Advancing Digital Government:
BETTER DECISION-MAKING
Through Data Sharing Agreements

NASCIO
Representing Chief Information Officers of the States

NASCIO Staff Contact:

Eric Sweden, MSIH MBA CGCIO™
Program Director, Enterprise Architecture & Governance

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street
Suite 1405
Lexington, KY 40507
Phone: 859.514.9153
Twitter: @NASCIO

Introduction

It has become almost a given that any function within state government can be and must be better *informed* when making decisions and generating policies that create desired outcomes for citizens. That necessary *informing* or *inform*ation needed for decision making comes from *inside* as well as *outside* the enterprise in focus, whether it is an agency, a task force, or the office of the governor. It has also become almost a given that jurisdictional and agency decision making must obtain much of its essential information from outside the agency itself. In the 21st century more and more data is *born-digital* and the advent of digital government makes data sharing more possible than ever. Data sharing enables digital government and is further enabled itself by digital government.

As government moves into 21st century with system modernization efforts, citizens are also demanding streamlined government services, a one-stop-service that is well informed about the citizen's whole circumstance. This along with federal and state mandates forces government to collaborate across programs and services in new ways. However, policies, siloed program requirements, and legislation sometimes lags behind in providing support for this concept – *an enterprise view*.

Interestingly, some of this *outside* information that resides within state government can be obtained from state open data portals. Some information can be classified as shareable through a state-wide information sharing clearinghouse. In this case the policy for information sharing is supported through legislation and an enterprise-wide, multi-agency, or cross-jurisdictional *memorandum of understanding* (MOU). But other information that is held more closely and classified as such is often difficult to obtain. And then once certain data and information is found to be useful there is the question of how to obtain it again as a continual information flow to inform operational as well as strategic decision making.

Key Question

Is there benefit to using a framework to manage data and information at an organizational level to ensure data sharing capabilities?

What is required in many cases is a formal *data sharing agreement* (DSA) that spells out *what* information is needed, *who* will transmit and *who* will receive such information. Such agreements must include necessary terms of agreement and the specificity of such terms increases with the value and classification of such information.

Data Sharing Agreements should be developed in a way that keep up with the changing mandates and services of government for the citizens we serve. This calls for an approach that is changeable, scalable and repeatable.

What is the Purpose of Data Sharing?

What is back of any data sharing is *informed* decision making. That decision making is tied to some issue, problem, opportunity and includes a question or set of questions that need to be answered before a decision can be made. Further, the circumstance may be that the decision maker(s) don't know what issue, problem, opportunity or questions exist and they are working to know and understand *the facts.*[1]

What data sharing does is provide agencies access to information about circumstances, constituents, locations (i.e., variables) they may not collect but that may be useful or even essential for answering business questions that are critical to the problem-solving process in their own agency.

The intention will vary depending on the situation, but for the most part, decision makers are intending to make a change, to improve current circumstances. The process of improvement starts with a question or set of questions. Answering those questions correctly means identifying the relevant information and selecting the right analytical method. It may entail experimenting to surface impactful correlations previously not known or leveraged. This is where the utility of shared data and information, and the necessary data sharing agreements enter the picture.

The answers decision makers are seeking can serve as evidence that supports some decision (decision making) or claim (our past decision was a good/bad one; our assumption/hypothesis was proven/disproven). The idea is that better decision-making leads to positive outcomes for clients, citizens, government, industry and the country. So, data sharing agreements play a critical role in government providing significant and tangible benefits.

