911.gov

911 DataPath

Model Data Governance Agreements and Governance Structure

May 2023

The National 911 Program

is housed within the National Highway Traffic Safety Administration's Office of Emergency Medical Services at the U.S. Department of Transportation.

U.S. Department of Transportation
National Highway Traffic Safety Administration

About the National 911 Program

The National Highway Traffic Safety Administration (NHTSA) National 911 Program (Program), in the Office of Emergency Medical Services (OEMS) at the United States (U.S.) Department of Transportation (DOT), provides leadership and coordination of federal efforts that support 911 across the nation. A seamless interoperable 911 system-of-systems across the U.S. advances NHTSA's mission to eliminate fatalities, illness, and injuries from motor vehicle crashes and improve post-crash care.

The Program works with many stakeholders—including federal, state, local, tribal, and territorial (FSLTT) governments, technology vendors, public safety officials, and 911 professionals—toward a goal of advancing 911 that takes advantage of existing and emerging communications technologies, improving response times and information available to first responders prior to and during a 911 incident.

About this Document

Prepared: May 2023

Version #: 1

Table of Contents

Executive Summary

Management and delivery of 911 service have always been a local issue, which has resulted in a national landscape of siloed 911 systems that face difficulty when trying to interact or interoperate across multiple jurisdictions. Part of that landscape includes 911 data that varies widely from one jurisdiction to another. This challenge inhibits the 911 community's ability to collect, use, analyze, and share data and information, and can result in call transferring issues, inadequate resources, lag times in incident response, and other consequences. Everyone stands to benefit from more effective 911 data management and information sharing—callers, 911 agencies, and emergency responders as well as legislators who influence 911 policy to the various vendors that equip 911 systems. Most importantly, every United States (U.S.) resident and visitor has the most to gain. Through the ability to base administrative, operational, and technical decision-making on evidence-based factors, 911 systems across the U.S. will be able to respond to 911 requests more efficiently and effectively, and with greater accuracy, situational awareness, resilience, and consistent quality.

Data sharing is unique to each organization involved and will vary by the jurisdictional area and over-arching 911 legislation and rules in each state. This document is developed to provide options and examples that an organization can use within its needs and constraints to help document and provide data sharing.

This document describes the reasons for data sharing and outlines data-sharing documentation that can be used for the sharing of 911 data at multiple levels. There are several types of data-sharing relationships, which can vary widely from each organization, jurisdictional area, or data-sharing instance. Generally, they will fall into the following groups:

- Authoritative
- Cooperative
- Commercial
- Peer-to-peer

Several document types can be used to document a data-sharing agreement, including:

- Memorandum of Understanding (MOU)
- Memorandum of Agreement (MOA)
- Intergovernmental Agreement (IGA)
- Interlocal Agreement (ILA)
- Contract

Each is described herein and includes when they may be appropriate.

Appendix A contains an example MOU that can be used as a starting point.

Data sharing can also include a governance organization. Several types of organizations are described in this document to allow an organization to determine what may be appropriate for it. These types include:

- Formal Authoritative
- Formal Non-authoritative
- Informal

To help an organization begin the process, steps to develop a governance organization are provided herein.

1 Background

Past Issues

In the United States (U.S.), 911 was deployed locally, and public safety communications systems operated predominantly as standalone systems serving a particular geographic (and very local) area—and many still do. This created silos of authority and operations. 911 data is typically shared only within the local jurisdiction, inhibiting the larger 911 community's ability to collect, use, analyze, and share data and information, which often results in call transferring issues, inadequate resources, lag times in incident response, and other consequences that can affect first responder safety and response to a 911 call.

There have been attempts in the past to share data—with some successes but also some issues. For example:

> *A region agreed to load the member PSAP's data without an agreement between the regional governance structure and member PSAPs. The raw data was then shared with the state 911 office and the state assumed it could share the data. The question of data ownership, data sharing, and data usage had never been discussed among the member PSAPs that had agreed to share the data among themselves. There was no policy in place on who had rights to the data, who could share the data or what portions of the data, and how the data was to be used. The quality and validity of the data came into question—did the data elements mean the same thing to each member PSAP and were they all measuring and calculating the same information or data element the same way? None of these questions were discussed and worked out by the member PSAPs until "the cat was out of the bag."*
>
> *A state 911 office prepared a statewide GIS data set for the implementation of NG911 by collecting GIS data from PSAPs. Once the statewide dataset was developed other state agencies requested access to the data. The question of who owned the GIS data and who had rights to view it had to be addressed after the data collection effort started.*

Governance is not new in 911; many regions and states have a strong governance structure for 911 such as a 911 authority board or council of governments. Major law enforcement and fire chiefs, city managers, county commissioners, and county supervisors, for example, have oversight into the decisions made by public safety answering points (PSAPs), also known as emergency communications centers (ECCs), within a jurisdiction. This is valuable because PSAPs are not making decisions without the oversight of those held responsible—it is a quality check by elected officials.

Why is data sharing important?

Data sharing can provide many benefits such as the following:

Statistical analysis – More data allows PSAPs the opportunity to articulate their challenges and make the case for additional support. They can compare their call statistics to neighboring agencies to understand trends. They can use statistics to better understand their call processing times for specific 911 call types, the times of day that are busier to gauge staffing needs and trends, and the use of language translation services to seek funding for bilingual call-takers. More data allows PSAPs the opportunity to articulate challenges and make the case for support.

Set expectations – The data can help reduce unrealistic expectations from some in positions of authority or influences from outside forces that impose unrealistic expectations—having the data allows reasonable expectations to be set, including those from the community; thus, raising the bar and status within the community.

