?

The identity of the requester and the type of data requested should be analyzed together. Some requesters may be entitled to receive individual pieces of data, and MVAs should ensure policies are in place to prevent disclosing information beyond that which is permitted by law. As an example, an attorney attempting to locate an individual to serve legal papers that pertain to a motor vehicle crash may be entitled to receive name and address information. The same attorney may not be permitted to have access to that customer's SSN. The application process should ensure these critical pieces of information are collected in detail and that controls on data disclosure are in place.

Generally, disclosure of nonpersonal vehicle information (e.g., how many blue Fords are registered in X county) poses less risk to the MVA and customers than disclosing personal driver information (e.g., the names and addresses of all registrants with blue Fords). This does not mean, however, that other types of data without PII may be freely released. Some jurisdictional statutes provide additional protections for other types of data, such as aggregated vehicle and driver information. Consider also that a piece of information may become PII when released with other data elements such that an individual person may be identified.

Purpose of the Request: How Are the Data Going to Be Used?

MVAs should also require data requesters to articulate how they will use the data during the application process. The same requester might be entitled under the law to receive a piece of data for one permissible use while at the same time be barred from using the data for a different purpose. For instance, customer name and address information should be released for recall purposes under federal law, but the data recipient might be barred from using that same data for solicitation purposes under state law. Furthermore, the DPPA makes it unlawful for any person to "obtain or disclose" personal information from a motor vehicle record for any reason not permitted under the law. Therefore, it is important to have the requester stipulate in the application process which specific permitted use applies. MVAs might want to create a list of approved purposes for requesters to check on the application. If an MVA chooses to create a checklist on the application, it should include all permissible uses for which the MVA will allow data sharing.

MVAs should also require data recipients to indicate if the data will be re-released to subrecipients. Subrecipients should have both a permissible use under the DPPA (if in the United States) and be entitled under state or provincial law to receive the data from the data recipient. This arrangement should be regulated through the data-sharing agreement, but the disclosure of subrecipients should be done at the application step if possible. When a data recipient begins sharing MVA data with a new subrecipient, it should be reported to the MVA at agreed-upon intervals.

Some data recipients consider their client lists of subrecipients to be proprietary information. Data recipients and MVAs may identify a process by which data recipients identify subrecipient names that, if disclosed, would harm the data recipient's competitive position. MVAs may withhold such information if permitted by the MVA's public records statutes.

Volume and Frequency of the Requests: How Often Are Data Requested?

As part of the application process, MVAs should require the requester to identify the frequency with which they would like to receive the data. For requesters who wish to receive the same type of data in a large volume or on a regular basis, the MVA should require the completion of a data-sharing agreement. For low-volume record requests, such as those that only request once or twice a year, MVAs might wish to adopt an abbreviated data-sharing agreement process. Although this is an acceptable business practice, the application process should remain the same regardless of whether a data-sharing agreement is completed to establish a permissible use. MVAs should have a process for revalidating or verifying identification credentials of regular or routine requesters.

Data Usage: Will the Requester Give the Data to a Subrecipient?

It is important to determine whether an applicant for MVA data plans to redisclose the information. Many recipients of driver and motor vehicle information repackage and redisclose the information as part of their business model. For example, a large data company might use the bulk data provided by the MVA, rearrange it, and provide it to car dealerships for research purposes. It is crucial to know what the requester ultimately plans to do with the data up front and determine allowable use before disclosing any information or entering into a data-sharing agreement.

Method of Data Transfer: How Does the Requester Want to Receive It?

MVAs should collaborate with their respective business, IT, and IT security teams to determine methods of data transfer that are acceptable, cost-effective, secure, and practical. The method of data transfer varies widely across MVAs, and statutes typically do not prescribe acceptable or mandated data transfer methods. Some examples of ways to transfer MVA data include:

- Mail paper records
- Electronic transmission by facsimile or secure email exchange
- Self-service online manual inquiry
- Secure file transfer protocol (SFTP) Batch file (daily, weekly, monthly, quarterly)
- Bulk data file through managed file transfer
- Real-time system direct login (government and law enforcement entities)
- Cloud-based storage, given proper security protocols

Security Standards for the Data Recipient: Is the Requester Safe?

MVAs may choose different methods of data transmission based on the data recipient's ability to meet IT security requirements. Such standards should be specified in the application, for example, compliance with ISO 27001 or the CJIS Security Policy (CSP). The application process might also include certification that the recipient's encryption meets FIPS 140-3 or documentation that CJIS Security Awareness training has been completed within the past two years by all personnel with unescorted access to the data.

MVAs may ask comprehensive security questions to determine the overall environment of data protection. Questions might concern

- The type of environment in which the data resides (e.g., virtualized, SFTP server)
- Whether the data recipient is using any end-of-life or unsupportable software or hardware to store MVA data (e.g., Windows Server 2008R2, CISCO ASA 3002)

- Whether cloud services and storage are being used and what security standards are applied
- Whether the data recipient conducts security assessments, such as penetration tests on a biannual basis
- Whether the data recipient is in compliance with regulatory requirements for the individual industry
- Whether the data recipient secures sensitive data in storage and in transit and the data recipient's plan for identifying and addressing cyber threats
- Whether the data recipient utilizes anonymization techniques

Verifying the Submitted Information: Did the Requester Support the Request?

Requiring substantiation for each request for MVA data, particularly if the requested data contains PII, is essential to making a determination. All requesters should provide a detailed outline of how the requested data will be used. To ensure the integrity of the process, jurisdictions might wish to require documentation to verify the intended purpose.

It is a best practice to verify the identity of the data requester. Conducting an informal internet background check and confirming that the business license is in good standing can help establish the company's validity. Many jurisdictions' applications require individuals to disclose a driver's license number, bar association number, or other identifying information.

The following table provides MVAs with suggestions as to the type of documentation that can validate a data recipient's identity or stated permissible use. MVAs may choose to validate one or more of each suggested piece of documentation as described in the table.

Permissible Use or Entity	Documentation to Validate
Government agency to carry out its official functions	• Citation to legal authority identifying entity's official function, such as a state code, regulation, ordinance, and so on • Validate government employee status via badge, official email address, or other proof of employment status from a government employee directory
Private entities obtaining data to notify customers in relation to motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories	• Company charter, annual report, or financial statement • Statement on company letterhead from an authorized applicant • Proof of incorporation, if applicable
Representative of motor vehicle manufacturer for purposes of performance-monitoring of motor vehicles or dealers	• Company charter, annual report, or financial statement • Statement on company letterhead from an authorized applicant • Proof of incorporation, if applicable
An insurance company for use in connection with claims investigation activities, antifraud activities, rating, or underwriting	• Business license or certification from controlling jurisdiction (e.g., a Department of Insurance) • License or license number of insurance agent
A licensed private investigator for purposes of locating the owner of a vehicle (or other purpose allowed under state statute)	• Copy of license from criminal justice agencies
An employer seeking the driving record of a commercial driver employee	• Proof of employer–employee relationship • Business documentation and function, such as company charter, incorporation documents, and so on

(continued on next page)

(continued from previous page)

Permissible Use or Entity	Documentation to Validate
An employer seeking the driving record of a noncommercial driver employee (with consent)	• Proof of employer–employee relationship. • Business documentation and function, such as company charter, incorporation documents, and so on • Proof of employee consent or authorization
Attorney on behalf of a client for client's driver or vehicle information	• Proof of attorney–client relationship, such as a retainer agreement or other consent documentation
Private toll facility for use in toll enforcement	• Agreement with state to operate toll, statutory authority, or incorporation documentation
Towing or storage companies for use in notifying customers of towed or impounded vehicles	• Copy of license or operating authority from jurisdiction

Attestation: Will the Requester Stand by Their Request?

Although many MVAs have laws against providing false information to an MVA, it is a best practice to require data requesters to affirm through the application process that all information provided is truthful and accurate. MVAs should also require the requester to acknowledge by signature that use of the data for any purpose other than that stated in the application is prohibited by law and might subject the requester to civil or criminal sanctions. Similar language should be included at the data-sharing agreement stage.

Fees: Are They Going to Pay?

Another key part of the application analysis is whether to charge a fee to the data recipient who will obtain the data and in what amount. Some jurisdictions provide data for a fee to cover their costs, and others do not charge for the data.

When determining whether to set a fee, MVAs should consider their administration's priorities and budgetary situation, as well as any statutes that may set or control data fees. The DPPA explicitly states that it does not prohibit states from charging administrative fees for the issuance of motor vehicle records. The amount to charge may be set by state, provincial, or territorial statutes. When finalized, the fees for data should be made clear to requesters during the application process and memorialized in the data-sharing agreement.

4.4 Recommendations

- MVAs should develop a process for requesting MVA data, including one-time, ongoing, and bulk requests.
- At a minimum, the application requests the identity of the requesting individual or organization, any history of misuse or contract violations from previous data uses, the type of data requested, the purpose of the request, the volume and frequency of the requests, the requested method of data transfer, and security information.
- Establish an application review workflow among MVA offices or business areas that allows for consistent review and for minimizing risk of release of PII. Review of individual applications by business, legal, IT, and information security personnel is optimal.
- Create agreed-upon criteria to help identify which applications should be elevated for further scrutiny.

- Treat all similarly situated requesters consistently.
- Requesters should state what permissible use(s) they have for receiving PII.
- Requesters should state if they plan to re-release MVA data or PII.
- Requesters should specify how often they want to receive data.
- Requesters should specify, when providing data to an MVA, what portion of the submitted record may include trade secrets or data that if disclosed would put the requester at a competitive disadvantage.

Chapter 5 Data-Sharing Agreements

5.1 Introduction

A data-sharing agreement is a written contract between two entities that typically specifies what and how data will be shared, procedures to safeguard data, and authorized use. Although the term "data-sharing agreement" is referenced in this section, jurisdictions might use several alternative terms to refer to these documents (e.g., contract, memorandum of understanding, interagency agreement, data-security agreement, information-sharing plan, memorandum of agreement).

Before any data is shared, both the provider and receiver should meet to discuss data-sharing and data-use issues. For jurisdictions, a data-sharing agreement serves several purposes. First, it protects the MVA providing the data and the individuals to whom the data pertains, helping to ensure that the data will not be used in an unauthorized manner. Second, it prevents miscommunication by resolving any ambiguities about the data-sharing relationship. Data-sharing agreements also hold the data recipient accountable and clearly outline data security requirements.

5.2 Pre-approval Standards

DPPA allows resale or redisclosure of personal information by an authorized recipient if the redisclosure is also for a permitted purpose. It is the MVA's responsibility to know the ultimate end user and intended use of its data to ensure the data is redisclosed for a permissible use per the terms of the data sharing agreement. The audit process should be used to verify that subrecipients have a permissible use to receive PII or protected MVA data. MVAs should set parameters for resale or redisclosure by data-sharing agreement.

It is the MVA's responsibility to know the ultimate end user and intended use of its data to ensure the data are redisclosed for a permissible use per the terms of the data sharing agreement. The audit process should be used to verify that subrecipients have a permissible use to receive PII or protected MVA data.

MVAs should implement a pre-approval process similar to the analysis of the initial request for subrecipients and prohibit release of MVA data prior to approval. MVAs should document the subrecipient approval process in the data-sharing agreement. For example, a subrecipient approval process might include a one-time affidavit identifying the subrecipient's information and permissible uses. As an alternative, MVAs might choose to require annual or semiannual reporting by data recipients to disclose subrecipients and end users to whom MVA data were released for a designated period. In certain cases, such as vehicle recalls and class action suits, MVAs might wish to waive pre-approval and ask for a quarterly list of subrecipients receiving data after the data have been released. MVAs might consider requiring each subrecipient identified by a data recipient to sign an acknowledgement of permissible uses and security procedures for access to MVA records.

5.3 Importance of Data-Sharing Agreements

The data-sharing agreement should outline all rights, duties, and responsibilities of the contract parties. The data-sharing agreement should cover the basics (who the parties are and what data are being disclosed), as well as the details of the agreement (how the data will be transmitted and protected, what the data can be used for).

MVAs should decide if their data-sharing agreements are subject to negotiation and, if so, which provisions are negotiable. Some jurisdictions may prefer that data-sharing agreements stay uniform, but circumstances might dictate flexibility in certain instances. Either way, it is important for both parties to communicate expectations before, during, and after the data-sharing agreement is executed. If, for example, an MVA is changing the terms of its standard data-sharing agreement, it should provide notice to any data recipients that the change would impact.

The process for setting up data-sharing agreements might vary between MVAs, depending on the MVA and legal requirements. MVAs should use the steps in this section as a best practices guide when developing data-sharing agreements. The following is a list of items typically found in a data-sharing agreement:

- Definition of the parties and signors
- Introduction explaining purpose and authority (a list of "whereases")
- Confidentiality and privacy provisions
- Definition of permitted uses, including release to subrecipients, if allowed
- Definition of the data and the data exchange (how and how often)
- Data retention provisions
- Term, renewal, and termination provisions
- IT security provisions
  - Protecting data in transit and at rest (storage)
  - Approved and unapproved devices
- Reservation of audit rights
- Definition of incident response plan
- Data license and ownership
- Notice of unauthorized use and data leakage
- Statement of governing law
- Indemnification and liability
- Definition of payment terms, if any
- Breach and cure provisions
- Training expectations
- Assignment, merger, and business changes
- Clauses about reducing data modifications or comingling clauses to writing
- Any applicable addendums

REMINDER CHECKLIST

- ✓ Check the data recipient's stated use against DPPA/state law.
- ✓ Check to ensure the MVA is releasing minimum amount of data for stated use.
- ✓ Verify the identity and use of any subrecipient.
- ✓ Ensure fewest number of people at the data recipient have access.
- ✓ Ensure the MVA is following proper data-sharing agreement review and approval process, including review by legal, IT, IT security, and executive or business departments.
- ✓ Ensure the MVA has researched the history of the data recipient prior to signing the data-sharing agreement.

Although this list covers basic steps, additional concerns might arise based on the particular data set or MVA. Ideally, the MVA should address any added concerns in the data-sharing agreement to facilitate clear communication and, if needed, establish additional safeguards.

5.4 Sections of the Agreement

Who Are the Parties?

When considering the type of data-sharing agreement, consider the type of entities receiving the data. A data-sharing agreement with another jurisdictional MVA might have different provisions than a data-sharing agreement with a private, for-profit company. However, no matter who the parties are, all data-sharing agreements should contain some of the same basic elements.

What's Being Shared?

A data-sharing agreement can also vary greatly based on the type of information being shared. MVAs need to determine the classification of the data, which will lead to the level of protection needed in the agreement. An agreement to share highly sensitive PII, such as SSNs, should include heightened security measures compared with a data-sharing agreement to share just vehicle information. MVAs should clearly state these requirements in the data-sharing agreement.

