Public Safety Data Sharing Recommendations and Best Practices

March 20, 2020

Gordy Coles
UCA Interoperability Director
Utah FirstNet SPOC/SWIC

UCA
UTAH COMMUNICATIONS AUTHORITY

This presentation was prepared by SAIC under contract with the Utah Communications Authority using funds under award 49-10-S18049 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, UCA, or FirstNet.

Public Safety Data Sharing Topics

- Data Sharing Best Practices – What You Can Do
- Governance Agreements – Recommendations for Leaders
- How to Get Started
- Planning for Data Integration Challenges
- Ensuring Comprehensive Data Sharing Policies
- Moving Up the Data Interoperability Continuum
- A Public Safety Data Sharing Bibliography

UCA
UTAH COMMUNICATIONS AUTHORITY

Data Sharing Best Practices – What You Can Do

UTAH COMMUNICATIONS AUTHORITY

Source: NIST Public Safety Communications Research (PSCR)

Improving Your Agency's Data Sharing – What You Can Do

1. **Develop inter-agency data sharing partnerships.** Build inter-agency commissions, task forces, working groups, etc., charged with identifying the agencies' collective data sharing interoperability goals, model use cases, requirements, and benchmarks of success. These bodies can build the foundation for a public safety-wide data sharing strategy.
2. **Make the case for investments in data sharing.** Leverage existing monitoring and evaluation data to analyze agency data use and data sharing patterns. Agency leaders can use such analyses to make evidence-based arguments regarding future investments in data sharing resources.
3. **Leverage Request for Proposal (RFP) requirements.** Be as specific as possible in RFP and contract language about the interoperability requirements and specifications of data sharing technologies, including data exchange standards where appropriate. Reference guidance from relevant bodies such as SAFECOM and the National 911 Program.
4. **Collaborate with the broader public safety community.** Extend the influence and knowledge base of regional task forces by engaging with national and international public safety entities, including state and federal bodies, practitioner organizations, research groups, industry groups, standards developing organizations, and others.
5. **Participate in Identity, Credentialing, and Access Management (ICAM) solution development.** Provide practitioner expertise on features and requirements for the SAFECOM ICAM working group and other bodies studying and developing federated identity management and access control approaches for public safety data systems. As soon as possible, include such tools in RFP and contract interoperability requirements.

Source: NIST.IR.8255

Governance Agreements – Recommendations for Public Safety Leaders

UTAH COMMUNICATIONS AUTHORITY

Source: IJIS Public Safety Technical Standards Committee (IPSTSC)

Governance Agreements Best Practices

Leaders of data interoperability projects recommend:

Learn all you can about change management

Effective change management will provide a strong communications plan among all stakeholders, support the creation of a strong Agreement, and ensure project success over time.

Search out and confer with similar project leaders

Ask them to share their Agreement with you and to advise you on unanticipated problems they had encountered that could have been addressed in a governance Agreement.

Secure real support from all stakeholders in leadership positions

The up-front time taken with conferences, calls and consensus in crafting the Agreement is well spent. Leadership must allocate sufficient time and resources for formulating and supporting the Agreement.

Agree upon a vision

It is essential for a shared vision for the end result of your project to be endorsed by all affected participants' executive leadership.

UCA
UTAH COMMUNICATIONS AUTHORITY

Source: IPSTSC

Governance Agreements Best Practices cont'd

Review existing inter-agency Agreements for inconsistencies

This should be done with a fresh look at the data sharing project to ensure that no inconsistencies exist, and that no manual processes limit or contradict the data sharing efforts.

Plan to deal with cost allocation issues early

Cost sharing is a major component of sharing Agreements. The potential impacts of a new system should be discussed, cleared with participants and budgeted well in advance of the impact date.

Involve legal advisors

Allow enough time for the Agreement to be reviewed by the legal advisors of the various stakeholder agencies. It is likely that they will have an opinion and that the Agreement will undergo revisions.

Assure independence and impartiality

There must be a perception of fairness in all aspects of the Agreement.