Situational awareness – Sharing data across a region can help explain what is being seen in a particular area or region. For example, a PSAP did not understand why it was receiving so many 911 calls from a neighboring PSAP, and a 911 call was transferred back six times. The call transfers could have been avoided if the PSAP understood that its neighboring PSAP had an active shooting incident and 911 calls were overloading that PSAP. Situational awareness can save lives and is important regionally as well as at the state level. A real-time regional dashboard would be helpful to provide insight as to what is happening across the region, and perhaps understand why calls are being routed the way they are.

Accountability and transparency – Increasing the ability of management and policymakers to translate data into meaningful reports for analysis, furthers informed decision-making. Sharing data discourages duplication of effort in data collection and encourages diverse thinking and collaboration. Sharing data also enables data from multiple sources to be combined for comparisons of jurisdictional boundaries.

2 Data-Sharing Relationships

Data-sharing relationships vary widely from each organization or instance, and will generally align with one of the following groups:

- **Authoritative** – The data-sharing organization has a statutory or regulatory authority to require cooperation and/or the mandatory reporting or sharing of data.
- **Cooperative** – A cooperative agreement or organization is developed between more than one PSAP or entity.
- **Commercial** – A commercial or non-profit organization develops a data-sharing environment and markets the solution to participants.
- **Peer-to-peer** – More than one organization determines they want to share data and enters into an agreement with other participants.

Regardless of the relationship the parties undertake, a governance document will assist participants in understanding the roles and responsibilities of each member organization and avoid misunderstandings such as sharing data with a third party.

3 Governance Documents

A data-sharing agreement is a formal document that clearly documents what data is being shared and how the data can be used. Such an agreement serves two purposes. First, it protects the agency providing the data, ensuring that the data will not be misused. Second, it prevents miscommunication on the part of the data provider and the receiving agency by assuring that any questions about data use are discussed. Before any data is shared, both the provider and receiver should discuss data-sharing and data-use issues and come to a collaborative understanding that will be documented in a data-sharing agreement.

It is important to recognize that the process for entering a data-sharing agreement varies from organization to organization as does the type of data being shared and the agencies sharing the data.

These documents may vary between organizations based on several things:

- Relationship of the parties
- Authority of the parties
- Jurisdiction of the parties

Some types of documents that may be used based on the parties' needs include:

- Memorandum of Agreement (MOA)
- Memorandum of Understanding MOU)
- Intergovernmental Agreement (IGA)
- Interlocal Agreement (ILA)
- Contract

Memorandum of Agreement

An MOA is a written document describing a cooperative relationship between two parties wishing to work together on a project or to meet an agreed-upon objective. An MOA serves as a legal document and describes the terms and details of the partnership. An MOA is more formal than a verbal agreement but less formal than a contract. Organizations can use an MOA to establish and outline collaborative agreements, including service partnerships or agreements to provide technical assistance and training. An MOA may be used regardless of whether money is to be exchanged as part of the agreement.

MOAs are typically "conditional agreements" between two or more parties where the transfer of funds for services may be anticipated. The MOA is prepared in advance of a support agreement/reimbursable order form that defines the support, the basis for reimbursement, the billing and payment process, and other terms and conditions of the agreement. MOAs often establish common legal terms that will be read into every reimbursable order that follows. MOAs do not obligate any funds themselves, but they establish the terms for future service and cite one of the appropriate authorities to do so.

Memorandum of Understanding

If your agency is in the beginning stages of a transaction with another party, an MOU is often the first step toward a formal agreement, defining how the parties will work together and recognizing each one's expectations and responsibilities. An MOU is an agreement between two parties outlined in a formal document and may not be legally binding. It may be used to indicate the parties' commitment to move forward with negotiations in cases where the MOU defines the scope and purpose of the discussions but does not provide more specific requirements.

MOUs can establish a paper trail and keep negotiations moving forward as each party has an opportunity to review the terms of the agreement, resolve any disputes or miscommunications, and make changes to the agreement before signing a contract.

Intergovernmental Agreement

When a grant program requires services between or among a state entity and a local entity (agency or procurement unit) exercising joint powers, an IGA may be the most efficient funding instrument. An IGA is a contract between two or more public agencies or public procurement units for services or the joint exercise of any powers common to the agencies.

Except for the right to a joint exercise of powers granted in state statutes, no additional authority or power is conferred upon any public agency by way of the statutes controlling IGAs.

Since IGAs typically involve the joint exercise of powers common to the contracting public agencies, when two public agencies enter an agreement for joint action, each agency must have the power to perform the action contemplated in the contract. Therefore, where there is no joint exercise of powers common to the public agencies involved, there is no IGA and the statutory requirements of such do not apply.

Interlocal Agreement

An ILA is a written contract between local government agencies such as a city, a county, or a constitutional office. An ILA is used when an authority or district is performing for or receiving a service from a local governmental entity. Any time a public service involves the joint operations and budgets of two or more local government agencies, an ILA must be drafted and approved by all sides, with each government's governing body enacting the agreement by vote. Typically, ILAs require board approval.

Contract

A contract is an agreement between two parties that creates an obligation to perform (or not perform) a particular duty. Understanding the required elements of a contract helps create valid agreements. With a valid agreement, parties can mitigate legal liability. To make a contract lawful, one must:

- Identify all parties involved
- Present an offer of value
- Confirm acceptance of the offer by the other party

- Ensure all parties are authorized to sign the contract
- Have mutuality (understanding) and agreement to the basic substance and terms
- Create a dispute resolution clause if the transaction deteriorates

With proof that all these elements occurred, a party meets its burden of establishing the legally required rebuttable presumption that a contract existed. The agreement may be used to enforce one's rights and hold the other party legally accountable.