The principle of data minimization is also important to remember. Keep in mind the data recipient's stated purpose for needing the data and work to minimize dissemination of the information. Only disclose the minimum amount of information sufficient to accomplish the stated goals of the data-sharing agreement.

Terms of Agreement

- Clearly state the expiration date or term of the data-sharing agreement.
- Consider the data-sharing agreement terms of no longer than five years, inclusive of any renewal periods, to ensure the data-sharing relationship is revisited and examined.
- If the agreement is terminated, suspended, or expired, all user access should be immediately terminated or suspended.

Frequency of Data Transfer

- Clearly define when the MVA will provide the data to the data recipient.

Data Ownership

- Clearly state in the data-sharing agreement that the data, even after the data have been disclosed to the requester, belong to the MVA. Retaining ownership rights of the data is critical to ensure that the requester understands that the requester is only granted temporary access to the data for a specific purpose.
- Data recipients might take the data that an MVA discloses and rearrange or repackage data in a different format. For example, a bulk data company might utilize MVA data to create software for car dealerships to be able to run more complex sales analyses. However, repackaging data does not transfer ownership to any data recipient or subrecipient.
- If the data recipient generates a report based on the data, then the report itself might belong to the data recipient, but the underlying source data should remain under the MVA's control.

Permitted Uses

The data-sharing agreement should include intended use of the data:

- Clearly state permissible use of the data. Copy the permitted uses directly from statute. Using statutory language helps to ensure legal compliance and that the data recipient knows the limitations of data use.

- State what functions the data recipient will perform with the data. Although statutory permissible uses may be general, the agreement should be specific to the use of the data.
- Prohibit the data recipient from using data to perform additional tasks without the approval or consent of the state MVA.
- Require regular or recurring reports to understand where the data are going and for what purpose upon MVA approval of subrecipient disclosure.
- Require any data recipient generating a secondary product based on the MVA data to include a disclaimer stating the secondary product was created using MVA data and that the MVA did not verify or authorize its creation.
- Require authorization from an MVA before the data recipient shares, publishes, or disseminates data findings and reports. After a particular publication is authorized, it does not need to be reauthorized for use by the same data recipient unless the nature of the request changes or additional or new data are included.
- Prohibit modification of source data by data recipients. It is the MVA's responsibility to ensure that data-sharing agreements do not interfere with or threaten the accuracy of driver and motor vehicle data.

Methods of Data Sharing

How data is shared is an important technology and security-driven decision. Decisions should be in writing in the data-sharing agreement.

- Identify how the data will be transferred from the MVA to the data recipient.
- If data is sent electronically, help to ensure that data is encrypted or otherwise protected during transit.
- If digital data is sent physically, help to ensure that media (e.g., DVD, USB drive) is encrypted or password protected.

Financial Costs of Data Sharing

Costs for compiling records or data may be established by statute or regulation. Considerations for costs include:

- A detailed fee structure, including data and administrative costs. Fees may be prescribed by statute.
- Determining whether the MVA and the data recipient will share costs or if the recipient will pay for all expenses.

Security – How Are Data Being Shared and Protected?

Outline security provisions clearly in the data-sharing agreement. They should include:

- Access should be restricted to the least number of necessary users at an organization.
- Access to users should only be granted while a data-sharing agreement is in place.
- MVA source data should be uniquely stored so it can be destroyed within agreed-upon time frame.
- Subrecipients may not retain MVA source data unless required by federal law or regulation or, when permitted by an MVA, in writing.
- Data-sharing agreements should address the process or requirements for destruction or returning data upon termination of the agreement. A destruction certificate of source data might be required.
- Electronic data destruction should be done using appropriate data-deletion methods to ensure the data cannot be recovered. Please note that simple deletion of the data is not effective. Often, when a data file is deleted, only the reference to

that file is removed from the media. The actual file data remain on the disk or cloud and are available for recovery until overwritten.

- The agreement should outline its data security requirements. The agreement could list specific requirements (e.g., minimum password length and complexity) or refer to standards for security and adequate data protection methods, including:
  - Methods that the data recipient should use to maintain data security.
  - Data recipients should keep hard copies of data in a locked cabinet or room, and electronic copies of data should be password protected or kept on a secure disk.
- Determine who among data recipient staff will have the same or different levels of access to data. This includes determining physical access to data, servers, and paper files.
- Determine what password protections should be in place.
- Determine disposition plans for data after the data-sharing period ends.
- Specify any penetration testing or forensic testing requirements needed to determine what data protection vulnerabilities may exist.
- Specify that data recipients should comply with all MVA IT security policies.
- Data recipients using a cloud-computing environment ensure data are kept within the jurisdiction's country boundaries (i.e., not stored "off-shore").
- MVAs may require annual (or other agreed-upon frequency) penetration testing or vulnerability scan. Such testing is conducted by a third party.

Data Integrity

As a matter of policy, MVAs may choose to restrict data recipient development or use of automated interfaces or other extraction or manipulation of data without written permission. However, if an MVA chooses to allow data recipients to generate its own data product from MVA source data, data recipients should be required to maintain an audit trail documenting how the data were manipulated. MVAs should ensure every event is associated with the unique identifier (ID) for the individual data recipient and is logged and time stamped.

Data-sharing agreements should require data recipients to include disclaimers about comingling MVA data in any secondary products. The disclaimer should state, despite the appearance of MVA data in a report, publication, abstract, or other resource made available by the data recipient, that MVA data are owned by the MVA and that the official and most up-to-date data record is in the custody of the MVA from which the information came. The following is a sample disclaimer used by Pennsylvania Driver and Vehicle Information Services for comingling in secondary products: "The Data Processor shall include the following language in secondary products developed from DRI (driver record information): This [product] was developed using data provided by the Commonwealth of Pennsylvania. This is a secondary product and has not been verified or authorized by the Commonwealth of Pennsylvania."

If an MVA chooses to allow authorized data recipients to make record changes (e.g., online dealers), then permission should be governed by a separate data-sharing agreement outside the use agreement context.

Performance Security

For the term of the data-sharing agreement, the data recipient should obtain and maintain a bond or escrow account for the MVA's benefit. A suggested amount is 10% of the annual payments due to the MVA from

the data recipient under the agreement. Regardless of the bond amount, it should renew each year on the anniversary of its issuance.

As a suggested best practice, the data recipient should submit for MVA review at least 15 calendar days before the bond renewal date an estimated annual payment amount for the coming year based on the amount of MVA data received by the data recipient. The 15-day period allows the MVA and the data recipient to finalize the amount for the coming year.

Cyber Insurance or Cyber Privacy Insurance

MVAs may require data recipients to obtain cybersecurity or cyber privacy insurance with specified minimum coverage for separate, per-instance and aggregate usage based on MVA-determined risk criteria (large bulk data containing PII). MVAs should be named as additional insured. Cyber insurance is separate and in addition to a general liability policy or umbrella policy.

Indemnification and Liability Section

The improper use of MVA data by the data recipient or subrecipients can cause harm to the data subject and economic loss for the MVA. When a driver or vehicle owner's data are misplaced, misused, or otherwise exposed, they often try to recover any damages they may have suffered from the MVA. Because of this possibility, clauses requiring full and complete indemnification of the MVA for any loss by the data recipient and from any claim by a third party is a recommended best practice.

Indemnification clauses in an agreement are a way for one party to protect itself against damages caused by another party's failure to comply with all contractual obligations. MVAs may consider including in the data-sharing agreement provisions mandating that the data recipient will reimburse the MVA for all economic losses resulting from a data recipient's breach of the agreement or a subrecipient's misuse or breach. Such losses may include lost MVA resources, causes of action filed by the data subject, attorney's fees, and so on.

When entering into a data-sharing agreement with another governmental entity, the MVA may wish to review the jurisdiction's controlling authority relating to sovereign immunity. Jurisdictions may have laws that limit the amount of liability a government entity is able to accept or impose on another.

Records Destruction or Disposition

MVAs should establish records retention and disposition clauses in the data-sharing agreement. When drafting the agreements, it may be difficult to accurately predict the appropriate retention and destruction period in advance. In these cases, MVAs and data recipients may wish to consider establishing a period for retention and destruction of the PII and then modifying the written agreement, if needed, to postpone the destruction date or move it sooner than initially specified. Although the time frame is within the MVA's discretion, the MVA should consider several factors before identifying a retention period.

The MVAs should also consider the type of data being released and the permissible use for which the data recipient is entitled to the information. As an example, if the data recipient is permitted to use driver information for employment or insurance purposes in a manner that implicates the FCRA, the MVA may consider the retention periods imposed within that law. The MVA should require the data recipient to disclose whether the data will be redisclosed. If so, the MVA's data-sharing agreement should specify the retention period for the end user of the data. Although lesser-protected data, such as vehicle information, might not be as sensitive, the record should be retained only for the length of time needed to satisfy the purpose for the release.

The data-sharing agreement should cover the following best practices:

- Include provisions that specify all PII that was provided to the data recipient should be destroyed when no longer needed for the specific

purpose for which it was provided, including any copies of the PII that might reside in system backups, temporary files, or other storage media.

- Address any prohibition of MVA data being manipulated or transferred into another database. In addition, specify that data collected for one purpose cannot be repurposed without further consent.
- Ensure accountability for destruction of PII by using certification forms containing detailed information about the destruction and signed by the individual responsible for performing the destruction.
- Address the distinction between data recipients who receive data from MVAs versus data recipients who have direct access to an MVA system. For data recipients who receive data files, identify the retention period and how it should be destroyed. For data recipients who have real-time access to a system, retention and destruction rules might include screen lock-out time periods, prohibiting printing screenshots, or other methods to secure MVA data in addition to the requirements.
- Specify retention periods both for the data itself and the use logs relating to the data recipient's permissible use. MVAs might wish to impose longer retention periods for records relating to how the data were used and the permissible purpose for which the data were obtained for audit purposes. A state or province might have disclosure laws that require the MVA to be able to disclose access to customer records for a set period.

Right to Audit

MVAs should retain the right to audit the data recipient in a way that allows the MVA to assess compliance with data-sharing agreement requirements. The right to audit subrecipients should also be included or considered.

Managing Data-Sharing Agreements After Signing

Certain events or changes may impact an active or executed data-sharing agreement. In the data-sharing agreement, the MVA should discuss and account for the following factors:

- Merger and acquisition – typically would require an assignment to the new entity responsible for the duties and obligations of the data recipient at the option of the MVA
- New laws passed – typically would require an amendment
- Fee change – sometimes the MVA has built-in rights to adjust fees to cover costs upon notice to the data recipient
- Data recipient goes out of business or changes business – the MVA should have a termination rights in these scenarios
- Change the permissible use or add a new use – upon request by the data recipient or upon notice by the MVA; typically requires an amendment
- Changes to security requirements – should be at the MVA's discretion

These factors might require action by the MVA or data recipients during or after the term of the data-sharing agreement. The agreement should allow for modification to the terms of the agreement.

Breach of the Data-Sharing Agreement

Specific breach circumstances should be addressed in the data-sharing agreement and are typically tied to a notice of breach and opportunity to cure. However, certain serious breaches should give rise to an automatic termination right for the MVA. MVAs should consider the range of sanctions for material or nonmaterial breach and articulate them in the agreement.

Data Breach (Unauthorized Use, Disclosure of, or Access) Notification

Data breaches are subject to state, provincial, and territorial notification laws. Data recipients must understand the legal requirements for the breach notification, roles, timing, manner of report, parties to whom a report or notification must be made, and cooperation with LEAs, among other considerations.

Data recipients should implement appropriate measures to protect against the unauthorized release of MVA records. Data recipients and subrecipients should be required to notify the MVA if data security has been compromised and should coordinate with MVAs in response to unauthorized use, disclosure, or access.

5.5 Recommendations

- Define the parameters for redisclosure, including recording every redisclosure and the permitted use for such redisclosure.
- Before any data are shared, both the provider and receiver should meet to discuss data-sharing and data-use issues.
- MVAs should implement a pre-approval process similar to the analysis of the initial request for subrecipients and prohibit release of MVA data prior to approval.
- It is important for both parties to communicate expectations before, during, and after the data-sharing agreement is executed.
- Practice the concept of data minimization and share only what is needed. MVAs can restrict how much data to share beyond the permissible uses in the contract.
- Prohibit modification of source data by data recipients.
- Capture, in writing, the method or means by which data are shared with a recipient.
- Outline security provisions clearly in the data-sharing agreement.
- If MVA data are manipulated or otherwise reconfigured, data recipients should be required to maintain an audit trail documenting how the data were manipulated.
- Data-sharing agreements should require data recipients to include disclaimers about comingling of MVA data on any secondary products.
- Data recipient should obtain and maintain a bond or escrow account for MVA's benefit in the amount of 10% of the annual payments due to MVA from the data recipient under the agreement.
- As a suggested best practice, the data recipient should submit for MVA review at least 15 calendar days before the bond renewal date an estimated annual payment amount for the coming year based on the amount of MVA data received by the data recipient.
- Consider a cybersecurity or cyber privacy insurance requirement.
- Data recipients should indemnify MVAs for losses arising out of unauthorized disclosure of PII by the data recipient or from a claim by a third party.
- MVAs should retain the right to audit the data recipient in a way that allows the MVA to assess compliance with data-sharing agreement requirements.
- Establish records retention and disposition clauses in the data-sharing agreement.
- Data recipients and subrecipients should be required to notify the MVA if data security has been compromised and should coordinate with MVAs in response to unauthorized use, disclosure, or access.
- Adopt procedures to address instances of noncompliance with data-sharing agreements.

Chapter 6 Response to Unauthorized Use, Disclosure of, or Access to MVA Data

6.1 Introduction

Unauthorized use, disclosure of, or access to MVA data can have wide-ranging impacts: loss of trust, financial penalties, and consumption of MVA resources to remediate. MVAs are often required by law to report data breaches, or what is referred to in this best practice as "unauthorized access" or "unauthorized use." Laws and cybersecurity policy govern the required response to unauthorized use of or access to MVA data. Jurisdictions should start with jurisdictional law when attempting to determine if an incident is reportable.

Each MVA should, or in some instances is required to, create and maintain an incident management plan. The plan provides a formal structure to respond to unauthorized use, access, and disclosure of MVA data. The incident management plan should include but not be limited to:

- Procedures for incident investigation
- Procedures for reporting and managing incidents
- Plans for mobilizing staff to respond to incidents
- Application of lessons learned from prior incidents*

Response to unauthorized use of MVA data is not only a responsibility of the MVA but also of data recipients. Recommended action by data recipients in response to unauthorized use, disclosure of, or access to MVA data are also listed in this section.