Source: IPSTSC

How to Get Started

Source: Urban Institute, Justice Policy Center

UTAH COMMUNICATIONS AUTHORITY

How to Implement Interagency Data Sharing

Research-oriented steps to implementing data sharing, integration, and analysis across agencies and jurisdictions:

- Develop a framework for data integration. Projects should begin by establishing what questions researchers and practitioners would like to answer by sharing and integrating data. This research framework should be shaped by both theory and practice, ensuring that the results of data integration will be relevant to practitioners (problem-driven approach) while allowing for more proactive exploration of new relationships between crime and other variables (theory-driven approach).
- Organize the research team. Data integration projects need clear but flexible leadership that provides the structure to make progress as well as the flexibility to pursue new opportunities as they arise. A central project manager who oversees the work of several subject matter experts can help balance these competing priorities.
- Identify data sources. When identifying the right data sources to support cross-sector projects, agencies must balance several considerations, including data availability and quality, provider willingness to share data, the utility of the data's content, and the effort needed to analyze data based on how they are formatted and organized. Partners providing data should be engaged regularly and consistently through both organizational and individual relationships. At the same time, the team should take care to avoid redundant requests and be judicious in when and how often they request new data. A timeline developed in collaboration with all partners can provide a basis for accountability and help ensure that efforts move forward.

Source: Urban Institute, Justice Policy Center

How to Implement Interagency Data Sharing cont'd

- Solicit partners and manage relationships. Soliciting partners to support the project can be a delicate process, particularly when the data involved could create public relations or operational risks for an agency. To build productive relationships and address these concerns, agencies must demonstrate the value of integrated data projects to prospective partners and ensure that both operational and technical frameworks exist to maintain the security of project data.
- Create data management structures. The research team will need to find ways to structure and manage project data so that analyses can be completed efficiently. Data from partner agencies will need to be cleaned, coded, and reconciled. Reconciliation is particularly important, and the team will need to devise a common framework for coding data when jurisdictions use different terms to describe similar observations. Likewise, when data is stored at different geographic levels (e.g., census tracts and block groups), the team will need a strategy for managing data across these different units of analysis. Developing a data dictionary will be an invaluable step in this process.
- Integrate data. After structuring data to facilitate efficient management, the team must integrate the data so it can support analysis. Data can be integrated at the individual or place level, but integrating data at the place level is often easier.

Source: Urban Institute, Justice Policy Center

Planning for Data Integration Challenges

Source: Urban Institute, Justice Policy Center

UTAH COMMUNICATIONS AUTHORITY

Planning for Data Integration Challenges

Expect and plan for these challenges:

Resources. Often the first concern surrounding data integration, resource constraints— including staff time—will determine the scope and sustainability of any data-sharing effort. Many agencies may also face substantial challenges using their data systems for analytic or practical purposes, especially in the early stages of transitioning to digital or automated systems. This limited technical infrastructure may impose further resource demands on data integration efforts.

Technological challenges. A key challenge of data integration is converting datasets so that they "speak the same language" and can be feasibly combined and analyzed. Supporting and maintaining data security is another major challenge.

Agency culture and politics. In many cases, data sharing requires overcoming cultural and political barriers that may include an aversion to information sharing. Agencies can address these issues by working with all partners to identify the shared goals and benefits of a data-sharing and integration project.

Staffing and management within individual agencies. A data-sharing agreement between agencies will have little utility if staffing and management in the partner agencies do not support data sharing or if frequent turnover among those assigned to oversee data sharing weakens lines of communication between partners.

Source: Urban Institute, Justice Policy Center

Data Integration Challenges cont'd

Identifying shared goals, benefits, and language. To bring together the wide array of partners needed, data integration projects will frequently require translational efforts to build a common language and shared set of terms. Each partner will have their own language and jargon; without a shared language, these variations will create friction in a data integration project.

Agency staffing and management. Staff members in charge of executing and overseeing data integration projects need substantive and technical expertise to efficiently manage project demands. Similarly, data integration partnerships may be weakened without the appropriate culture or lines of communication in place to introduce new leadership and management to data-sharing protocols.

Central leadership to promote system utility. Coordination across partners is essential to maintaining the momentum of data-sharing efforts over time. Stable central leadership can improve the effectiveness and efficiency of these ventures, but it can be challenging to identify long-term leadership structures that will be accepted by all project partners.

Issues of public access. In some cases, efforts to share data as a tool for research or practice may be accompanied by a desire to allow greater public access to the data. Though public access can be a strong demonstration of transparency, agencies may fear exposure to public scrutiny or worry that releasing information will have a negative economic impact on their communities.

Source: Urban Institute, Justice Policy Center

Ensuring Comprehensive Data Sharing Policies

UTAH COMMUNICATIONS AUTHORITY

Source: NIST Public Safety Communications Research (PSCR)

Ensuring Comprehensive Data Sharing Policies

Public safety agencies should address the following in their data sharing policies:

Data Definitions: What data are collected? Are they shared in real time, with time delay, or only following an incident? The following considerations may be different for different data types.