The sections below outline considerations for the development of an intergovernmental cooperative agreement (ICA) or MOU for data sharing between agencies. This is intended to be a guide for writing an ICA or MOU. The document is outlined in a recommended structure with suggested headings for each section of the Agreement. The sections can be used or not based on the type of sharing and local laws. A legal review should occur to ensure all sections required locally are included and those not permitted are excluded.

3.1 Introductory Section

The Introduction section is a simple explanation of the Agreement and why it is necessary. It describes the purpose of the Agreement, names the parties to the Agreement, and describes why it is important/useful to work together in the manner outlined in the Agreement. It does not need to include details about past efforts or discuss how the parties reached this level of agreement.

3.1.1 Parties

The parties should be listed as legal entities with the common names that will be used throughout the document.

3.1.2 Parties' Authority

The authority to be parties to the document should be described, including the authority to enter into the agreement as well as the authority to share or not share data.

3.1.3 Purpose

The reason for the data exchange and why it is important should be identified. Examples are provided below (items in brackets, but not limited to, can be individualized).

> *Exchanging operational data as defined in the [XYZ Data Dictionary] is critical to the [operations, staffing, and funding] of 911 in My State. The sharing of this data to [the My State Board] monthly will be accomplished using [My State's] data-sharing environment.*
>
> *The exchange of incident data from and to the computer-aided dispatch (CAD) systems of the parties to this agreement will improve the ability of all parties to provide mutual-aid responses and protect the public.*

Implementation of this Agreement is intended to enhance and foster the exchange of [X data], assist in decision-making, and improve [X].

3.2 Definitions

The terms and phrases used within the document that need to be defined should be listed.

3.3 Roles and Responsibilities

The roles and responsibilities of the participants and staff that may have access to the shared data should be clearly defined and documented. It is important to include sufficient detail to provide guidance and instruction regarding who is responsible for what. This might include general statements about system(s), administration, updates, financial obligations, operations, maintenance, upgrades, and data management. Anything specific to this Agreement should be touched upon in the Roles and Responsibilities section.

The following list of roles is informative for a data-sharing Agreement and should be considered; not all roles are needed for every situation. Some roles could be performed using algorithms and technology.

Data Owner/Source	The source of the data is the agency or manager that is responsible for providing the data to the environment. This may include ownership of the data or only delivery.
Data Custodian/Administrator	The data custodian is responsible for the management of the systems used to receive, store, merge, and analyze the data. In many cases, if other roles are not defined, the administrator may be required to take on those roles.
Data User	There may be multiple user levels (e.g., those with access to the raw data or those with access to reports only). If the data is contemplated to be shared with third parties such as academic, state, or national organizations, a third-party user should be defined. It is important to define what each user type can see and do with the data.
Data Security Officer	The data security officer is responsible for the security of the data in motion and at rest. They should also develop, train, test, and enforce security policies and procedures.
Data Privacy Officer	Some states require a privacy officer. This may be an already appointed role in the agency or a new role for data sharing. This role develops, trains, tests, and enforces privacy policies and procedures.
Data Quality Officer	This role, in part, may be performed by the technology. This role develops, trains, tests, and enforces data quality policies and procedures.

3.4 Data and Services

The Data and Services section defines the data being shared, the methods of exchange, and the services to exchange, store, and analyze the data.

- **Data** – Define the specific data elements, labels, and tags of other labels or formats. This can be defined in the document or point to a specific version of a separate data dictionary.

  - Define how local data elements will be translated to a standard data element to allow comparison. (e.g., incident type code to the national standard).

- **Exchange** – Define the method used to transport or allow access to individual systems to permit data sharing.
  - Identify the way data will be transferred from the source to the custodian.
  - Will data be transferred physically or electronically?
  - Is the data encrypted?
  - If data is to be sent over the internet, how can a secure connection be guaranteed?
- **Storage** – Define the systems and locations where the data can be stored.
- **Intended use and constraints of data** – Define the valid uses of the data.
  - List any restrictions on how the data or data findings can be used.
  - Is the custodian required to document how the data is used?
  - Can the custodian or user share, publish, or disseminate data findings and reports without the review of the source/owner?
  - Can the custodian or user share, sell, or distribute data findings or any part of the database to another agency?
- **Analysis of data**– Define the authorized use of the data.
  - Define what examinations are allowed.
  - Define ownership of the analysis results. (Is it the same as the source data?)
  - Is artificial intelligence (AI) or machine learning permitted to be used with the data?
    - Is bias testing required? If so, what type?
- **Timeframe** – Define the timing for when and how often data is shared.
  - How long will the data remain available?
  - Do records retention rules apply to the data?
- **Privacy** – Define privacy requirements, including for data storage and handling.
  - How does the Freedom of Information Act (FOIA) or open records rules impact the data?
  - Describe the required processes that the custodian must use to ensure data remains confidential.
  - Because some data may contain information linked to individuals, it is important to have safeguards to ensure that sensitive information remains private.