6.2 What Are Unauthorized Use, Disclosure of, and Unauthorized Access to MVA Data?

Unauthorized use is use of MVA data for a purpose other than the permissible purpose for which the access was granted. The original access to the data may have been proper, but the subsequent use is not permitted. Unauthorized access means gaining access to MVA data without authority. Unauthorized disclosure occurs when an individual with access to MVA data discloses the data to another individual(s) without authority.

Unauthorized access, disclosure of, or access to MVA data may be intentional or unintentional. Unintentional instances may arise from lack of training, internal controls, or safeguards. Intentional instances might be malicious or simply a misunderstanding of permissible use.

Unauthorized access and subsequent use by an external source is often called a "data breach." A breach or unauthorized use in this instance may be accomplished maliciously by an external actor (e.g., hacking) or from an insider threat. An "incident" is an occurrence that actually or potentially jeopardizes the confidentiality, integrity,† or availability of an information system or availability of the information the system processes, stores, or transmits. An incident may also be a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

* State of California, California Department of Technology, Office of Information Security, Incident Reporting and Response Instructions, SIMM 5340-A, January 2018, available from https://cdt.ca.gov/wp-content/uploads/2018/01/SIMM-5340-A_2018-0108.pdf

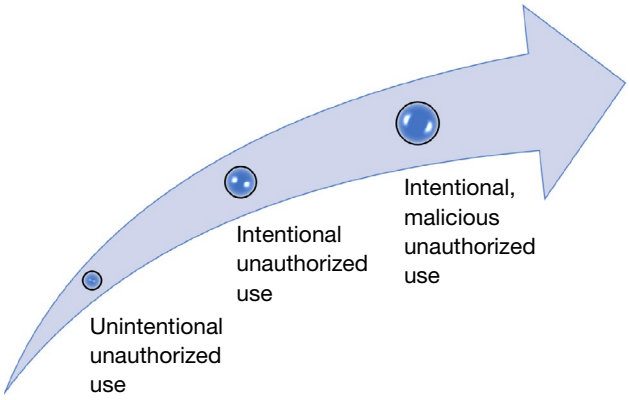
† Incident Reporting and Response Instructions, page 1.

Incident Severity

At the lowest end of the spectrum of severity is unintentional unauthorized use. This is when a person or organization inadvertently uses data for other than their intended purpose. This may be discovered during an audit or internally by a supervisor reviewing employee work performance. If there is no malicious intent and the unauthorized use resulted in little to no data compromise, education is an appropriate remedy, and it may not rise to a level requiring official reporting per state statute or policy.

Next in severity is intentional unauthorized use that does not rise to the level of malicious unauthorized use. This is when data are used for other than their intended purpose but is lacking malicious intent. For example, a data recipient may receive a list of vehicle registrations with physical mailing addresses for purpose of recall notification by regular mail. The list provided also includes vehicle registrant email addresses. After making the recall notification by regular mail, the data recipient then sends a non-recall marketing or other communication to the list of registrant emails. This is an example of intentional unauthorized use. This may be the result of an organizational process not providing strong enough guidance to its employees (in the case of MVA staff or data recipient staff) or a blatant disregard for permissible use as defined in their data-sharing agreement with the MVA (data recipient). Appropriate remedies to this type of unauthorized use may be education, disciplinary proceedings, enhanced monitoring, audit compliance findings, or even termination of the data-sharing agreement if the unauthorized use continues.

Finally, the highest severity is intentional, malicious unauthorized use. This may be internal or external but is defined by the malicious intent behind the unauthorized use. This includes data breaches in which external entities access data for financial or political gain. There are many examples of high-profile breaches of corporate or government data. For instance, the retail store Target paid an $18.5 million dollar fine after a malicious cyberattack that affected the data of more than 41 million customers.*



Unauthorized Use, Disclosure, or Access at an MVA

BEING PREPARED: ESTABLISH AN INCIDENT OR UNAUTHORIZED USE RESPONSE PLAN.

MVAs should create and keep current an incident response plan. Addressing these items prior to an unauthorized use, disclosure, or access incident helps MVAs efficiently and quickly detect and mitigate unauthorized data uses. The plan should be based on guidance from entities such as the U.S. Department of Education,† the Federal Trade Commission,‡ the California Department of Technology,§ or other reputable sources and should include guidance on the following:

- Identify the incident response team, along with a team manager who will be in charge of the incident response (with at least one other person designated to assume authority in the absence of the manager). Assign and establish team roles

* Kevin McCoy, "Target to pay $18.5M for 2013 data breach that affected 41 million consumers," May 23, 2017, USA Today, available from https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

† U.S. Department of Education, Privacy Technical Assistance Center and the Student Privacy Policy Office, "Data Breach Response Checklist," available from https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

‡ Federal Trade Commission, "Data Breach Response: A Guide for Business," May 2019, available from https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

§ State of California, California Department of Technology, Office of Information Security, "Incident Reporting and Response Instructions," January 2018, available from https://cdt.ca.gov/wp-content/uploads/2018/01/SIMM-5340-A_2018-0108.pdf

and responsibilities, along with specifying access credentials.

- Address response goals, strategy, and requirements.
- Assign and establishing team roles and responsibilities, along with specifying access credentials.
- Establish employee response expectations in conjunction with Human Resources.
- Conduct regular reviews of the policy to include any necessary improvements and ensure that it reflects up-to-date federal and jurisdictional requirements.
- Conduct frequent privacy and security awareness trainings as part of an ongoing training and awareness program.

Response to Unauthorized Use, Disclosure, or Access

If unauthorized use, disclosure, or access occurs, the incident response team and the MVA should execute the incident response plan. Key steps in incident response include:

- Activate the incident response team. This includes activating a communication plan that is both internal and external. Assemble a team of experts to conduct a comprehensive unauthorized use response. Forensic data experts may be part of the response.
- Preserve evidence (backups, images, hardware, and so on) for later forensic examination. Some best practices for the collection and handling of digital evidence can be found in the Personnel/ Resources chapter. Locate, obtain, and preserve (when possible) all written and electronic logs and records applicable to the unauthorized use for examination. Establish a chain of custody for preserved evidence.
- Interview people who discovered the unauthorized use.
- Validate unauthorized use. MVAs need to determine and verify that data were disclosed or used in an unauthorized manner, how severe the incident was, and how to work with law enforcement if there is evidence of criminal activity.
- Determine the scope and composition of the unauthorized use. Plans should include steps to identify all affected data, machines, and devices and document facts.
- Determine whether notification of affected individuals is appropriate or required and, if so, when and how to provide such notification. Determine whether notification is warranted and when it should be made. Notification decisions should be elevated to executive leadership at the senior technical or administrative level in coordination with legal counsel.
- Specifying incident-handling procedures, strategies for deciding on the course of action in a given situation, and procedures for communicating with organizational leadership and outside parties and law enforcement. Incident handling procedures may include:
  - Controlling access to information systems or physical location of records and data immediately after an incident
  - Stopping additional data loss by removing affected equipment or access to them
  - Updating credentials to existing systems because those with unauthorized access may still have passwords
- A list of potential notifications, including:
  - Affected individuals, parties, businesses, and the public: MVAs should have a policy on

how customers will be informed and what actions they will need to take to protect themselves (refer to this guide for Disclosure Notification). Nearly all states and provinces have legal requirements to notify the public and those who are affected by unauthorized access.

  - Law enforcement. The sooner law enforcement learns about the theft, the more effective they can be. Consult with law enforcement contacts about the timing of the notification so as not to impede the investigation.
  - Major credit bureaus if MVA data that could be used to impersonate someone have been accessed and used

- Implement lessons learned from prior incidents and evaluate the effectiveness of these remediations.

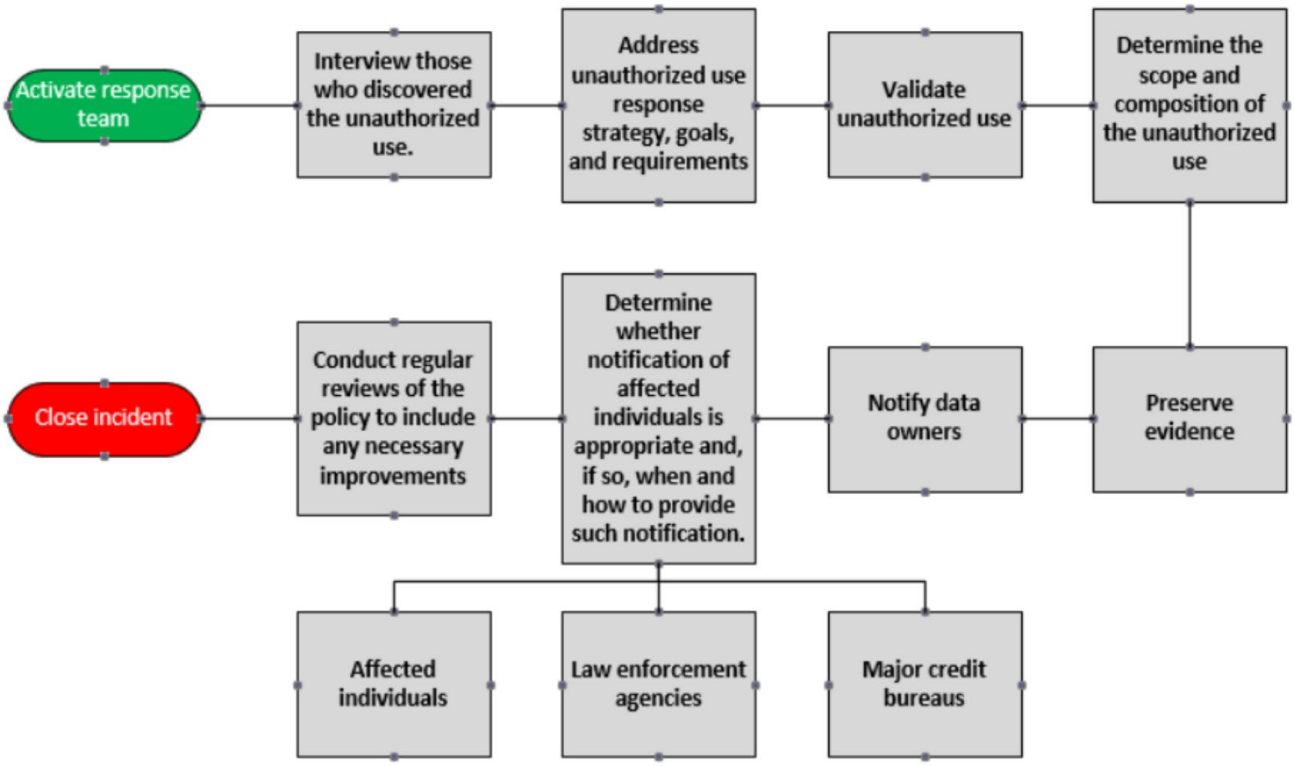
The following chart illustrates the team preparation and response approach defined.

Please refer to the Federal Trade Commission's publication "Data Breach Response: A Guide for Business" from May 2019 and updated from time to time, for additional details of how to respond to a breach or unauthorized access of MVA data.

MVAs can reduce their risk of unauthorized use, disclosure, or access to MVA data by following the guidance in the following list. This list is not exhaustive and should only be used as a general guide that is meant to be tailored to each MVA's unique operational security needs.

- **Identify or plan for where the threat may come from.** Even with laws and policies in place, the potential for unauthorized use of MVA data is growing. The most common perpetrators include third-party contractors and insider threats.

  Although organizations focus significant resources on the mitigation of external threat actors, insider risks are likely to pose an even greater threat to the MVA. According



to the Ponemon Institute's "2018 Cost of Insider Threats" report, the average cost of insider-caused incidents was $8.76 million in 2017—more than twice the $3.86 million global average cost of all unauthorized uses during the same year.* That figure rose to more than $11 million in 2020.† Insider threats may come from those who fail to follow training, policy, or guidance on the importance of protecting data or how to protect data; those who are negligent or careless about protecting MVA data; collusion or those with criminal intent; or those who are disgruntled.‡ §

Adequate controls help reduce the likelihood of insider threat. Proactively monitoring use of information systems can alert an MVA to possible unauthorized use before it happens. Software tools, including artificial intelligence, can alert an MVA to possible risk.

- **Categorize, classify, and inventory assets.** MVAs should conduct an inventory of all data assets. It is especially important to understand what compliance standards exist as provided by law (e.g., the DPPA), where they are stored (including backup storage and archived data), and how they are kept secure. MVAs should discover and classify at-risk assets. Data classification is a key part of data governance and protecting data from vulnerabilities.¶
- **Continuously monitor for PII and other sensitive data leakage and loss.** This includes using automated tools, such as intrusion detection and prevention systems, next-generation firewalls, and antivirus and anti-malware tools, to monitor and alert about suspicious or anomalous activity.
- **Keep security protocols up to date.** Continuous monitoring of security, as described in the Security section and the Impact and Risk Mitigation section, is crucial. MVAs need to keep security policy up to date, run the most recent software on all systems, and keep patching efforts current.
- **Establish controls.** MVAs should establish internal controls to reduce the likelihood of internal unauthorized use. MVAs may also rely on privately contracted SOC audits to identify controls or that prevent unauthorized use of MVA data. Establish separation of staff duties to reduce the likelihood of one person having too much access to data.
- **Review and keep accurate data destruction policies.** Consistent with records retention guidelines, data destruction policies should be established and reviewed regularly, and staff should be aware of these polices. Removal of data that are beyond the retention period is a key part of data and records hygiene that limits data that can be exposed.
- **Conduct regular risk assessments.** MVAs should plan for and conduct regular assessment of risk. See the Impact and Risk Mitigation section.
- **Conduct frequent education and outreach.** MVAs should provide mandatory information security training for MVA staff who handle PII. Penalties for unauthorized use, disclosure, and access should be provided to all MVA staff. The reporting process for suspected violations should be plain and easy to follow.**

* Ponemon Institute, "2018 Cost of Insider Threats: Global," April 2018, page 2.