Data Management: Who is responsible for maintaining different data elements during an incident?

Data Ownership: Who owns the data generated by an agency (the agency itself, or a third party)? How is ownership affected by sharing data with another agency?

Data Access: Who is allowed to access, download, write, change, or delete the data and how is that controlled? In the event of unauthorized data access, what procedures are required for informing affected agencies or other parties and containing the breach?

Data Security Practices: How are data protected from unauthorized use (copying, modification, deletion, etc.)? In the event of unauthorized data use, what procedures are required for informing affected agencies or other parties and containing the breach?

Data Integration: How are incident data integrated into other agency data systems (dispatch/CAD data, accounting data, Records Management System data, forensic data, evidentiary data, etc.)? Are specific data exchange standards employed to achieve this?

Data Retention: How long are data retained (minimum and maximum time periods)? If copies are made of the data, how are they managed after an incident, or after the retention period has ended?

Data Redaction: How is sensitive data or PII defined, flagged, and removed from records for internal retention and public records requests?

Data Policy Consistency: How will differences in the above policies be resolved?

UTAH COMMUNICATIONS AUTHORITY

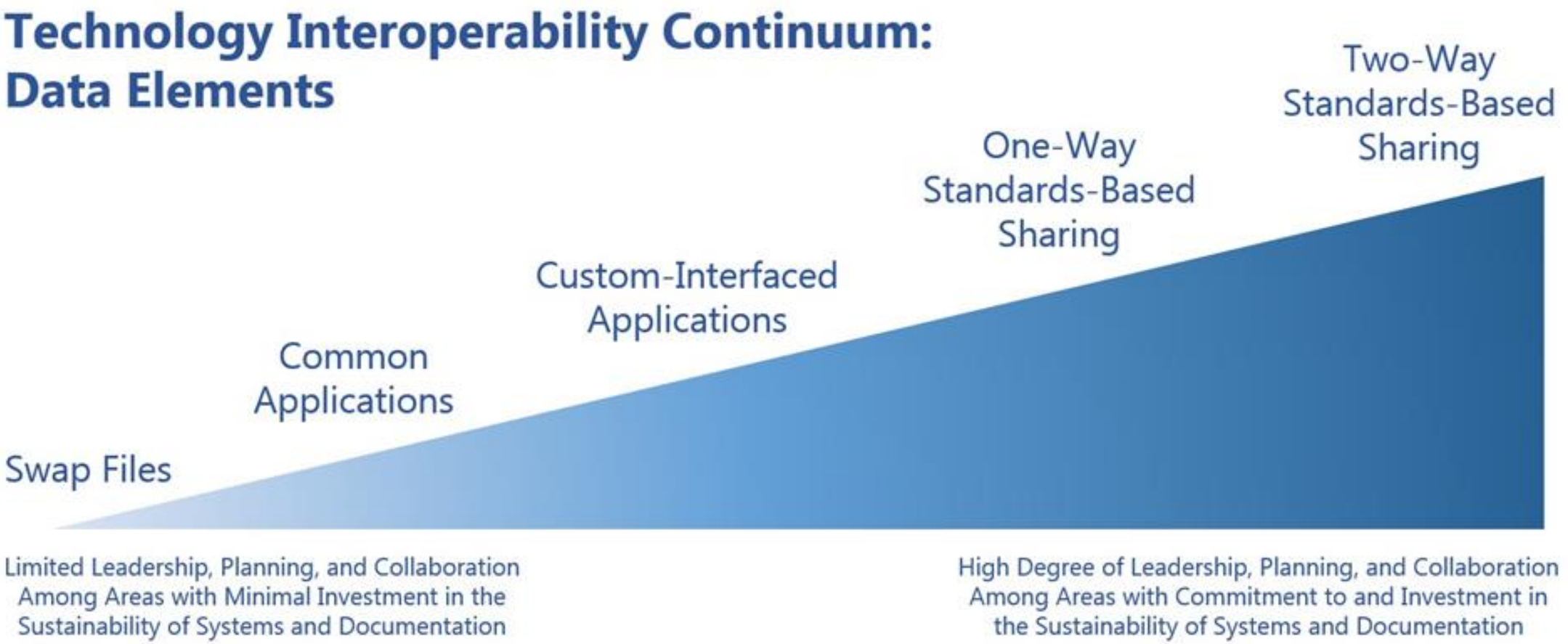
Source: NIST.IR.8255

Moving Up the Data Interoperability Continuum

Source: U.S. Department of Homeland Security

UTAH COMMUNICATIONS AUTHORITY

Data Interoperability – Moving up the Continuum



Source: DHS

Data Interoperability – Moving up the Continuum

Swap Files—Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, emails, faxes). This process effectively creates a static "snapshot" of information in a given time period. Though swapping files requires minimal planning and training, it can become difficult to manage beyond one-to-one sharing. With data frequently changing, there may be issues concerning the age and synchronization of information, timing of exchanges, and version control of documents. Each of these issues can hinder real-time collaborative efforts. In addition, the method of sharing files across unprotected networks raises security concerns.