        - Personal data should remain confidential and should not be disclosed verbally or in writing to an unauthorized third party, by accident or otherwise.
        - Will the custodian or user report information that identifies individuals?
    - What safeguards are in place to prevent sensitive information from becoming public?
- **Security** – Define the security, encryption, access control, logging, and auditing requirements.
    - Describe the methods that the custodian must use to maintain data security.
    - Will everyone at the custodian agency have the same level of access to data, or will some people have restricted access?
    - What password protections need to be in place?
    - Who will have physical access to the data, including the servers and paper files?
    - What will happen to the data after the data-sharing period ends?
    - Address what happens in the event of a cyber breach and data is compromised.
        - Are the parties required to have a cybersecurity policy? Or a policy for handling breaches?
- **Insurance** – Detail the need (or not) for insurance.
    - Is cyber insurance required? If so, does the system provide?
    - How are the costs appropriated to users?
- **Identifiable data** – Define how identifiable data can be used or removed to permit data use.
- **Ownership/custodial relationship** – Define the ownership or custodial relationship of the data between the parties.
- **Extended use** – Define additional data uses beyond the basic intent of the document. Define the process to permit the extended use of the data by the parties to the document or third parties.

3.5 Terms of Document

Each document should have defined terms of the document.

- **Effective date** – Define when the document is effective (e.g., on signature, at the time of the first data exchange).
- **Period of performance** – Define how long the document is effective.
- **Extension of period of performance/renewal** – Will the period of performance automatically extend? If not, what process must be followed to extend it?

- **Suspension** – Define the circumstances that will suspend a party from participating in the data-sharing environment.
    - Misuse of data – Keep the definition broad in the Agreement but address the specifics of what is considered misuse by parties in policies or bylaws/rules.
    - Quality of the data
    - Lack of participation
- **Termination** – Define the process for a party to terminate their participation or the group to terminate the participation of another party.
    - What is the impact to the data shared?
    - Will the party no longer have the right to use the data?
    - Will the data be returned to the owner/source, or will it be destroyed (deleted from hard drives, shredded, etc.)?
    - Will any funds be refunded or forfeited?
    - What is the due process for participants?

3.6 Costs

The Costs section describes the costs and how they will be distributed among participants. Even if there are no user fees, the costs should be clearly defined. In some cases, each agency may be responsible for its incurred costs; however, this should still be documented.

The monetary costs of sharing the data should be clarified. For example. Will there be expenses related to sharing the data? Will the provider or the receiver share the costs, or will one agency pay for all data-sharing expenses?

- **Fee** – If fees are used to support the system, define the fees and timeframes for payment.
- **Hardware, software, and hosting costs** – Define how the costs are distributed or which party will cover the costs.
- **Staffing costs** – Define the costs for staff to submit, manage, and use the data and which party will be responsible for them (e.g., each party their own costs, an organization, or grants).
- **Cost modifications** – Define the process for changing the cost allocation, fees, and other costs.
- **Cost formula or basis for determining costs** – Identify how costs are determined within an exhibit of the Agreement, making it easier for changes to be made.

3.7 Terms and Conditions

The Terms and Conditions section contains the legal language required for the document. This is frequently referred to as boilerplate language as many organizations have a fixed format or language. These will vary by the type of document and the parties to the document.

- **Entire agreement** – Define that this is the entire agreement. Include language that no other agreements, verbal or written, are enforceable.
- **Relationship of the parties** – Define the relationship between the parties. Define that each party is a separate entity and not an employee, partner, or agent of the other(s); this will vary by the type of document.
- **Severability** – Provides notice that the agreement shall remain in force even if a part is found to be invalid.
- **Force majeure** – Excuses parties from liability or obligation when an extraordinary event outside of their control occurs.
- **Governing law** – Determines which law shall apply in the event of a dispute.
- **Assignment and binding effect** – Define the parties the document is binding on and the impact of transfer and/or assignment of the document to other parties.
- **Venue and jurisdiction** – Define the court where any legal actions will be handled.
- **Review, amendment, and modification process** – Define the process of reviewing the document and how to make changes. Explain if edits replace or incorporate into the document.
- **Notices** – Define the responsible parties to send/receive notices, updates, and other communications regarding the document and the methods for communication.
- **Signature page** – The part of the document that the parties sign to make the document valid. Include witnesses or notary marks as required by the jurisdiction.

4 Policies and Procedures

In addition to the governance documents, many functions and activities can be documented with policies and procedures. The Policy section describes the specific practices, procedures, methods, and standards to be followed by all parties to the Agreement. These can be referenced in the governance documents for the record, or used separately. The use of policies and procedures allows for changes without the formal legal agreement processes of the governance documents.

Topics to be addressed may include:

- Standards or procedures to be applied and followed
- Change notification procedures
- How changes that impact the parties or systems will be made
- Recordkeeping and reporting requirements
- How notification to the parties of changes or modifications will occur

5 Governance Organizations

Local governance is a key component for data-sharing success and is often overlooked until a problem occurs. Good governance encourages better decision-making and the efficient use of resources and strengthens accountability. It builds collaboration and coordination between organizations. However, governance can be challenging due to the number of members and their divergent interests and concerns, and the variety of stakeholders involved (law enforcement, fire, emergency medical services [EMS], information technology [IT], 911, and others).

Governance allows stakeholders to:

- Establish lines of authority
- Provide an effective means of communication
- Establish policies and procedures
- Manage system changes or issues
- Establish fiscal responsibility
- Mitigate risk
- Encourage change and break down barriers to data sharing
- Overcome political barriers
- Clarify jurisdictional boundaries

To be effective, there must be a clearly defined vision and mission to assist leadership in the decision-making process. Policies, procedures, and processes need to be defined and enforced, and finances, risk, and change must be carefully managed.