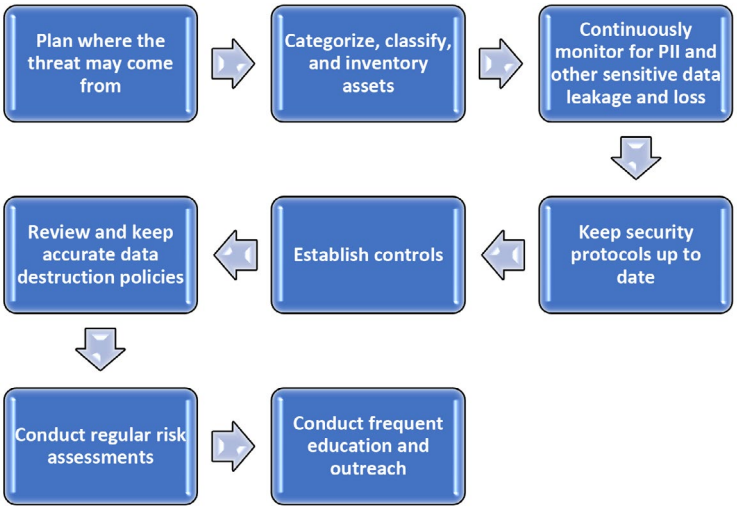
† Ponemon Institute,"2020 Cost of Insider Threats Global Report," available from https://www.observeit.com/cost-of-insider-threats/

‡ Media Sonar, "Fixing the Insider Threat Investigation Gap," October 2019, available from https://mediasonar.com/2019/10/10/insider-threat-intelligence/

§ Jasmine Henry, Security Intelligence, "These 5 Types of Insider Threats Could Lead to Costly Data Breaches," August 2018, available from https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

¶ *ibid.*

** Privacy Technical Assistance Center, "Data Breach Response Checklist," available from https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf



The above chart illustrates the prior steps in flow chart form.

External

Data recipients are subject to unauthorized use, disclosure, and access laws. MVAs should be aware of jurisdictional laws regarding breaches and should include clauses in data-sharing agreements that make data recipients aware they are subject to public laws. Specific actions required of data recipients may include:

- Reporting the unauthorized access without delay
- Providing details of the unauthorized disclosure and providing updates (e.g., new numbers of disclosures or persons affected)
- Assisting in remediation and cooperate on public disclosure or awareness
- Conducting or cooperating with an investigation into the cause of the unauthorized disclosure. This could include paying for third-party resources acceptable to the MVA to determine the cause and extent of the disclosure and a list of actionable recommendations.
- Providing written notice to the individuals whose PII was impacted by the unauthorized access or reimburse MVA for costs incurred providing notice, including costs for mailing notices
- Offering credit monitoring services or credit freeze for a specified period or identity theft insurance and credit freezes to affected parties at the data recipient's expense
- Paying for costs of notifications and investigations associated with unauthorized use, disclosure, or access
- Providing a mechanism to respond to inquiries from affected parties about the unauthorized disclosure, such as a dedicated call center
- Subject to data-sharing agreement terms, data recipients should coordinate with MVAs in response to an unauthorized use, disclosure, or access

6.3 Recommendations

- Jurisdictions should start with jurisdictional laws when assessing whether an incident is reportable and promptly report incidents in accordance with the notification requirements in their jurisdictions.
- MVAs should create and keep current an incident response plan.
- Incident response plans should include prompt investigation of incidents involving loss, damage, or misuse of information assets.

Chapter 7 Compliance and Audit (People and Organization)

7.1 Introduction

Audit is defined as the verification activity, such as an inspection or examination, of a process or quality system, to ensure compliance to a set of defined requirements. An audit promotes accountability and efficiency within an organization. Financial, operational, performance, compliance, IT, and data integrity are some of the types of audits that MVAs perform. Data integrity or compliance audits assess an organization's processing or handling of personal data using Generally Accepted Government Auditing Standards (GAGAS) and other best practices. This includes, but is not limited to, compliance with the requirements of data privacy protection laws and regulations.

Compliance encompasses a broader range of responsibilities. Compliance activities and processes should consider how an MVA or a data recipient applies internal controls to protect against loss or exposure of PII. Its function is to provide operational, legal, or regulatory recommendations to MVAs and data recipients. In contrast, the audit function focuses on point-in-time review or assessment and related findings of organizational activities. Point-in-time reviews may be a singular instance or may be conducted at recurring intervals or at specific periods of performance. In summary, compliance is an operational function of an entity. It exists to manage risk. Audit is a more focused business assurance function.

7.2 Audit Purpose

A compliance and audit program typically oversees an organization's internal controls, governance, systems, records, and activities to

- Ensure that appropriate policies and procedures are in place.
- Verify that these policies and procedures are being followed by both the organization's personnel and by data recipients.
- Test the adequacy of controls in place.
- Detect unauthorized uses or potential unauthorized uses.
- Identify risks and recommend areas that need improvement and how to implement the proper changes and adjustments.

7.3 Audit Benefits

Audits enforce data protection requirements. Audits identify and control risks, preventing unauthorized use of personal data. The benefits of an audit include

- Helping to raise awareness of data privacy and protection, general information security, and cybersecurity
- Promoting transparency and accountability
- Showing the MVA's commitment to and recognition of the importance of data privacy and protection of an individual's right to privacy
- Independent assurance of data protection policies and practices

- Assessing risks, economy, efficiency, and quality
- Identifying data protection risks and development of practical, realistic, organizational-specific recommendations to address them
- Preventing fraud, waste, and abuse
- Providing an opportunity for the MVA to provide training and guidance to data recipients on best practices for handling sensitive data
- Assessing controls to ensure their proper application
- Ensuring compliance with laws and regulations
- Verifying procedures are adequate, clear, and followed

Audits enforce data protection requirements. Audits identify and control risks, preventing unauthorized use of personal data.

7.4 Audit Method

The following are examples of common methods of conducting audits:

- **Desk audit** – A desk audit typically includes review of documents, evidence, records, or data from a remote setting, often the auditor's office. Desk audits are usually conducted remotely and review material either submitted by the subject of the audit or material already available to the auditor.
- **On-site audit** – An on-site audit is a verification of activity, such as inspection or examination, of a process or quality system, to ensure compliance to requirements.
- **Follow-up audit** – These are audits conducted after an internal or external audit report has been issued. They are designed to evaluate corrective action that has been taken on the audit findings from the original report. The purpose of a follow-up audit is to revisit a past audit's recommendations and management's action plans to determine if corrective actions were taken and are working or if situations have changed warranting different actions.

7.5 Audit Type

The following are types of audits an MVA will conduct:

- **Internal operational audit** – an independent, objective assurance and consulting activity designed to add value to and improve an MVA's operations. The objective of an operational audit is to determine whether the MVA has sufficient and appropriate internal controls to include the implementation of policies and procedures to regulate the processing or handling of personal data and whether that processing or handling is carried out in accordance with such policies and procedures.
- **External compliance audit** – an external compliance audit assesses the overall effectiveness of a data recipient's compliance practices and protocols. The auditor examines processes and transactions and should determine whether the item being examined complies with established standards. A compliance audit mainly focuses on whether the data recipient is complying with local laws, regulations, and related rules. A compliance audit also reviews
  - Whether the data recipient is complying with internal rules, regulations, policies, decisions, and procedures
  - Who accesses the data
  - Why data are needed

- The approval of data usage – ongoing ad hoc spot checking to verify proper and approved usage
- Prior compliance audit findings
- Audits conducted of subrecipients

- **IT audit** – The goal of an IT audit is to ascertain that IT systems are safeguarding assets, maintaining data integrity, and efficiently operating to achieve business objectives.

7.6 Monitoring Access to MVA Data

MVAs should actively monitor data recipients' use of access to MVA records. MVAs may take several steps to monitor use absent or in between formal audits.

Monitoring may be enhanced by data salting. Data salting is an information security or cryptographic practice of adding random characters, such as a password, to sensitive data to obscure the data or prevent it from being discovered. Salting is also used to trace data from its source to later determine where the data originated, like the way paper currency might be marked in a way known only to a select few.

MVAs should ensure there is a mechanism to review and track the use of each user-provided access to MVA records. In addition to being able to re-create which users accessed an individual's record, the MVA should be able to re-create what any individual user accessed the data. This allows the MVA to create reporting around regular review of data recipient access to identify any anomalies that could suggest unauthorized use. As an example, a spike in access, such as a data recipient who normally processes 6 transcripts a month jumping to 30 transcripts a month, may be flagged for follow-up upon review of regular reports. System-generated reports may include the data recipients' and subrecipients' account information, number of requests by day, each MVA record number, transaction identification number, and purpose code associated with each record request. MVAs may determine the frequency such reporting is needed based on request volume.

MVA data system user logs and identifications should be reviewed on a regular basis. Designated users and logon IDs should be updated at the time of data-sharing agreement renewal. Data recipients should be required to keep records of each access for a designated amount of time. The length of time may be set by the MVA's record retention schedules, statutory requirements, and the provisions of any data-sharing agreement but should be at a minimum the term of the data-sharing agreement plus any applicable statutory requirements for further retention. If asked, the data recipient should be able to provide the MVA with the name of the user for any individual access and the purpose for the access. MVAs may recommend that data recipients keep access logs to note anything they would have difficulty explaining (e.g., a record was accessed by mistake because of a typo). This requirement should be reconciled with the requirement that the data recipient not keep the actual data for longer than necessary to complete the permissible purpose for access. Data recipients are encouraged to keep access logs and justifications without maintaining the actual data themselves.

In addition to the MVA monitoring, data recipients may also be required to conduct internal monitoring of access to MVA data. MVAs should require data recipients to designate a representative at each organization with multiple users to be responsible for internally monitoring the use of the organization's employees with access to MVA records. The organization may not allow use by any outside entity of the access provided to MVA records and should have safeguards and active monitoring in place to protect against such access. MVAs should require the data recipient to notify the MVA immediately if any employee unauthorized use or misconduct is detected.

7.7 Recommendations

- MVAs should actively monitor data recipients' use of access to MVA records
- Create an audit finding database or matrix to track all audit findings, recommendations, and corrective action plans for auditees (data recipients and subrecipients). This database or matrix is used to trigger follow-up audits.
- MVAs should ensure there is a mechanism to review and track the use of each user-provided access to MVA records.
- MVA data system user logs and identifications should be reviewed on a regular basis.
- MVAs should require data recipients to designate a representative at each organization with multiple users to be responsible for internally monitoring the use of the organization's employees with access to MVA records.
- MVAs and their designated auditor should develop an annual audit plan.
- The areas that may be covered during an audit are
  - Unauthorized use or noncompliance with controlling laws and data-sharing agreements
  - Data protection or privacy governance and accountability
  - Security of personal data
  - Unauthorized transfer and access of personal data and data portability
  - Direct marketing
  - Information sharing
  - Records management
  - Data privacy and protection training for personnel

Chapter 8 Records Management

8.1 Introduction

Records management refers to a set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions. It is the practice or life cycle of intake, use, and disposition. A structured records management program allows an MVA to comply with laws, understand and execute defined business processes, and be accountable to the public and regulatory bodies. Effective records management allows an MVA to fulfill its mission, comply with legal requirements, and minimize risk.

8.2 Data Protection Techniques

Data Minimization

Data minimization can help guard against privacy-related risk. If a data recipient collects and retains a large amount of MVA data, there is an increased risk that the data will be used in a way contrary to stated permissible use. To minimize this risk, MVAs should examine a data recipient's data requests and business needs to develop practices that impose reasonable limits on the collection and retention of MVA data. Customer profiles should be set up to allow access to the least amount of data requested, needed, and authorized under any permissible use agreements.

MVAs should consider creating template profiles (e.g., a private investigator template, insurance template, or law enforcement template) that permit electronic access through an interface only to data fields needed to accomplish the stated purpose of the agreement. MVA should not "overshare" data and then limit scope or use by data-sharing agreement.

Redaction of records is an effective means to minimize sharing of data. Redaction of PII or other protected MVA data removes the need for a documented permissible use. MVAs should adopt processes for redacting PII or MVA data from requested records.

> *"Only disclose the minimum amount of information sufficient to accomplish the stated goals of the data-sharing agreement."* —**THERESA EGAN, Former Executive Deputy Commissioner, New York State Department of Motor Vehicles**

Data Anonymization

For PII that can reasonably be anonymized, MVAs should require the data recipient to do so before sharing with subrecipients who are not otherwise entitled to the data. This practice should be used to supplement data minimization practices, particularly in situations in which the data recipient is entitled to permissible uses beyond those of the subrecipient or end user. The MVA or the data recipient should remove PII so it cannot be used to identify an individual or relate the information back to an individual. The data recipient should prohibit the subrecipients from reidentifying data. For PII that cannot be completely anonymized, the data recipient must not redisclose it to a subrecipient.

Internal Records Management Practices

A records series is a group of records that allows for retrieval by a unique ID. Establishing a records series allows MVAs to understand what data are kept and from what business processes they were gathered.

Records management is a practice that keeps MVA records organized and builds accountability and transparency by stating what records are kept, for how long they are kept, and how, if there is a correction needed, that correction is made.

PRIVACY STATEMENT OR PRIVACY POLICY

For any data or PII that is collected, MVAs should publish a privacy statement or privacy policy. Privacy statements may be associated with all MVA records or be specific to each system of records created by an MVA. Privacy policies should be made readily accessible to both individuals and MVA staff. Individuals should be able to find the privacy statement or policy on the MVA website or when coming to an MVA office to conduct a transaction. Privacy policies should include the following:*

- What PII is collected
- Why it is collected
- What choice the individual has, if any, to comply with the request for PII (consent, or whether there is an opportunity to opt out)
- How PII is collected
- How long PII is kept
- What access the individual has to their PII or to how to determine what PII the MVA has
- Which data recipients the PII may be shared with (not each individual data recipient but which data recipients in general)
- What security is in place to protect PII
- What measures are taken to ensure data quality or accuracy (and relevance)
- How an individual may dispute or correct PII held by the MVA

* American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, 2009. "Generally Accepted Privacy Principles, CPA and CA Practitioner Version," available from https://iapp.org/media/presentations/11Summit/DeathofSASHO2.pdf

RECORDS INVENTORY AND ESTABLISHING A SYSTEM OF RECORDS

MVAs should develop systems of records to allow MVAs to better understand and categorize what data and PII they maintain. It also serves as a basis for privacy impact analyses that help determine the level of security and risk mitigation needed around a type of record or system of records.

INTERNAL RECORDS LIFE CYCLE

Although the retention period for records maintained by an MVA is set by the state or provincial public records laws, jurisdictions should implement protective measures to ensure records are maintained in a safe and secure manner from creation until destruction or final disposition.

Physical records should be maintained in a stable environment to ensure the records' continued existence, usability, and authenticity. Jurisdictions should implement measures for non-electronic records. Examples of physical records protection and preservation include considerations around temperature and humidity, fire protection, sunlight, laying records flat, and so on. Specifics may be found with state archivists.

Storing records in an electronic format poses additional challenges because of the changing nature of technology. Records might need to be converted or migrated to properly maintain them through the required retention period. Electronic records should be stored in a cool facility, not be handled excessively, stored on media that is protected from deterioration due to date of storage manufacture, and migrated to newer hardware or software as technology becomes unsupported or obsolete. Cloud-based storage is another option that is gaining traction and should be considered.