Some of the benefits of data sharing agreements include:

- Better program performance
- Greater effectiveness in uncovering and preventing fraud, waste, and abuse
- Better decisions based on more and better information and data
- Evaluation of past decisions and potential course corrections

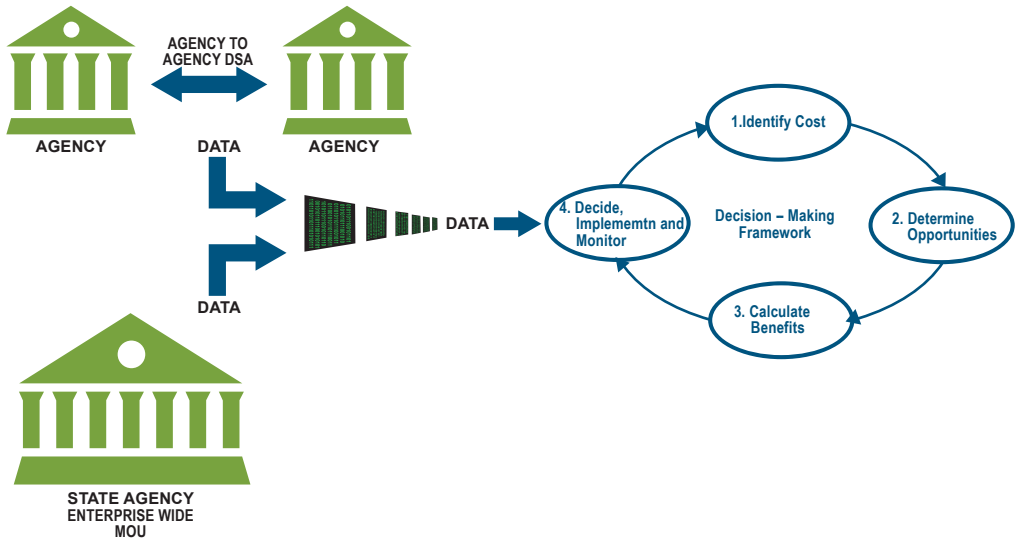
Key Question

Is there value in managing data sharing agreements centrally?

"When agencies share data, lives are saved and public offices become more efficient. Sharing data encourages collaboration among agencies, provides for informed decision-making and reduces redundancy of data production. Further, planning and policy groups become better informed, particularly in terms of emergency calls and disaster response. We can be proud that all 92 counties are now sharing their map data, a major milestone that will benefit all Indiana taxpayers."

~ David Vice, Executive Director of the Indiana Integrated Public Safety Commission

- Evaluation and potential change to a decision-making process
- Testing of assumptions regarding some issue
- Surfacing of confounders and bias



Governance

Managing and administering data sharing agreements and memorandums of understanding will require proper governance. This governance will include all stakeholders across government that will be supplying and consuming data. The governance body will determine principles, standards, operating discipline, necessary required approvals, and oversight of the portfolio of DSAs and MOUs.

Managing Information Sharing Agreements

We embark on yet another discussion of *enterprise portfolio management* (EPM) in this topic.[2] This time regarding data sharing agreements. There are a variety of such agreements with varying specified timelines. A jurisdiction or agency may have literally hundreds or thousands of such agreements and therefore they must be proactively and properly managed using the discipline of enterprise portfolio management. We might call this the *data sharing agreement portfolio*, or the *portfolio of data sharing agreements* whether they are formally managed as such or not.

Within this *portfolio* there will be varying degrees of detail or specificity. One size does not fit all. Some agreements may be created using a simple *memorandum of understanding* (MOU) template. An MOU may be created as an enterprise wide MOU and act as the default DSA. In such case, the state, or agency, will create a formal DSA on an exception basis when more specificity is required. Some circumstances will require very carefully crafted DSAs with pages of specific terms and conditions including commitments from all parties involved in the agreement. The *portfolio* of such

Key Question

What governance structure should be in place for managing data sharing agreements?

agreements and appropriate templates across state government are comprised of many agency specific portfolios. In most cases there is no central oversight or management of such portfolios at present. However, there is great value in moving toward central oversight in future to ensure:

- agreements are closed when they are no longer needed
- agreements are properly constructed
- the right kind of DSA or MOU is used
- there is proper review by legal, privacy, security, data management, records management
- data and information is properly destroyed when it is no longer needed

Other such requirements will be presented in Part II of NASCIO's DSA series.