A governance structure can range from an existing multi-functional governance structure that adds data sharing as part of its responsibility, to a standalone cooperative organization with the specific purpose of data sharing. For example, an existing regional emergency communications board can create a specific data-sharing committee that establishes policies and procedures and makes recommendations to the existing board, or an informal committee can be created between a group of PSAPs specifically to support data sharing among that group without being defined in statute or regulation.

5.1 Governance Structures

Different types of governance structures can be used to manage various functions. Data sharing among several entities will benefit from a governance structure of some type. This structure can range from an informal committee made up of those sharing the data that develops policies on what and how data can be shared to a more formal governance organization focused on the proper function and protection of the data.

Governance committees and organizations can be categorized by the method used to create the organization and the authority that the organization has.

Formal Authoritative	A formal authoritative governance organization is created by statute, regulation, or contract and includes the authority to define and enforce the rules and procedures for data sharing.
Formal Non-Authoritative	A formal non-authoritative governance organization is created by statute, regulation, or contract but does not include the authority to define and enforce the rules and procedures for data sharing. These are usually advisory in nature to an authoritative organization or person.
Informal	An informal governance organization is a group that is developed to fill a need for standardization and effective operation of data sharing. This type is not defined by statute, regulation, or contract. These organizations do not have actual authority but frequently lead the data-sharing effort.

Regardless of the type of governance selected, all stakeholders should be represented through the various committees, subcommittees, and positions in the governance framework, and must be fully engaged in the governance process.

5.2 Building a Governance Organization

Setting up an informal or formal governance structure or an oversight organization can be accomplished in several ways. There are available studies and detailed information on what elements are required to create a solid governance organization. Before setting up a special governance organization, consult any relevant state statutes. Some general steps that can guide the new organization are identified below:

Set the vision for the data-sharing governance

Establishing the need for a governance organization is the first step. This will guide how the governance organization is set up as well as the long-term operation of the organization. Clearly define the goals and objectives of the governance organization and data sharing among the partners.

Identify the participants and representatives

Gather an active, balanced, and accountable membership. Align the membership with the needs and priorities of the group that engages in and is impacted by data sharing. Document membership requirements and identify the roles and responsibilities of the participants and the entities they represent. Routinely assess if the requirements are being met by each participant and that their participation is sanctioned by the entity they represent. Determine how member attrition is handled and how jurisdictional differences are managed.

Establish organization documents, committees, and subcommittees

Once the organization has defined the why and who should be engaged, the next step is to determine the how. Some tasks included are:

- **Charter with bylaws** – Frequently referred to as articles of incorporation, a charter brings the organization into existence as a legal entity. Bylaws are also legal documents, but they set up

the internal structure and rules of the organization (i.e., the framework for internal governance and day-to-day operations).

- **Committees or subcommittees** – Set up temporary or permanent committees or subcommittees.
- **Policies and procedures** – Develop the policies and procedures necessary to operate the organization.
- **Funding** – Determine funding needs and sources.

Establish data sharing and policies that achieve goals set in the governance vision

With the organization identified, data-sharing systems are implemented and data sharing and its use can begin.

- Identify data stewards and owners within each participating entity.
- Educate stewards and the organization about data governance.
- Implement systems policies and procedures to share data.

Maintain and store data

Maintain the organization, systems, policies, and procedures of data sharing. This should include a regular review of all documents and data to keep them up to date. It is also important to ensure there is a cybersecurity policy in place to protect the data.

Appendix A: Model Agreement

The following pages provide a template of a sample MOU.

911 DATAPATH

DATA AND INFORMATION SHARING PROCEDURES

MEMORANDUM OF UNDERSTANDING (MOU)

The introduction section of the MOU helps the reader understand the agreement subject matter. This section should be a simple explanation of the agreement and why it is necessary. This section does not need to include details about past efforts or discuss how the agencies reached this level of agreement.

The **[INSERT PARTY A's Board/Commission/Authority HERE]** of **[INSERT PARTY A's NAME HERE]** and the **[INSERT PARTY B's Board/Commission/Authority HERE]** of **[INSERT PARTY B's NAME HERE]** have entered into this Memorandum of Understanding (MOU) pursuant to a framework established between **[INSERT PARTY A's NAME HERE] ([INSERT PARTY A's ACRONYM HERE])** and **[INSERT PARTY B's NAME HERE] ([INSERT PARTY B's ACRONYM HERE])** (hereinafter the "Parties") to share and process data to meet the needs of the region's public safety.

Data sharing is the process of making data available to others. Data sharing is a way to optimize higher-relevant data, generating more robust data and analytics to solve business challenges and meet enterprise goals. This MOU authorizes and directs the **[INSERT PARTY A's AUTHORITY TITLE HERE]** of **[STATE/REGION's NAME HERE]** and the **[INSERT PARTY B's AUTHORITY TITLE HERE]** of **[INSERT PARTY B's NAME HERE]** to enter a Data and Information Sharing Procedures Memorandum of Understanding (hereinafter referred to as "Data and Information Sharing MOU") to establish procedures for sharing and processing data.

The headings contained in this Data and Information Sharing MOU are for convenience of reference only and shall not affect in any way the meaning or interpretation of this Data and Information Sharing MOU. As the 911 centric name for dispatch centers, public safety answering point (PSAP) and emergency communications center (ECC) may be used interchangeably throughout this Data and Information Sharing MOU to describe the centers that answer and/or dispatch 911 calls.