SPECIAL DATA TYPE CONSIDERATIONS

Jurisdictional laws might mandate that MVAs treat certain types of records or data with a higher level of

protection or by different procedures. Examples of such special data type considerations include crash reports, biometric data, SSNs, and photographs. MVAs should be aware of any such requirements to ensure that procedures exist to protect these special data types in data-sharing agreements.

DATA HYGIENE

MVAs should strive for an accurate record for each individual. MVAs should establish a process to periodically review data for accuracy, integrity, and destruction of records that have reached their statutory disposition date.

As with an information systems modernization effort, MVAs may need to adopt an initiative to conduct a periodic or one-time cleanse of data and then adopt new rules or measures to maintain data quality and integrity. Some initial steps, based on guidance in the AAMVA System Modernization Best Practice (published in 2017), include:

- Data profiling – the act of identifying issues and questions about MVA source data. Data stewards typically drive the data profiling effort, given their familiarity with the business processes that drive data collection. Data stewards should consult with MVA program staff to determine what data needs correction, where there are weaknesses in data entry points, and where databases could use standardization or data validation.
- Cleansing data – the process of evaluating source data for inconsistencies, errors, or inaccuracies. Data cleansing exercise can also add methods or data collection and entry rules to prevent against future degradation of data.
- Data masking – protecting specific, sensitive or personal data elements from disclosure or discovery using rules, algorithms, or other methods to protect MVA data. This is another method or strategy for data minimization and data anonymization.

REVIEW OF PERSONAL INFORMATION KEPT BY MVAS

Many jurisdictions have laws that allow individuals to request disclosure of their PII or personal data kept by the MVA. MVAs should be aware of their obligations and should have a publicly available process for requesting and correcting any inaccuracies in the data retained by the MVA.

RETENTION PERIODS AND RECORDS DISPOSAL

MVAs should consider how long the relevant record retention laws and policies require an individual piece of information to be held. As public entities, MVAs are subject to the record management laws of the individual jurisdiction. MVAs and data recipients (including other government entities) alike should understand how long data may or must be legally retained.

MVAs should destroy data according to statutory federal and jurisdictional retention schedules. For example, DPPA specifies a five-year retention period for personal information re-disclosure, and FCRA requires a 90-day retention period for records used to establish creditworthiness for the request and dispute process.

Timely disposition of records that contain data helps advance data minimization. Retaining these records only as long as required by law helps minimize the risk of data loss.

MVAs should review their individual security requirements in determining the methods by which data, especially data containing PII, should be destroyed. Considerations include

- Electronic media containing MVA data (hard drives, optical media, USB flash drives) should be sanitized (data are permanently removed or overwritten) or the media should be physically destroyed (shredded, incinerated, holes drilled though it, and so on) in accordance with the NIST SP 800-88 Guidelines for Media Sanitization.

- Paper records should be handled in a similar fashion to electronic data. When data are no longer required, destroy paper using secure means such as a cross-cut shredder, commercial shredding, or incineration.
- Consider the level of risk associated with the sensitivity of data being destroyed. If data are highly sensitive, their destruction may require MVA observation.
- Address in a timely manner the sanitization of storage media that might have failed and might need to be replaced under warranty or service contract. Many instances of unauthorized use of data result from storage media containing sensitive information being returned to the manufacturer for service or replacement.

External

Data recipients should maintain traceable records of what data are received from MVAs to allow for auditing and accountability. The following provisions provide guidance for data recipients about maintenance of systems of records containing MVA data.

DATA RECIPIENT CUSTODIAN OF RECORDS OF MVA DATA

Data recipients and subrecipients should designate a data custodian of MVA data. The data custodian should be responsible for maintaining records of MVA data receipt, access, and disposition. The data custodian should have responsibility for understanding MVA policies governing the use of MVA data, training of employees (where applicable), assistance with MVA external audits, and safeguarding of MVA data.

Record management requires maintaining a comprehensive record of relevant security documents, assessment, and decisions. This will increase operational efficiencies, improve services, support mission needs, and safeguard sensitive information. This will help MVAs to establish an ongoing due diligence process and monitoring plan.

CUSTOMER DATA RETENTION

MVAs should clearly identify the length of time the data recipient is permitted to retain MVA data. A general best practice is to require the data recipient to destroy, purge, or return MVA data after they have been used for their permitted use.

The FIPPs have been criticized as too reliant on timely notification and consent procedures that must be repeated each time PII is collected in a system of records. Individuals are regularly asked to read privacy policies and give consent if they want to complete an online transaction. Many click past the notice and cannot keep track of when they have provided consent.*

As a default best practice, the data recipient should destroy MVA data within 24 hours of when the data are no longer needed to meet the stated purpose and performance obligation articulated in the data-sharing agreement. Subrecipients should not retain redisclosed data unless required by federal law or regulation, or when permitted by MVAs in writing. If the data-sharing agreement permits use of a third-party records destruction service, data recipients should observe the destruction process and obtain a certificate of destruction of both paper and electronic records.

8.3 Recommendations

- MVAs should consider creating template profiles (e.g., a private investigator template, insurance template, or law enforcement template) that permit electronic access through an interface only to data fields needed to accomplish the stated purpose of the agreement.
- For any area that data or PII is collected, MVAs should publish a privacy statement or privacy policy.
- MVAs should develop systems of records to allow MVAs to better understand and categorize what data and PII they maintain.

* https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf

- Jurisdictions should implement protective measures to ensure records are maintained in a safe and secure manner from creation through destruction or final disposition.
- MVAs should establish a process to periodically review data for accuracy, integrity, and destruction of records that have reached their statutory disposition date.
- MVAs should be aware of their obligations and should have a publicly available process for requesting and correcting any inaccuracies in the data retained by the MVA.
- MVAs should destroy data according to statutory jurisdictional retention schedules.
- Data recipients should maintain traceable records of what data are received from MVAs to allow for auditing and accountability.
- Data recipients and subrecipients should designate a data custodian of MVA data.
- MVAs should clearly identify the length of time the data recipient is permitted to retain MVA data.
- As a default best practice, data recipients should destroy MVA data within 24 hours of when the data are no longer needed to meet the stated purpose and performance obligation articulated in the data-sharing agreement.

Chapter 9 Security

9.1 Introduction

MVAs are entrusted with PII of the citizens of their jurisdiction and expected by those citizens to protect that information from unauthorized use, disclosure, or access. Security, both physical and electronic, is of paramount importance to ensure data integrity, availability, and reliability.

The intent of this section is to provide general information and resources with enough guidance and background on information security to assist MVAs in making informed decisions. The main goal of this content is to help decision makers implement, maintain, and monitor a comprehensive written information security program that complies with applicable privacy laws, adheres to industry best practices or security principles, and promotes the availability of data for authorized use. The security program should include documented policies, procedures, standards, guidelines, and references as necessary to precisely define the security controls and how the controls should be implemented.

9.2 Security Program

Security programs are critical for proactively protecting data while maintaining compliance with both regulatory and customer requirements. The first step in implementing a functional security program is to determine the parameters and boundaries, or the scope, of the system and the users. In other words, a security program should account for what MVA data exist, which entities or individuals may receive the data or have access to the data, who will use the data and for what purposes, where the data will be used, and what systems will process the data.

To be effective, MVAs should maintain and enforce a security program at any location where MVA data, particularly PII, might be stored, processed, or accessed. During the course of providing services, the security program should not be altered or otherwise modified in such a way that will weaken or compromise the security, confidentiality, integrity, or availability of MVA data.

The security program should cover management controls, technical controls, operational controls, physical controls (key cards, locked doors, signage, offshore access), all networks, systems, servers, computers, notebooks, laptops, tablets, mobile phones, and other devices and media that process, host, or store PII or provide access to systems hosting or processing PII. The program also needs to require necessary and appropriate supervision over the relevant personnel to maintain appropriate privacy, confidentiality, and security of the PII.

A designated primary security manager will be responsible for managing and coordinating the performance of the organization obligations set by the MVA and coordinating any audit, review, inspection and communication with the MVA. Program governance shall include representatives from other business areas aside from the security function. The organization must designate an executive or someone within the senior management team with the responsibility to monitor the implementation and performance of the program.

9.3 Minimum Security Safeguards

MVAs should establish minimum safeguards to protect MVA data. The list of safeguards should include the following.

Personnel

- Criminal background checks should be performed for all MVA and data recipient staff who access PII. The background check reduces the chance that those with a criminal background or history of poor data stewardship do not have or have limited access to PII. If there is statutory authority to obtain fingerprint-based criminal background checks, that is the preferred method. To reduce costs and potentially eliminate the need for future background checks, jurisdictions should consider enrolling in the Record of Arrest and Prosecution Background (RAP Back)* program if it is available in their jurisdiction.
- If fingerprint-based background checks are not allowed, a commercial background check is permissible but should include checks from every jurisdiction in which the individual has resided in the past five years.
- It is a best practice for employees, including contractors or vendors, to sign a user agreement before receiving access to a system or facility with PII. A good user agreement will outline conditions of access to facilities or systems with PII, and there should be a mechanism for updating agreements if system database or file layouts are changed.†
- All personnel should undergo a new background check at least every five years unless the jurisdiction and the individual are enrolled in RAP Back.
- All personnel should be trained on the applicable requirements defined by the program.
- All personnel should acknowledge being covered by a security and confidentiality policy. Any security and confidentiality policy should clearly identify the consequences and actions that may be taken by the MVA.

Administrative or Procedural Security

- Establish procedural, technical, and physical internal controls.
- Keep records of who accessed PII and when it was accessed and from where.
- Encrypt PII at rest and in transit.
- Implement authentication and access controls for applications, operating systems, and equipment.
- Create and maintain a privacy policy, including what PII is collected, the purposes for collection, and with whom it is shared.
- Create and update an emergency or incident response plan to determine:
  - How data will be shared in times of limited access to information systems
  - What degree of data can be lost if there is an interruption in its processing
  - How data will be secured if physical controls typically in place are unavailable or less available
  - Creation of a continuity of operations plan (COOP) for long-duration incidents
- Establish policies and procedures to remove access to facilities and information systems when an employee or vendor or contractor is terminated.

* Federal Bureau of Investigation, "Next Generation Identification (NGI)" (see section entitled, "NGI Capabilities"), available from https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

† AAMVA, "System Modernization Best Practices," May 2017, page 40, available from https://www.aamva.org/SystemModBP/.

Technical Security

- Implement of any MVA-required security program and data-sharing agreement provisions by data recipients.
- Implement network, device application, database, and platform security.
- Apply secure methods of MVA data transmission, storage, and disposal.
- Use current antivirus software.
- Apply security measures for transmission or storage of MVA data on mobile devices including endpoint security, VPN, secure web gateway, email security, cloud access security broker, or ActiveSync policies and mobile device management tools.
- Enforce security controls on the use of removable media (e.g., USB flash drives, secure digital (SD) cards or other portal drives) that contain sensitive data.
- Do not transmit unencrypted MVA data over the internet or a wireless network.

Physical Security

- Maintain areas with access to MVA records in a secure manner with locks and controlled access.
- Secure business facilities, data centers, paper files, servers, backup systems, and computing equipment (including mobile devices and other equipment with information storage capability).
- Store secure printed documentation in locked filing cabinets or drawers with controlled access.
- Store backup and archival media containing MVA data in secure, environmentally controlled storage areas. Backup and archival media containing MVA data should be encrypted.

Standards and Guidelines

After the scope of the security program has been determined, the use of generally accepted industry or governmental standards is an effective way to ensure the day-to-day operations are meeting the stated policies of the plan. The security program should include, at a minimum, the following standards:

- Encryption of data in transit and at rest*
- Industry-standard password protections
- Firewalls
- Intrusion detection and prevention
- Data leak prevention
- Antivirus and malware protection
- Appropriate administrative, technical, physical, organizational, and operational controls and other security measures that meet or exceed an applicable third-party security assurance standards, such as ISO 27001, Statements on Standards for Attestation Engagements (SSAE) 16 SOC 2, NIST 800-53, NIST 800-171, International Standard on Assurance Engagements (ISAE) 3402, and ISO/International Electrotechnical Commission IEC 27001:2013

MVAs should consider data in all three states when protecting their PII—in use, in transit, and at rest. Data in use are data on endpoints being used by employees or authorized recipients to do their jobs. Data at rest are information stored on endpoints, file servers, and information repositories such as Microsoft Exchange servers, SharePoint, and web servers. Data in motion are data being sent over networks. MVAs should require that all PII, at rest or in transit, be encrypted using FIPS 140-3–certified algorithms.

To ensure the security program is within scope, the implementation status of the controls and effectiveness

* Encryption is the process of converting information or data into a code, which can then be accessed by entering a secret key or password, converting the information back into its original form.

of such controls should be audited by an independent third party at least every three years or whenever material changes are made to the security program. The controls are designed to ensure the security and confidentiality of PII by protecting against any anticipated threats or hazards to the security and integrity of PII, including unauthorized access; collection; use; copying; modification; disposal; disclosure; unauthorized, unlawful, or accidental loss, destruction, acquisition, or damage; or any other unauthorized form of processing. Any ineffective controls should be remediated immediately or within the time frames specified in audit findings.

Remote Working for MVA Employees

MVA employees are working remotely with greater frequency. The ability to telework is leveraged globally by large companies such as Microsoft and Google, as well as state or provincial and local government agencies, to expand their employee base and to meet business demands around the clock. The ability to allow MVA employees to work securely outside the physical confines of an MVA facility depends on the technological infrastructure in place at the MVA. Additional guidance may be found in NIST SP 800-46 REV. 2 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security.

In its most basic form, all that is needed for telework is a secure encrypted connection called a virtual private network (VPN) and an active internet connection. This creates a virtual connection to the MVA's computer network (in the facility) that allows the employee access to data, applications, and other resources. Because the work location is no longer under the control of the MVA, it is even more important to train employees on appropriate security measures while they are working remotely. Remote work emphasis areas include

- Awareness of surroundings (e.g., avoiding shoulder surfing)
- Securing physical documents when not working
- Locking unattended computers
- Removing proximity to virtual digital assistants (e.g., Amazon Alexa or Apple Siri) because these devices can hear and record portions of work conversations

In the absence of a computer connection, remote work can still be performed by providing the employee work in a physical format. Doing so, however, requires some additional steps to ensure the MVA data are protected, such as

- Require physical documents to be "checked out" and "checked in" to ensure accountability for the employee and the integrity of the documents.
- Adopt policies for the secure transport of documents by the employee including the use of
  - Sealed envelopes
  - Encrypted USB flash drives for electronic files for use on MVA-owned computers (not on personal computers)
  - Registered or tracked mail or delivery service for documents sent to or from the employee
  - A couriered service for delivery or pickup of documents if there are multiple employees in a confined geographic area

Administratively, an MVA should implement a telework agreement with the employee that specifically outlines the details of what is expected and allowed. The following is a list of items to consider:

- Telework location(s) such as home, another office, changing locations because of travel. A home office or other "lockable space" may be required for telework.
- Whether equipment (e.g., a laptop computer) will or will not be provided to the employee by the MVA

- The minimum specifications required for the connection (minimum bandwidth or Mbps)
- If allowing "BYOD" (bring your own device), the minimum requirements (e.g., operating system, virus protection, processor speed, memory, storage capacity, device registration)
- Inclusion of privacy clauses to make it very clear that MVA data cannot be shared with non-MVA personnel such as family members

Jurisdictions should coordinate any telework agreements or plans with their human resources and legal counsel to ensure risk to MVA data are minimized.