Common Applications—The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data. Common proprietary applications can increase access to in- formation, improve user functionality, and permit real-time information sharing between agencies. However, the use of common proprietary applications requires strong governance to coordinate operations and maintenance among multiple independent agencies and users; these coordinated efforts are further compounded as the region expands and additional agencies use applications. Common proprietary applications also limit functionality choices as all participating agencies must use compatible applications.

Source: DHS

Data Interoperability – Moving up the Continuum

Custom-Interfaced Applications—Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom "one-off" links or a proprietary middle-ware application. As with common applications, this system can increase access to information, improve user functionality, and permit real-time information sharing among agencies. Improving upon common applications, this system allows agencies to choose their own application and control the functionality choices. However, if using one-to-one interfaces, the use of multiple applications requires custom-interfaces for each linked system. As the region grows and additional agencies participate, the required number of one-to-one links will grow significantly. Proprietary middleware applications allow for a more simplified regional expansion; however, all participants must invest in a single "one-off" link to the middleware, including any state or Federal partners. Additionally, custom-interfaced applications typically require more expensive maintenance and upgrade costs. Changes to the functionality of linked systems often require changes to the interfaces as well.

One-Way Standards-Based Sharing—One-way standards-based sharing enables applications to "broadcast/push" or "receive/pull" information from disparate applications and data sources. This system enhances the real-time common operating picture and is established without direct access to the source data; this system can also support one-to-many relationships through standards-based middleware. However, because one-way standards-based sharing is not interactive, it does not support real-time collaboration between agencies.

Two-Way Standards-Based Sharing—Two-way standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly. As with other solutions, a two-way approach can increase access to information, improve user functionality, and permit real-time collaborative information sharing between agencies. This form of sharing allows participating agencies to choose their own applications. Two-way standards-based sharing does not face the same problems as other solutions because it can support many-to-many relationships through standards-based middleware. *Building on the attributes of other solutions, this system is most effective in establishing interoperability.*

UCA
UTAH COMMUNICATIONS AUTHORITY

Source: DHS

A Public Safety Data Sharing Bibliography

UTAH COMMUNICATIONS AUTHORITY

A Public Safety Data Sharing Bibliography

1. Voss, B., Anderson, E. (June 2019). *Interoperability of real-time public safety data: Challenges and possible future states*. NISTIR 8255.

2. DHS. Interoperability Continuum. *A tool for improving emergency response communications and interoperability*. Retrieved from: https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf. See also https://www.dhs.gov/publication/interoperability

3. NPSTC. (2019, June). *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes*.

4. DHS. *Emergency Data Exchange Language (EDXL)*. Summary flyer.

5. La Vigne, N., Paddock, E., Irvin-Erickson, Y., Kim, K., Peterson, B., Bieler, S. (2017, July). *A Blueprint for Interagency and Cross-Jurisdictional Data Sharing*. Urban Institute, Justice Policy Center.

6. Ward, B., et al. (2015, November). *Use Cases In Public Safety CAD-to-CAD Data Sharing*. IJIS Institute, Public Safety Technical Standards Committee.

7. Ward, B., et al. (2014, November). *Change Management: Best Practices In Public Safety Data Sharing Project*. IJIS Institute, Public Safety Technical Standards Committee. Retrieved from: https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/ijis_wp_changemgmt_best_practice_2014.pdf

8. Ward, B., et al. (2013, July). *Critical Decision Criteria for Data Sharing*. IJIS Institute, Public Safety Technical Standards Committee. Retrieved from: https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/IPSTSC_Critical_Decision_Criteria_for_Data_Sharing_20130710.pdf

9. Ward, B., et al. (2013, August). *Governance Agreements in Public Safety Data Sharing Projects*. IJIS Institute, Public Safety Technical Standards Committee. Retrieved from: https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Governance_Agreements_in_Public_Safety_Information_Sharing_Projects_White_Paper_20120817_-_FINAL.pdf

UCA
UTAH COMMUNICATIONS AUTHORITY