This Data and Information Sharing MOU is not intended to define parameters, components, or technical architectures of 911 data and/or an information system, or to define specific data elements that should or would be collected. This is not a technical document, and while this Data and Information Sharing MOU may contain references to other similar initiatives and relevant tools, it does not intend to identify any specific effort or resource as "the model" for **[the Region's]** PSAPs. Additionally, this Data and Information Sharing MOU is not intended to replace or conflict with ongoing activities of organizations such as the Association of Public-Safety Communications Officials (APCO) International, the National Emergency Number Association (NENA), and the National Association of State 911 Administrators (NASNA).

I. DEFINITIONS

Word, phrase, and/or acronym – A statement of the meaning of a word or word group.

A data dictionary would also be appropriate in this section, published with all elements of call data using NENA standards; references; and/or checklists, which will allow more flexibility any time an element change is needed.

[Word/Phrase] – [Definition language].

II. ROLES AND RESPONSIBILITIES

Parties shall determine the intended use: how the provider will distribute the data and how the receiver will use the data.

Sharing data between the parties shall encourage accountability and transparency, enabling PSAPs and ECCs to validate one another's information; combine data to allow for comparisons that cross regional and departmental lines; encourage diverse thinking and collaboration; and prevent miscommunication by making certain the provider of the data and the receiver of the data understand data-use considerations and come to a collective understanding recognized by this Agreement.

Parties agree there are no restrictions on how the data or data findings can be used if written disclosure of usage is made beforehand. The receiver shall document how the data is used. The receiver may share, publish, or disseminate data findings and reports without the review of the provider, including distribution to **another** agency (third party) with the provider's identifiable information.

III. DATA AND SERVICES

Data services—sometimes described as Data-as-a-Service (DAAS)—generally refer to independent functions that enhance, organize, share, or calculate information collected and saved in data storage volumes.

A. Data – specific data elements may include **[labels, tags of other labels or formats including numbers, characters, time, and/or boolean].**
B. Exchange – the method used to transport or allow access to individual systems to permit the sharing of the data will be **[data encrypted using Secure Sockets Layer (SSL) and/or military-grade encryption**; **an email when receiver opens their file; will not require special software to install; may use a web browser such as Chrome, Internet Explorer or Firefox; ensure ability to bypass firewall and email attachment restrictions that often prevent sending or receiving files; and/or will exclude third-party storage providers. If physically sending data by mail or parcel carrier, the data should be encrypted using an encryption method, such as Pretty Good Privacy (PGP), which allows encryption of the data to a**

specific person's key].

C. Storage – the systems and locations that the data shall be stored include **[cloud storage, cloud backup, Universal Serial Bus (USB) flash drive, and/or optical media storage].**

D. Timeframe – data will be shared by the provider at **[quarterly intervals, not to exceed one fulfillment every ninety (90) days. Data may also be shared by written request from the receiver with a fifteen (15) business day fulfillment expectation. The data will remain available for three (3) calendar years. No extended use is permitted without written permission. Records retention rules will not apply to the shared data].**

E. Security – to maintain data security, both parties will possess cybersecurity protections. The receiving agency will **[have differing levels of access to data, which shall include restricted access; password protections are required to be applied; only Deputies/Sheriffs and PSAP Supervisors ("Data Custodians") will have physical access to the data, servers and paper files; after the data-sharing period ends, the receiving party will return or destroy the data ensuring that the data cannot be recovered and used for unauthorized purposes or employ a data destruction method including overwriting the current data with random data until the current data can no longer be retrieved].**

The categories of data will be separated and listed for selection.

[CALL DATA]

- ☐ 911 voice
- ☐ 911 text
- ☐ 10-digit emergency
- ☐ 10-digit non-emergency/administrative (admin)
- ☐ Alarms
- ☐ Images/Video to 911

[INCIDENT DATA]

- ☐ 911 voice
- ☐ 911 text
- ☐ 10-digit emergency
- ☐ 10-digit non-emergency/admin
- ☐ Alarms
- ☐ Images/Video to 911

[HISTORY DATA]

- ☐ 911 voice
- ☐ 911 text
- ☐ 10-digit emergency
- ☐ 10-digit non-emergency/admin
- ☐ Alarms

☐ Images/Video to 911

[GEOGRAPHIC INFORMATION SYSTEM (GIS) DATA]

☐ PSAP boundaries, provisioning boundaries, emergency service boundaries (ESBs), police/fire/emergency medical services (EMS) boundaries, address points, road centerlines, and site/structure address points (SSAP)

☐ Full master street address guide (MSAG) and automatic location identification (ALI) extract records and source information whether automatically or manually retrieved for comparison of the road centerlines with the provided GIS, ALI, and MSAG data based on NENA 71-501 and NENA 02-014 standards

[OPERATIONAL/STAFFING DATA]

☐ Average number of **[911 specialists, call-takers, and/or dispatchers]** per shift

☐ Average number of **[supervisors, trainers, technicians, and/or Quality Assurance (QA)]** per shift

IV. TERMS AND CONDITIONS

Standard (written) terms and conditions (T&Cs) are the legal basis on which parties will be engaging with each other.

1) Compliance with Laws. Each party will comply with all applicable laws and regulations and with all applicable orders issued by courts or other governmental bodies of competent authority.
2) Force Majeure. Except for payment of amounts due, neither party will be liable for any delay, failure in performance, loss or damage due to fire, explosion, cable cuts, power blackout, earthquake, flood, strike, embargo, labor disputes, acts of civil or military authority, war, terrorism, acts of God, acts of a public enemy, acts or omissions of carriers or suppliers, acts of regulatory or governmental agencies including the declaration of a public health emergency or other causes beyond such party's reasonable control.
3) Governing Law. This Data and Information Sharing MOU will be governed by the law of **[State],** without regard to its conflict of law principles, unless a regulatory agency with authority over the applicable Service applies a different law. The United Nations Convention on Contracts for International Sale of Goods will not apply.
4) Independent Entity. Each party is an independent entity. Neither party controls the other, and neither party nor its affiliates, employees, agents, or contractors are affiliates, employees, agents, or contractors of the other party.
5) Injunctive Relief. Nothing in this Data and Information Sharing MOU is intended to or should be construed to prohibit a party from seeking preliminary or permanent injunctive relief in appropriate circumstances from a court of competent authority.