Security Expectations of Data Recipients

Data recipients and subrecipients should be required to comply with all MVA IT security policies at their own expense. Data-sharing agreements should refer or link to the controlling IT and MVA policies. Data recipients and subrecipients should be required to periodically review security policies for updates and remain in compliance throughout the life of the agreement.

MVAs should review and approve the data privacy training of data recipients and subrecipients or end users before providing MVA data and from time to time during the length of the agreement. Security reviews may be done by completing a security survey or attestation. Additional security verification may be accomplished through audit.

The MVA should require individual logon credentials prior to data access (i.e., disallow group logons). A recommended practice is to build into the system a quarterly, automated review to identify and remove individuals who have not accessed the information during that period. This also allows for a verification that all individuals or contractors with access have current certifications.

To ensure the physical security, MVA should enforce the data residency controls on data recipients. PII that was processed and stored in data recipient's IT system should remain within the country of jurisdiction's borders. This should include both physically and electronically stored data. Access to MVA records should be limited to authorized individuals.

Logging, Tracking, and Accounting for Data Recipients

MVAs should be able to ensure that data recipients are accessing data only for permissible purposes and in accordance with data-sharing agreement requirements. Using audits and confirming that MVA records are accessed through sample checking of business records are good steps toward data protection, the best practice is for the MVA to know how data recipients used MVA data each time. To achieve this end, MVAs should implement logging, tracking, and accounting practices.

Every data recipient who receives data from an MVA should be granted a unique ID that matches to a use agreement account number or other unique ID. Every data recipient with electronic access to MVA records should be assigned a unique logon ID. A logon ID should be assigned to one individual and should not be shared or reassigned.

MVAs should require data recipients who release MVA data to subrecipients to identify all subrecipients and end users. The MVA should give subrecipients and end users subaccount numbers or some other type of tracking mechanism to link with the original data recipient.

Data recipients should maintain access logs of physical and electronic access to data. Storage arrangements or controlled access should be subject to inspection or audit by MVAs. For data recipients with electronic access to MVA data, every time a user logs into their account to access a customer record, the privacy or audit logs in MVA's system for that data recipient

should note the user's logon ID and the associated organization or use agreement. If the MVA allows multiple permissible uses under the same use agreement number, the data recipient should be prompted to input the purpose of the individual request. For data recipients who receive MVA data files without electronic access to the MVA system, the unique ID for that recipient should still be noted on the individual customer record when the data are taken and sent to the recipient through a file transfer. In other words, the release of MVA data should be noted in the MVA tracking logs regardless of the method of release. The data recipient's account may be set to record a specific length of record history (e.g., basic record, 3 years of history, 10 years of history, full history).

Each access to a record containing PII should be logged and associated with a business record showing the data or record access and reason for access. Thus, the MVA will be able to produce for any individual customer a list of entities that have accessed their customer record and the purpose for the access. Some MVAs are obligated by law to produce an access report upon request by the customer. MVAs might consider exceptions to this public reporting feature, such as secure law enforcement accesses that could jeopardize an ongoing investigation. MVAs should note, however, that if they choose not to require pre-approval and tracking of subrecipients and end users, the MVA audit logs will only show the original data recipient. The MVA will be required to contact the data recipient to establish a complete tracking and audit trail for any released MVA data.

Additional Considerations

Below are recommendations designed to prevent unauthorized use of data:

- **Do not use email for data sharing.** Standard consumer-grade email is not a secure method for sharing MVA data. In most cases, data sent in email is not encrypted. Incorrect entry of an email address risks sending MVA data to the wrong party. Email encryption options are available, but they are not standard to email and will incur cost and resources to implement as additional software.
- **Do not use consumer-grade file-sharing tools.** Consumer-grade file-sharing tools, such as Dropbox, Box, and Google Drive, are not secure. MVAs cannot guarantee the security of data shared via a public cloud, and consumer-grade file-sharing services do not have enterprise-grade security features.
- **Do not create generic accounts for others to use while accessing data.** Always ensure that everyone has unique credentials that can be traced back to a single person or company.

9.4 Recommendations

- MVAs should maintain and enforce a security program at any location where MVA data, particularly PII, might be stored, processed, or accessed.
- MVA should establish minimum safeguards for data recipients to follow in order to protect MVA data. It is important to review the data recipient and subrecipient information security processes and safeguards before providing PII or MVA data.
- Criminal background checks should be performed for all MVA staff who access PII.
- If fingerprint-based background checks are not allowed, a commercial background check is permissible but should include checks from every jurisdiction where the individual has resided in the past five years.
- All personnel should undergo a new background check at least every five years unless the jurisdiction and the individual are enrolled in RAP Back.

- All personnel should be trained on the applicable requirements defined by the program.
- All personnel should acknowledge being covered by a security and confidentiality policy. Any security and confidentiality policy should clearly identify the consequences and actions that may be taken by the MVA.
- The program should include appropriate administrative, technical, physical, organizational, and operational controls and other security measures that meet or exceed an applicable third-party security assurance standards.
- MVAs should consider data in all three states when protecting their PII—in use, in transit, and at rest.
- The security program should cover management controls, technical controls, operational controls, physical controls (key cards, locked doors, signage, offshore access).
- MVA should implement a telework agreement with work from home employees that specifically outlines security protocol.
- MVAs should review and approve the data privacy training of data recipients and subrecipients or end users before providing MVA data and from time to time during the length of the agreement.
- For the data to be accessed, the MVA system should require individual logon credentials (disallow group logons). Best practice is to build into an information system a semiannual, automated review to identify and remove individuals who have not accessed the information during that period.
- Data recipients and subrecipients should be required to comply with all MVA IT security policies at their own expense.
- Electronic devices used to access MVA data should have current anti-virus software.
- MVAs should enforce mobile device security controls on the use of secure digital (SD) cards or other removable media that contain sensitive data.
- PII that was processed and stored in data recipient's IT system should remain within the country of jurisdiction's borders.
- To ensure the security program is within scope, the implementation status of the controls and effectiveness of such controls should be audited by an independent third party at least every three years or whenever material changes are made to the security program.
- MVAs can consider adopting and communicating common practices that safeguard personal data, including but not limited to the following:
  - Do not create generic accounts for others to use while accessing your data.
  - Do not use email for data sharing.
  - Do not use consumer-grade file-sharing tools.
  - Do not share any unnecessary information.

Chapter 10 Personnel and Resources

10.1 Introduction

A key part of data privacy is helping to ensure the jurisdiction has a comprehensive and cohesive organizational structure to allow appropriate levels of decision making, responsibility, and accountability. This section provides MVAs with best practice recommendations for position functions based on specific knowledge, skills, and abilities, as well as organizational levels of responsibility (executive, operations, and business owner).

Some of the recommended positions in the chart below may be staffed by other agencies (e.g., attorneys general, chief information officer). In such cases, MVAs should establish good working relationships with these organizations to allow for effective communications and a shared understanding of MVA data privacy requirements. Ideally, the role of data privacy officer should be a dedicated, full-time position within the MVA. However, if the roles of the Chief Information Security Officer (CISO) and data privacy officer are assumed by an individual outside an MVA, it is essential that this person be fully in sync with MVA operations and other roles within the MVA.

The following table defines roles and responsibilities that support management of data privacy. Titles are provided in the right-hand column to illustrate what individuals performing the duties might be called. A sample organizational chart is provided to give visual context to levels of responsibility and allow the reader to see how the various roles are related. Although some jurisdictions may choose to assign each level of duties to separate individuals, others, because of budgetary constraints, might need to combine roles. This is an acceptable practice, but it is important to avoid inherent conflicts of interest (e.g., combining auditor duties with data-sharing agreement duties) when assigning multiple roles. Although it is not essential to staff each position detailed in the following list separately, each duty should be covered by at least one MVA representative. In addition, some responsibilities and duties may be a potential duty for more than one role listed below. It is important to identify and delineate duties for multiple personnel positions within an MVA.

10.2 MVA Privacy Management Responsibilities and Titles

Executive

Titles:

- Chief Data Officer
- Data Privacy Officer

Responsibilities:

- Develop and oversee data protection policy and implementation to ensure compliance with federal and jurisdictional laws regarding both disclosure and protection of MVA data.
- Educate staff regarding compliance requirements, including federal and jurisdiction laws, and train staff who are involved in data processing.
- Make staff aware of what data the MVA processes.
- Monitor data-sharing agreement performance and provide advice on the impact of data protection efforts.
- Ensure necessary records of all data-processing activities conducted by the jurisdiction, including the purpose of all activities, for mandated retention period.
- Ensure security of records.

Executive

Titles:

- Counsel
- Records Access Officer
- Freedom of Information Officer

Responsibilities:

- Serve as a subject matter expert to executives regarding jurisdictional and federal laws for privacy and compliance.
- Provide access to public MVA records and fulfill open records requests.
- Receive requests from individuals about the personal data or information the agency maintains on said subject or the system of records pertaining to the individual.

Executive

Title:

- Contracts (or Data-Sharing Agreement) Compliance Officer

Responsibilities:

- Be intimately familiar with all the business functions that are related to the data-sharing agreement, including business, legal, finance, security, and privacy.

(continued on next page)

Executive and IT

Titles:

- Information Security and Privacy Compliance Manager
- Data Sharing and Privacy Manager

Responsibilities:

- Manage the agency-wide Information Security and Privacy Compliance Program.
- Serve as the first level of communication for auditors, in-house data security IT managers, and data recipients regarding privacy, data-sharing agreement obligations, performance, transaction support, and investigations of unauthorized use.
- Provide innovative leadership and expertise in managing complex data-sharing agreement compliance activities.
- Implement and maintain programs, policies, and procedures regarding data security, privacy, and permissible use for sharing data.
- Establish criteria and protocols to ensure processes are followed consistently when reviewing data requests, data-sharing agreement compliance, curing, and termination.
- Provide compliance and investigative services.
- Serve as subject matter expert on industry standards for data-sharing agreement audits and compliance requirements, policy issues and proposed changes to agency procedures.

IT

Titles:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)

Responsibilities:

- Develop security strategy, security program oversight, and security architecture development and implementation for the organization.
- Develop data and information security policies, standards, guidelines, evaluations, roles, and organizational awareness.
- Work closely with other stakeholders, such as those defined here and the business owners, to ensure that technological, operational, and managerial security controls and policies meet the organization's data security requirements.
- Manage data and information risks related to product development, technology solutions, crisis management, and security regulatory compliance.
- Direct the preparation activities to support Payment Card industry Data Security Standard (PCI-DSS), SOC 2, and other compliance audits.
- Develop and manage a comprehensive information security risk-based program to ensure the integrity, confidentiality, and availability of information assets.
- Develop an IT security architecture roadmap that will identify security controls; identify and assess current and new technologies that will enforce the organization's security priorities.
- Define and facilitate the information security risk assessment process and work effectively with technology group in implementation of security measures.
- Provide strategic risk guidance, consultation, and coordination with business teams for IT projects, including the evaluation and recommendation of technical standards and controls related to data privacy.
- Establish and implement a process for incident management to effectively identify, respond, contain, and communicate a suspected or confirmed incident.
- Be aware of the latest developments in data security and how they may be applied to an MVA.

(continued on next page)

IT

Title:

- Data Custodian

Responsibilities:

- Maintain data.
- Control access to data.
- Apply physical and technical safeguards to protect data.
- Understand MVA policies governing the use of MVA data, training of employees (where applicable), assisting with MVA external audits, and safeguarding MVA data.

Business

Title:

- Risk Manager

Responsibilities:

- Create a risk management policy for an MVA.
- Conduct education and outreach on risk awareness (e.g., internal posters or flyers on sensitive document shredding, changing passwords).
- Establish and update internal controls program.
- Conduct internal control inventory and or use of internal controls.

Business

Title:

- Data Steward

Responsibility:

- Assist with the identification of data sources and assets.
- Define business terms and rules of data fields and data relationships.
- Validate internal and partner access rights to data assets.
- Identify and monitor data regulatory compliance.
- Identify data quality improvement opportunities through data usage monitoring.
- Ensure consistent data quality, establish data standards and governance, and certify internal and external data sharing.
- Serve as guardian and decision maker for data assets.
- Gather and document metadata, understand how data migrates across the organization systems; improve data quality, analyze process controls, and coordinate the development of security and privacy requirements with the CISO and Data Privacy Officer.
- Understand how MVA data are collected, maintained, and interpreted.
- Understand the day-to-day operational and administrative management of the systems that house MVA data, including intake, storage, processing, and transmission of data to internal and external systems.
- Incorporate processes, policies, guidelines, and responsibilities for administering an organization's data in compliance with business and regulatory obligations.
- Understand the business domain and the interaction of business processes with data entities or elements.
- Work with other data custodians, database and warehouse administrators, and other related staff to plan and execute an enterprise-wide data governance, control, and compliance policy.

(continued on next page)

Business

Titles:

- Records Officer
- Records Manager

Responsibilities:

- Oversee a records management program to include the storage, retrieval, retention, and disposition of public records.
- Provide training to staff on the requirements of the MVA's records management program.
- Ensure the MVA has implemented an emergency response plan in the event of a disaster.
- Identify essential and archival records to be permanently preserved and maintained.
- Conduct internal reviews to ensure MVA compliance with the controlling record retention laws.

Business and IT

Title:

- Data Owner

Responsibilities:

- Act as data asset champion.
- Prioritize data improvement opportunities.
- Approve data access and business rules related to data files and relationships.
- Assist with the identification of data regulatory compliance.
- Decide improvement strategies, monitoring, reporting, and implementation.
- Correspond with data stewards and business partners to implement data improvement strategies.