6) Legal Action. Any legal action arising in connection with this Data and Information Sharing MOU must be filed within two (2) years after the cause of action accrues, or it will be deemed time-barred and waived. The parties waive any statute of limitations to the contrary.

7) No Third-Party Beneficiaries. This Data and Information Sharing MOU is for the benefit of **[INSERT PARTY A's ACRONYM HERE] and [INSERT PARTY B's ACRONYM HERE]** and does not provide any third party (including evaluators) the right to enforce it or to bring an action for any remedy, claim, liability, reimbursement, or cause of action or any other right or privilege.

8) Notices. Any required notices under this Data and Information Sharing MOU shall be in writing and shall be deemed validly delivered if made by hand (in which case delivery will be deemed to have been effected immediately), or by overnight mail (in which case delivery will be deemed to have been effected one (1) business day after the date of mailing), or by first class pre-paid post (in which case delivery will be deemed to have been effected five (5) days after the date of posting), or by facsimile or electronic transmission (in which case delivery will be deemed to have been effected on the day the transmission was sent). Any such notice shall be sent to the office of the recipient set forth on the cover page of this MOU or to such other office or recipient as designated in writing from time to time.

9) Publicity. Neither party may issue any public statements or announcements relating to the terms of this Data and Information Sharing MOU or to the provision of Services without the prior written consent of the other party.

10) Severability. If any portion of this Data and Information Sharing MOU is found to be invalid or unenforceable or if, notwithstanding (Governing Law), applicable law mandates a different interpretation or result, the remaining provisions will remain in effect and the parties will negotiate in good faith to substitute for such invalid, illegal, or unenforceable provision a mutually acceptable provision consistent with the original intention of the parties.

11) Survival. The respective obligations of **[INSERT PARTY A's ACRONYM HERE] and [INSERT PARTY B's ACRONYM HERE]** that by their nature would continue beyond the termination or expiration of this Data and Information Sharing MOU, including the obligations set forth in Confidentiality, will survive such termination or expiration.

V. CONFIDENTIALITY

The confidentiality section (also known as the privacy section) is used to define the protection of sensitive information. Clearly describe what information is confidential, outline the permitted uses for the information, and record the receiving party's promise to abide by the agreement.

1) It is understood that the above authorizations include the sharing of information between the Parties for purposes of the authorization granted, and that such information provided to **[Party B]** on **[Party A's]** behalf may be Customer Proprietary Network Information (CPNI) even if CPNI is not expressly requested, or Confidential Information (as defined in **[Region's]** relevant service agreement(s) with Wireless Service Provider(s), Data Provider(s) and/or Provider(s) of Call

Aggregation [Services]), as well as unique usernames and passwords needed to access that information.

2) **[Party A]** represents that **[Party B]** is bound by an agreement with **[Region]** to (i) keep confidential any information received on its behalf, which agreement is at least as restrictive as the confidentiality obligations of **[Party A]** under its agreement(s) with Wireless Service Provider(s), Data Provider(s) and/or Provider(s) of Call Aggregation (Services) for the services to which the received information relates, exercising at least the same degree of care as it uses with its own data and confidential information, but in no event, less than reasonable care, to protect information from misuse and unauthorized access or disclosure, and (ii) limit the information received on its behalf by **[Party B])** to only those individuals with a need to know, and under a duty of confidentiality, in order to accomplish the purposes of this Data and Information Sharing MOU on **[Region's]** behalf. If such agreement does not expressly permit **[Party B]** to enforce such agreement as a third-party beneficiary, then **[Region]** is responsible for any use or disclosure of the said information.

VI. UPDATES, AMENDMENTS, AND WAIVERS

This section will address routine assessment of the document and any alteration of addition to, or change(s) made, even by correction. A waiver of contract can occur if either party deliberately fails to take certain actions or takes a positive act to waive a term of the agreement. To constitute a legal release or waiver of a right, the action must be intentional and voluntary.

The Parties agree to review this Data and Information Sharing MOU on a **[bi-annual]** basis, at a minimum, to update any processes or understandings.

The Parties acknowledge that any modifications must be by mutual consent, in writing, with as advanced notice as possible considering the circumstances, and will be treated as an amendment to this Data and Information Sharing MOU being signed by authorized representatives of both parties. A waiver by either party of any breach of this Data and Information Sharing MOU will not operate as a waiver of any other breach of this Agreement.

VII. LIABILITIES

Issues of liability involve liability between the parties as well as liability to third parties, noting that these issues can be complex and should be discussed with counsel as to how best to structure liability provisions that work for a party.

VIII. COSTS

The costs section will describe the cost and distribution. Even if there is no fee for the receivers, the cost of each agency is assumed by the respective agency, or a grant is being applied, this should still be documented. Determine the formula of cost or basis for determining costs within an exhibit (attachment) to make changes easier.