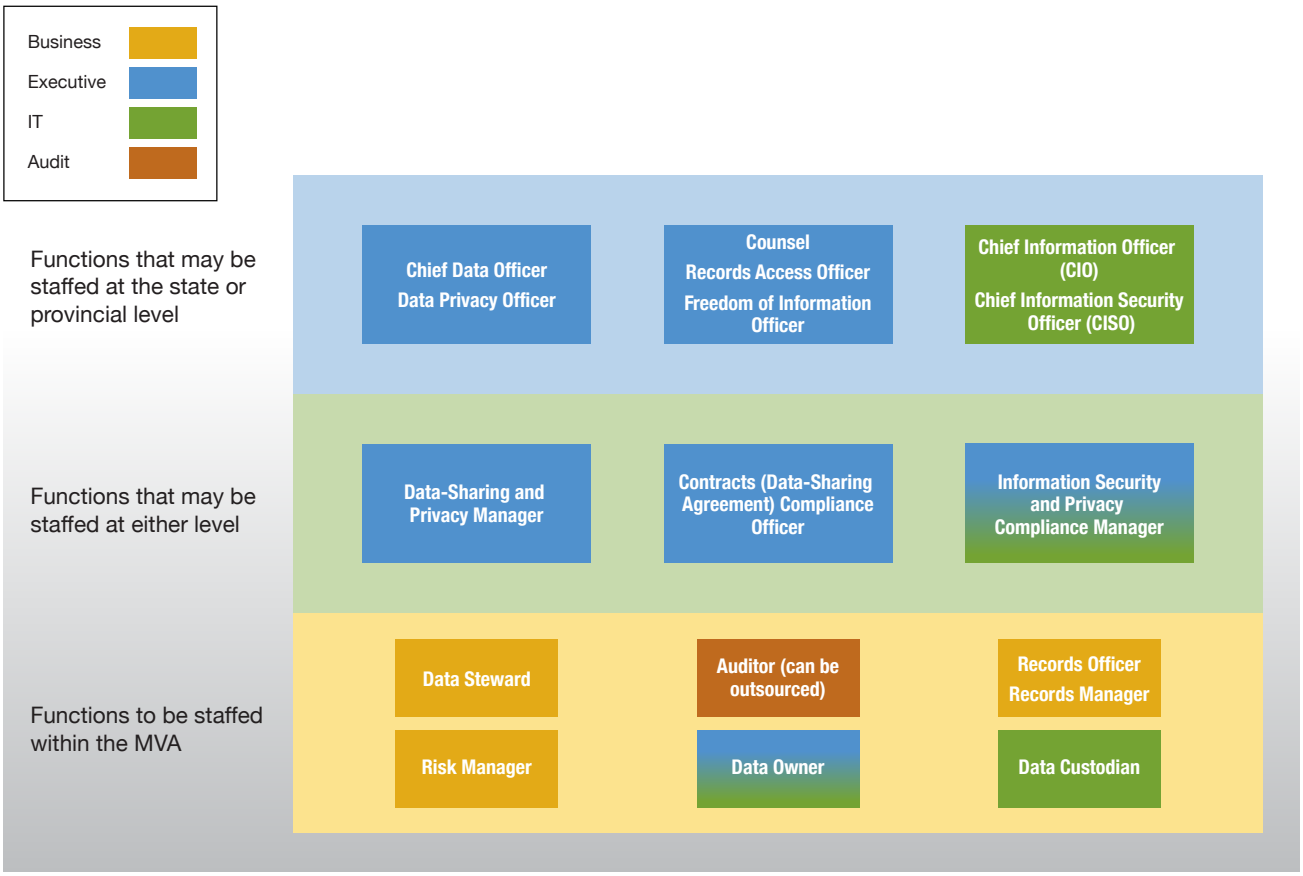
Audit

Title:

- Auditor

Responsibilities:

- Conduct operational, privacy compliance, or IT audits in accordance with established standards, policies, and regulations.
- Conduct regular audits both internally and externally to ensure compliance.
- Perform audit planning, develop audit programs, and perform test procedures, interviews, and evidence review.
- Develop and document audit findings in accordance with GAGAS; develop audit conclusions and recommendations designed to improve the effectiveness and efficiency of the MVA operations.
- Be intimately familiar with all the business functions that are related to the data-sharing agreement, including business, legal, finance, security, and privacy.
- Ensure compliance with established internal control procedures by examining records, reports, operating practices, and documentation.
- Appraise adequacy of internal control systems by completing audit questionnaires.
- Maintain internal control systems by updating audit programs and questionnaires; recommend new policies and procedures.
- Communicate audit findings through a comprehensive report; discuss findings with auditees.
- Ensure compliance with federal, state, and local security legal requirements by studying existing and new security legislation; enforce adherence to requirements; and advise management on needed actions.
- Prepare special audit and control reports after collecting, analyzing, and summarizing operating information and trends.
- When noncompliance is determined, direct data recipients to develop written corrective action plans that include time frames for compliance.
- Review and respond to data-recipient-submitted compliance plans.



The above figure depicts responsibility relationships between business, legal, technology, and audit. The blue band generally delineates roles that may be performed at an enterprise level versus those that typically are performed by the MVA.

10.3 Recommendations

- It is recommended that MVA staff, at a minimum, fill the following roles to protect MVA data and PII:
  - Data Privacy Officer (DPO)
  - Contracts Compliance Officer
  - Chief Information Security Officer (CISO)
  - Auditor
  - Data Steward(s)
  - Data Sharing Manager
  - Information Security and Privacy Compliance Manager
- MVAs should establish a good working relationship with cooperating organizations to allow for effective communications and a shared understanding of MVA data privacy requirements.
- The role of data privacy officer should be a dedicated, full-time position within the MVA.
- If the roles of the CISO and data privacy officer are assumed by an individual outside an MVA, it is essential that this person be fully in sync with MVA operations and the other roles within the MVA.

Chapter 11 Outreach and Education on the Importance of Safekeeping Records

11.1 Introduction

An effective outreach and education program focusing on the value of and need for MVA data protection is an important element in managing data privacy. Educating employees and data recipients about the importance of MVA data protection and training them how to protect and handle MVA data will help reduce the likelihood of an unauthorized use or disclosure. Jurisdictions may choose to offer structured education, such as annual permissible use training, for entities receiving customer data. Such training could be used as a mandatory prerequisite for a data-sharing agreement initiation or renewal. Outreach, education, and training are preventive measures to reduce risk of data leakage and fraud. Training should be continuously updated and provided on a regularly scheduled basis to help anticipate and thwart unauthorized access and use of MVA data.

The benefits of training, outreach, and education include:

- Improved policy and regulatory compliance
- Increased public trust
- Improved ability to safeguard data
- Improved accountability
- Mitigation of the risk of unauthorized disclosure/use

11.2 Privacy Training Requirements

Training should be based on policies and standards and address the key elements necessary for helping to ensure the safeguarding of PII and MVA data. The required training should be foundational and role based, provide advanced levels of training, and have measures in place to test the knowledge level of data recipients. Privacy training for both MVAs and data recipients should occur when an employee begins (onboarding) and then on an annual or recurring basis. A best practice for MVAs is to have data recipients and subrecipients annually certify that the training took place and the results. Initial and annual data-privacy training topics may include but are not limited to:

- Federal and jurisdictional requirements for protecting PII and MVA data
- The appropriate handling and safeguarding of PII, including basic privacy principles (data minimization, data quality, and so on)
- Processing and understanding the foundations for open record requests – federal, state, and provincial requirements
- Applicable industry-specific requirements and controls such as credit card handling (PCI audits) or SOC controls for service organizations as defined by the American Institute of Certified Public Accountants
- Code of conduct and policies and procedures
- Public records and the balance between transparency and privacy
- Information security, including password protection and awareness and avoidance of malware, phishing, and social engineering; device security; and internet security

- Physical security, including building access, security, and location of records
- Incident response procedures and reporting

Internal

Establishing a solid internal privacy training and education program is a great first step for MVAs to take in this area. Employees should be equipped with the tools needed to manage and understand privacy obligations. MVAs can leverage quality internal training and outreach materials to use for external training and outreach.

MVAs may be subject to both internal and external audits. MVAs that do not have policies and procedures developed to protect PII and do not provide privacy training will likely receive an audit finding. Depending on the organizational structure in the jurisdiction, the responsibility to deliver training might vary.

External

DATA RECIPIENT EDUCATION AND OUTREACH

MVAs should require data recipients who have access to MVA data or who handle PII to provide annual privacy training to their employees. Data recipients may provide their own training as long as the content meets minimal content requirements of the MVA. For data recipients with multiple subrecipients, the data recipients are responsible for implementing the training requirements mandated by MVAs. The data recipient should retain documentation of completed privacy training and make documentation available for review by the MVA upon request.

MVAs may allow data recipients to use an MVA created training course or use an MVA-approved internal training course to continue to access MVA data. The MVA should retain complete discretion as to whether a data recipient's training is sufficient. Such a decision should consider whether the MVA-required training includes jurisdiction-specific information.

11.3 Recommendations

- Jurisdictions might offer structured education, such as annual permissible use training, for entities receiving customer data.
- Training should be continuously updated and provided on a regularly scheduled basis to help anticipate and thwart unauthorized access and use of MVA data.
- MVAs should require data recipients, who have access to MVA data or who handle PII, to provide annual privacy training to their employees.
- MVAs may allow data recipients to use an MVA created training course or use an MVA-approved internal training course in order to continue to access MVA data.

Chapter 12 Public Sector Entities

12.1 Introduction

Public sector entities regularly access and use MVA data. MVA data helps government entities provide services, such as protecting public health, establishing individual's identity, and enforcing laws. As with nongovernment requesters, MVA data may be shared with governments one record at a time or in bulk. Individual requests may be for common transactional reasons, such as validating identity for employment, and bulk requests may be driven by research needs, support for identity systems, or support for data analytics platforms.

12.2 One-Time, Limited Records Request and Permissible Use

Government entities are bound by the same permissible uses as private sector data recipients. A request from a government entity for MVA records or data should use an established request form. Identification requirements for release of PII should be the same as nongovernment entities, and the use of a ".gov" or similar government email extension may help validate identity. This is important both for permissible use validation and document or record fee waiver reasons.

The DPPA (applicable in the United States) provides that PII must or shall (as opposed to "may") be disclosed for certain reasons, and in some instances, government requesters may have one of those reasons, such as motor vehicle or driver safety and theft. Otherwise, disclosure of PII may be made to government requesters for use in carrying out a government function.

12.3 Request for Bulk Data and Frequent Requests

MVA data may be requested in bulk for several reasons. Bulk requests for MVA data access may include public safety, validating or establishing automobile crash or crash research databases, voter registration validation, census record validation, or to support data analytics tools or platforms. Some jurisdictions may request MVA data for use with a government supported data platform or trust to combine and share data amongst multiple government entities.

12.4 Law Enforcement Agencies

Federal, state, provincial, territorial, county, city, and tribal LEAs throughout the United States and Canada rely on MVA data for the administration of criminal justice. The reciprocal partnership between MVAs and LEAs has existed for many years. Data sharing with LEAs is necessary to enforce laws and maintain public safety. MVAs and law enforcement should maintain a collaborative working relationship and have a joint approval process for acceptable access to and usage of MVA data for authorized law enforcement purposes.

MVAs share data with LEAs to enforce laws and protect the public. LEA officers use MVA data and documents primarily for identification purposes. Comparing the driver's license image and other PII associated with a driver's license is efficient, reliable, and widely accepted by the public as a normal process. Other uses include vehicle registration information, which is used by officers to enforce registration and tonnage requirements, as well as to ensure lawful ownership of vehicles and vessels.

In some instances, MVA data may be shared through Nlets with an LEA for a reason that is not specifically related to criminal justice. These scenarios require some explanation of how MVA data are electronically shared with LEAs:

- Each jurisdiction (state or province) has a link to "Nlets," a telecommunication network made available through a private, not-for-profit corporation owned by state LEAs. Nlets is the primary connection between the LEAs in the United States, U.S. territories, and Canada.
- Every criminal justice agency in the United States, U.S. territories, and Canada has a nine-character ID assigned by the FBI for use in requesting and receiving criminal justice related telecommunications. The nine-character ID is called an Originating Agency Identifier, or ORI.
- An electronic data request for criminal justice specific purposes is issued using an ORI. In instances in which a data recipient has a legitimate but non–criminal justice–specific need for MVA data and does not work for an LEA, a request with an "S" in front of the ORI is issued. Parking enforcement, code enforcement, animal control, toll authorities, and commercial vehicle enforcement are often performed by individuals who are nonsworn or work for a non-LEA department. The "S" is a designator to allow easy identification of non–criminal justice recipients.

12.5 Data-Sharing Agreements with Government Entities

As with nongovernment entities, request for access forms and data-sharing agreements with government entities should be structured with provisions outlined in this best practice (See Data-Sharing Agreements and Analysis of Request). The following guidelines are offered for sharing of large amounts of MVA data in a data analytics context:

- Read all agreements and determine if appropriate safeguards to protect MVA data are in place. Sharing MVA data with a data aggregator, even when run by a government entity, is a release that is subject to data privacy laws.
- Review and approve any entities with access to data aggregation platforms to ensure each one has a permissible purpose, as governed by federal or jurisdictional laws, for receipt of MVA data.
- Explore and understand the mechanisms protecting a data aggregating platform because de-identified or anonymized data may be at risk when combined with other data sets.
- Large amounts of combined data sets containing customer information may be a particularly appealing target for exploitation or hacking. Conduct a risk analysis before participating with PII in any analytics platform.

To keep release of PII and MVA data consistent with the principles and guidelines established in this best practice, Nlets and MVA members should:

- Individually and together review the jurisdiction laws and data-sharing agreements in place that allow access to and secondary dissemination of MVA data for approved purposes.
- Jointly discuss the procedures by which "S"ORI access is considered and granted in each jurisdiction and incorporate a MVA review/approval step into the process if one does not already exist.
- Examine the list of current "S"ORIs in a jurisdiction and jointly affirm that their access is consistent with interagency agreements, and if not, discuss a mutually acceptable path to resolve.

To account for the range of access to MVA data that may be enabled through Nlets and assure MVA data access and use requirements are met, an interagency

agreement between the MVA and lead LEA that considers best practices and provisions outlined in this document is recommended.

See Appendix E for an Nlets relationship diagram.