Both **[INSERT PARTY A's ACRONYM HERE]** and **[INSERT PARTY B's ACRONYM HERE]** agree to **[bear their own costs, if any,]** for:

- Fees/charges used to support the system
- Hardware, software, and hosting expenses
- Staffing rates to request, analyze, and/or manage the data

IX. ENTIRE AGREEMENT

The purpose of the agreement clauses is to lessen the chances of a dispute relating to agreements preceding the current arrangement. They also clarify that the document is considered the complete agreement made by and between the parties.

Entire Agreement. This Data and Information Sharing MOU constitutes the entire agreement between the parties with respect to its subject matter. This Data and Information Sharing MOU supersedes all other agreements, proposals, representations, statements, and understandings, whether written or oral, concerning the Services or the rights and obligations relating to the Services, and the parties disclaim any reliance thereon. This Data and Information Sharing MOU will not be modified or supplemented by any written or oral statements, proposals, representations, advertisements, service descriptions, or purchase order forms not expressly set forth in this Data and Information Sharing MOU.

X. EFFECTIVE DATES

This is the date agreed upon by the parties for beginning the period of performance under the agreement. In no case shall the effective date precede the date on which the designated authority signs the document.

This Data and Information Sharing MOU shall take effect upon its signing by authorized representatives of each party.

Signatures:

[INSERT PARTY A's NAME HERE]

_____ Date: _____

By: _____

Title: _____

[INSERT PARTY B's NAME HERE]

_____ Date: _____

By: _____

Title: _____

Acronym Dictionary

Some definitions provided are from NENA's Master Glossary.[1]

Acronym	Term	Definition
AI	Artificial Intelligence	The ability of a computer program or a machine to perform tasks commonly associated with intelligent beings.
ALI	Automatic Location Identification	Tabular reference for the current 911 system. Defines destination PSAP for every landline telephone number and cellular tower.
APCO	Association of Public-Safety Communications Officials	APCO (Association of Public Safety Communications Officials) is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications.
CAD	Computer-Aided Dispatch	A computer-based system that aids PSAP telecommunicators by automating selected dispatching and record-keeping activities.
COOP	Continuity of Operations Planning	A plan to implement continuity of operations to ensure that primary mission essential functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.
CPNI	Customer Proprietary Network Information	Information that telecommunications services, such as local, long-distance, and wireless telephone companies, acquire about their subscribers.
DAAS	Data-as-a-Service	A web-based data collection, delivery, storage, and analytics solution.
ECC	Emergency Communications Center	ECC is a facility designated to receive and process requests for emergency assistance, which may include 9-1-1 calls, determine the appropriate emergency response based on available resources, and coordinate the emergency response according to a specific operational policy.
EMS	Emergency Medical Services	EMS is a service providing out-of-hospital acute care and transport to definitive care, to patients with illnesses and injuries which the patient believes constitute a medical emergency.
FOIA	Freedom of Information Act	Generally provides that any person has the right to request access to federal agency records or information except to the extent the records are protected from disclosure.
GIS	Geographic Information System	A system for capturing, storing, displaying, analyzing, and managing data and associated attributes which are spatially referenced.
ICA	Intergovernmental Cooperative Agreement	An agreement between or among two or more local governments for achieving common goals, providing a service or solving a mutual problem.
IGA	Intergovernmental Agreement	A contract between two or more public agencies or public procurement units for services or the joint exercise of any powers common to the agencies.

[1] https://kb.nena.org/wiki/Category:Glossary

Acronym	Term	Definition
ILA	Interlocal Agreement	An agreement among governmental jurisdictions or privately owned systems, or both, within a specified area to share 911 system costs, maintenance responsibilities, and other considerations.
IT	Information Technology	The use of any computers, storage, networking, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data.
MOA	Memorandum of Agreement	A document written between parties to cooperatively work together on an agreed upon project or meet an agreed upon objective.
MOU	Memorandum of Understanding	An agreement between two or more parties outlined in a formal document that defines expectations and responsibilities of the parties.
MSAG	Master Street Address Guide	Tabular reference for address validation in the current 911 system. Defines all possible addresses within a jurisdiction.
NASNA	National Association of State 911 Administrators	NASNA is the voice of the states on public policy issues impacting 911. State 911 leaders' expertise can assist industry associations, public policymakers, the private sector, and emergency communications professionals at all levels of government as they address complex issues surrounding the evolution of emergency communications. An association that represents state 911 programs in the field of emergency communications.
NENA	National Emergency Number Association	Standards body for 911 and NG911.
NHTSA	National Highway Traffic Safety Administration	The Federal Government agency tasked with transportation-related education, research, safety standards, and enforcement. Is also the home of the National 911 Program, under its Office of Emergency Medical Services.
OEMS	Office of Emergency Medical Services	The Office of Emergency Medical Services (OEMS) is responsible for planning and coordinating an effective and efficient statewide EMS system
PSAP	Public Safety Answering Point	The entity responsible for receiving 911 calls and processing those calls according to a specific operational policy.
RMS	Records Management System	Public safety RMS are often interfaced to public safety communication centers. RMSs are sometimes accessed directly through computer systems deployed within communication centers for research and analysis purposes.
SSL	Secure Sockets Layer	A computer networking protocol that manages server authentication, client authentication, and encrypted communication between servers and clients.
SLA	Service Level Agreement	A contract between a service provider and the end user that defines the level of service expected from the service provider.
SOP	Standard Operating Procedure	A written directive that provides instruction for conducting an activity.
USDOT	U.S. Department of Transportation	The top priorities at DOT are to keep the traveling public safe and secure, increase their mobility, and have our transportation system contribute to the nation's economic growth.