12.6 Recommendations

- Read all agreements and determine if appropriate safeguards to protect MVA data are in place.
- Review and approve any entities with access to data aggregation platforms to ensure each one has a permissible purpose, as governed by the DPPA or state or provincial laws, for receipt of MVA data.
- Explore and understand the mechanisms protecting a data aggregating platform, as de-identified or anonymized data may be at risk when combined with other data sets.
- Conduct a risk analysis before participating with PII in any analytics platform.
- Nlets and MVA members should
  - Individually and together review the jurisdiction laws and data-sharing agreements in place that allow access to and secondary dissemination of MVA data for approved purposes.
  - Jointly discuss the procedures by which "S"ORI access is considered and granted in each jurisdiction and incorporate a MVA review or approval step into the process if one does not already exist.
  - Examine the list of current "S"ORIs in a jurisdiction and jointly affirm that their access is consistent with interagency agreements, and if not, discuss a mutually acceptable path to resolve.
  - Develop an interagency agreement that considers the best practices outline in this document.

Conclusion

MVA data are valuable resources to many entities, both public and private, and the data sources expects their PII to be protected. Providing these data benefits public safety and is critical for law enforcement activity and administrative actions such as motor vehicle recalls. However, keeping and releasing PII brings some level of risk. This best practice provides a framework for protecting MVA data against the risk of abuse or improper use and preventing the loss of public trust if that data are improperly accessed or used.

Common principles, as laid forth by this document, can be adopted by MVAs and data recipients to develop a common understanding of protecting data, identifying the steps used to protect the data and incorporating the legal foundation for the data's protection.

MVAs need to understand the data they have, what value and what risk the data carry, and how best to protect the data. Following the guidelines set forth in this best practice will help prevent unauthorized access disclosure or use by reducing risk exposure. Limiting risk and safeguarding MVA data so that it is used in a way consistent with public expectations is critical to preserving trust of MVAs as stewards of public assets.

The recommendations in this best practice are designed to be recommendations. The best practice is provided for MVAs to have guidance to make incremental change over a time period that works best for them in pursuit of a stronger data privacy posture. Using it is a best practice in its own right.

Appendix A References to Court Cases and Laws

Court Cases

DPPA and collision reports – Washington State. https://www.leagle.com/decision/infdco20180119b58

U.S. Supreme Court – Maracich et al. *v*. Spears et al. (2013) (*Held*: An attorney's solicitation of clients is not a permissible purpose covered by the (b)(4) litigation exception.)

Laws

California Consumer Privacy Act (CCPA). Passed in 2018 and effective January 1, 2020, the law applies to businesses generating $25 million in annual revenue, gathering data on more than 50,000 users, or making more than half its revenue from user data. The law provides:*

- That California residents have the right to
  - Know what personal information is collected, used, shared, or sold.
  - Delete personal information held by a business or business service provider.
  - Opt out of the sale of personal information.
  - Not be charged a higher cost or provided a lower grade of service by exercising said rights under CCPA.
- That California businesses must make available two means to make requests about what data or personal information was released. The business must answer free of charge.
- A threshold for compliance of $25 million gross revenue annually or the purchase, receipt, or sale of the PII of 50,000 or more consumers, households, or devices, or when 50% or more annual revenue comes from sale of consumer personal information. Businesses handling the personal information of more than four million records have additional obligations.
- That personal information is broadly defined and could include utility usage.

2019 Vermont S 110 – 3/5/2020

- This bill proposes to create a chief privacy officer; to direct the state to conduct a privacy audit concerning the collection and use of citizens' data; to adopt a student online privacy protection act; to expand the definition of PII subject to the Security Breach Notice Act and ensure consumer notice of a data breach; and to require internet service providers to provide notice concerning the potential sharing of private data.

2020 Washington S 6187 – 3/18/2020

- Modifies the definition of personal information for notifying the public about data breaches of a state or local agency system.

* https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

Appendix B Privacy Framework Function and Category Unique Identifiers

The following table is taken from the NIST Privacy Framework, Appendix A: Privacy Framework Core.

Privacy Framework Function and Category Unique Identifiers			
Function Unique Identifier	**Function**	**Category Unique Identifier**	**Category**
ID-P	**Identify-P**	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	**Govern-P**	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	**Control-P**	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	**Communicate-P**	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	**Protect-P**	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	**Detect**	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	**Respond**	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	**Recover**	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Appendix C Security References

International Organization for Standardization/International Electrotechnical Commission 27001:2013, Information Technology—Security techniques—Information security management systems—Requirements
https://www.iso.org/standard/54534.html

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
https://doi.org/10.6028/NIST.SP.800-53r4

NIST SP 800-55, Revision 1, Performance Measurement Guide for Information Security, December 2014.
https://doi.org/10.6028/NIST.SP.800-55r1

NIST SP 800-88, Guidelines for Media Sanitization, December 2014.
https://doi.org/10.6028/NIST.SP.800-88r1

National Archives and Records Administration, Controlled Unclassified Information (CUI) Registry.
https://www.archives.gov/cui

Federal Information Security Modernization Act (P.L. 113-283), December 2014.
https://www.govinfo.gov/app/details/PLAW-113publ283

U.S. Privacy Act (P.L. 93-579), December 1974.
https://www.govinfo.gov/app/details/STATUTE-88/STATUTE-88-Pg1896

CJIS – Security Policy Resource Center
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Appendix D Security Use Case Scenarios

Many of the concepts and protections described in this section are from the FBI, CSP, the rulebook followed by every criminal justice agency in the United States as it relates to protecting CJI, which often is PII with additional MVA data.

The CSP is available for download from the FBI and could provide the starting point for a security plan. Throughout the CSP, use-case scenarios are provided to allow a "real-world" explanation of what might otherwise be a technically accurate but difficult-to-understand IT explanation. The following use cases are modified for use in this best practice but come from the CSP to help illustrate the best practices outlined in this section.*

Multifactor Authentication Scenarios

An MVA Uses Multifactor Authentication for Access to Their Data from a Nonsecure Location

An MVA employee working from home attempts to access MVA data using an agency-issued mobile broadband card or their home Wi-Fi connection. To gain access, the employee first establishes the remote session via a secure VPN tunnel (satisfying the MVA requirement for encryption). Upon connecting to the agency network, the employee is challenged for a username, password, and a one-time password (OTP) from a hardware token (a USB key fob with a digital number display) to satisfy the requirement for multifactor authentication. After the employee's credentials are validated, their identity may be used by all authorized applications needed to perform their work.

Improper Use of a One-Time Password

Using an MVA-issued laptop, an employee connects to the agency network via an agency-issued mobile broadband card and an encrypted VPN tunnel. Upon opening the software application allowing the employee access to MVA data, they are prompted to enter a username (identification) and a password ("something you know"). Then an OTP is sent to the employee's MVA-issued laptop via a pop-up message. The employee is then prompted by the MVA data application for that OTP. However, because the delivery of the OTP is directly to the device that is being used to access MVA data, it defeats the purpose of the second factor (if someone had stolen the laptop, they would be able to gain access to MVA data). This method does not satisfy the requirement for multifactor authentication (MFA); therefore, the user should not be granted access to MVA data. However, if the OTP is send via a separate "route," such as a text message to an MVA-issued cellphone or in email, then the requirements of MFA have been met.

Risk-Based Authentication Implementation

An MVA employee has moved office locations and requires email access (to emails containing MVA data) via Outlook Web Access. The user launches the Outlook Web Access program and is prompted to enter a username (identification) and a password ("something you know"). The risk-based authentication (RBA) detects this computer has not previously been used by the user and is not listed under the user's profile and then presents high-risk challenge or response question(s), which the user is prompted to answer. If the correct answers are given, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects device forensic information and captures the user pattern analysis to update the user's profile.

* U.S. Department of Justice. "Criminal Justice Information Services (CJIS) Security Policy," June 2020, available from https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Faxing from a Multifunction Device Over a Network – No Different Than Emailing

An MVA employee needs to fax MVA data to a data recipient. The MVA data are printed, and the MVA employee uses a multifunction copier to fax the file to the data recipient. The document containing MVA data are automatically converted to a digital file and routed to the data recipient over the MVA network and the internet. Because the multifunction device uses a network and the internet for transmitting documents containing MVA data, the same network requirements for any MVA data are necessary (i.e., FIPS 140-3–certified 128-bit symmetric encryption).

Encryption for Data at Rest

A data recipient is converting all MVA data they have in hard copy form to an electronic format. The records will be scanned from hard copy to electronic files and placed on a network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location as approved by the MVA, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, IT staff have decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256-bit strength and use an MVA-approved passphrase to lock the folder's encryption. When an authorized data recipient needs to access the MVA data, the data recipient accesses the folder on the server and is prompted to enter the designated passphrase to decrypt (unlock) the folder. The data recipient can then access all files within the folder.

Cloud Utilization Scenarios

Encrypted PII in a Cloud Environment – Key Management Control, Security Awareness Training, and Personnel Controls

Prior to permitting MVA data to be stored in or travel through a cloud environment, MVAs should ensure proper encryption key management control procedures are implemented. Key management control procedures determine who has access and control over encryption keys. Proper key management control is vital to PII security because those individuals (jurisdiction or cloud employees) with access to the keys can decrypt the stored files and therefore have unescorted access to unencrypted MVA data. This means these individuals should receive privacy training and meet the same standards as MVA personnel.

MVA Data Stored in a Cloud

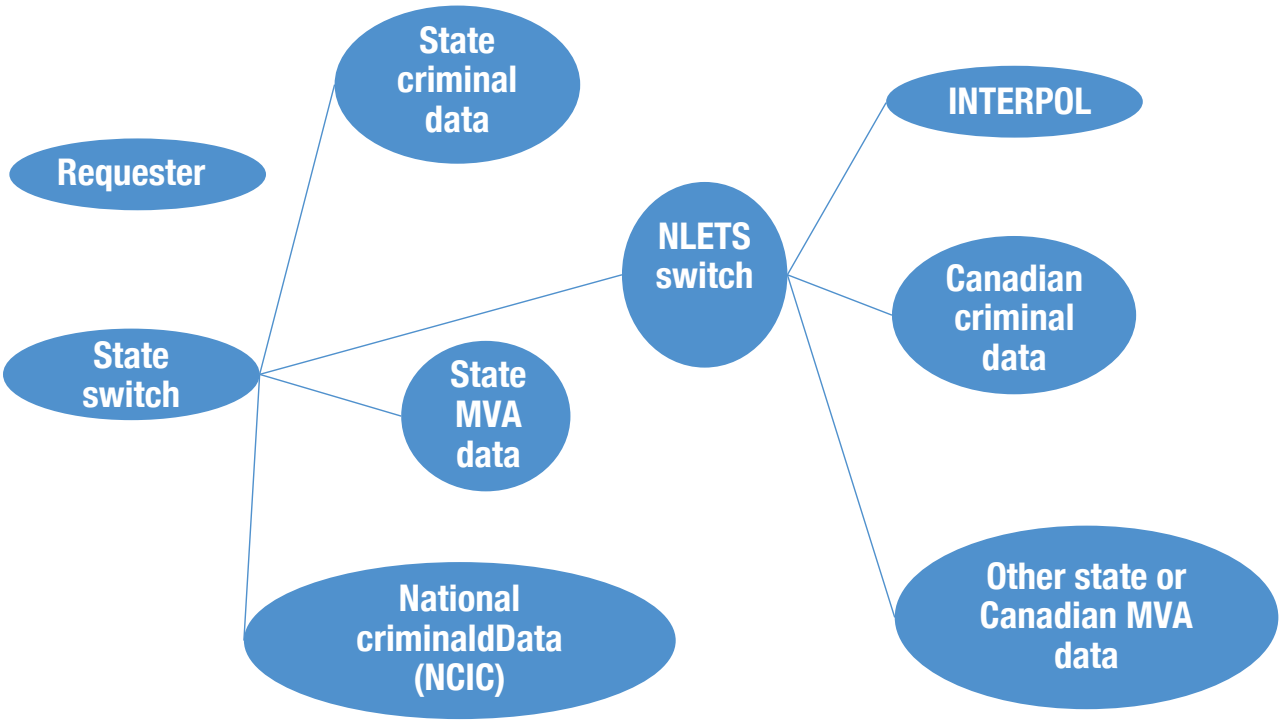
An MVA stores its encrypted data in a cloud service provider's environment. To access the MVA data, the MVA employee will download the data from the cloud to a computer and decrypt it. The MVA data are processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the jurisdiction always encrypts the data prior to placing it in the cloud, and only authorized MVA employees have access to the encryption keys. Because the MVA maintains the encryption keys, the cloud service provider employees do not undergo any additional background checks nor need to have privacy training. These requirements are negated because only authorized MVA personnel with access to the keys have the ability to view MVA data in an unencrypted form.

MVA Accesses Its Data in a Cloud

An MVA stores its data in a cloud service provider's environment, but as part of daily operations, authorized users (MVA employees and data recipients) remotely access the encrypted MVA data in the cloud. The user decrypt the MVA data while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. MVAs maintain the keys, and the cloud service provider does not have access to the encryption keys. However, because the MVA data are decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider who have the ability to access the virtual environment should be identified and subjected to privacy awareness training and personnel security controls as required by the MVA.

Appendix E Nlets Relationship

Each jurisdiction has a link to "Nlets," a telecommunication network made available through a private, not-for-profit corporation owned by state LEAs. Nlets is the primary connection between the LEAs in the United States, U.S. territories, and Canada. The diagram below depicts data-sharing relationships between various LEAs:



Appendix F Working Group Members

CHAIR

Minty Patel
Manager, Driver and Vehicle Information
Pennsylvania Driver and Vehicle Services

MEMBERS

Albert Hwang
Chief Privacy Officer
California Department of Motor Vehicles

Ann Perry
Director, Bureau of Driver Services
Wisconsin Division of Motor Vehicles

Bradford Booth
Deputy Chief of Legal Services
Rhode Island Division of Motor Vehicles

Brooklyn Wasser
Revenue Manager
Missouri Department of Revenue

Dominick Capotosto
Manager, Legal Affairs
Georgia Department of Revenue

Kevin Baird
Information Security Officer
Washington State Patrol

Marcy Klein
Manager
New Jersey Motor Vehicle Commission

Jeff Smith
Information Security Officer and Acting CIO
Georgia Department of Driver Services

Saundra Jack
Director, Data Management Services
Virginia Department of Motor Vehicles

Joe Mandala
Chief Information Officer
Kansas Bureau of Investigation

BOARD ADVISOR

Terri Egan
Executive Deputy Commissioner
New York Department of Motor Vehicles

AAMVA STAFF

Julie Knittle
Director, Member Services, Regions 3 & 4

Pierre Yves Boyer
Chief Information Security Officer

CONSULTANT

Brad Hanscom
Manager
BerryDunn Consulting

OUR VISION

Safe drivers
Safe vehicles
Secure identities
Saving lives!

American Association of Motor Vehicle Administrators
4401 Wilson Blvd, Suite 700
Arlington, Virginia 22203
703.522.4200 | **aamva.org**