Why is guidance needed for data sharing agreements?

Because the proliferation of such agreements is expanding and is anticipated to entail some level of risk for state government it may be useful to centralize such activity. States will be exposed to the risk of unintended outcomes if such agreements are not properly constructed, governed and managed. Central coordination or optimization may save time and achieve consistency, and with consistency help avoid or reduce certain risks.

Some of the risks may be described with the following statements:

- "Oops, we should have thought of that! We're missing critical conditions!"
- Provider:
  - "We must maintain ownership of the data."
  - "The data we share must be properly managed."
  - "The data is no longer needed after this date."
  - "There is potential for re-identification. Therefore we must de-identify prior to sending."
  - "We should have required a periodic privacy impact assessment (PIA). Now we're in trouble!"
  - "Do we have necessary informed consent to share certain data?"
- Receiver:
  - "We must have timely, reliable data – it is informing critical decision making and deployment of resources."
  - "We didn't understand the sensitivity of the data."

Key Question

What statutes or executive directives exist or should exist for supporting data sharing agreements?

- "The data is so 'clean' it isn't useful. Measures taken to de-identify have also scrubbed out the meaning of the data."
- "We don't have a "Plan B" when something happens that prevents the creation and distribution of this information!"

Some of this risk is related to the construction of the presiding agreement and contracting arrangements. Other risk is related to properly managing the data itself. Depending on the nature of the data and information being shared – e.g., aggregated data, or raw data – there may be some level of risk regarding the possible re-identification of persons and even organizations from the data when such re-identification is prohibited either by statute or by request. Such risks must be anticipated and dealt with in the *terms and conditions* of the data sharing agreement.

There is also the risk related to quality of the data being shared and the commitment on the part of the provider to ensure the data is at some guaranteed minimum level of quality. The data and information being shared may be informing routine operational decisions, or critical strategic decisions. It may be informing "right now" emergency response decision making. The continuums of decisions from *tactical to strategic; from low security to high security; from long-term trending to immediate emergency response*, all determine the *shape and content* of information sharing agreements.

NASCIO has been looking at this area of state government activity to determine how states might move forward with a discipline that reduces risks, optimizes the process of forming such agreements, selects the appropriate type of agreement (DSA vs MOU) and pulls the best examples of effective DSAs and MOUs. All of this activity is intended to inform the community regarding what works and what doesn't work. This guidance document is expected to be one member of a growing library of reports and webinars on data sharing agreements and will essentially kick off the NASCIO work in this subject area.

NASCIO has published on other relevant supporting discipline such as data governance and cross-jurisdictional collaboration. NASCIO also maintains a growing library of ideas from across the states and territories that should be referenced as part of any planning activity. That is the NASCIO Awards Archive at www.nascio.org/Awards/SIT.

Key Question

Should data sharing agreements be managed as a portfolio?

"The statewide data sharing initiative has been invaluable to our work on behalf of Indiana counties in analyzing and mitigating their risks to natural disasters. Two significant initiatives in this area are FEMA's Risk MAP program and Multi-Hazard Mitigation Planning. In order for communities to be eligible to receive federal mitigation funding, they must have FEMA-approved mitigation plans that include quantitative risk analyses. The availability of parcel and address point data from the data sharing initiative has significantly improved the accuracy of our risk analyses, helping the communities to focus their attention on specific points within the county and prioritize specific strategies to mitigate their vulnerabilities.

~ Laura Danielson, Deputy Director of Strategic Initiatives and Civic Engagement, The Polis Center at IUPUI

Benefits of Data Sharing Agreement

Foremost among the many benefits of data sharing agreements is the notion of reaching an informed "agreement." Parties coming together to embark on any initiative *together* must have agreement on some very basic elements regarding *how* they will work together. These elements are part of any discussion regarding projects, programs and management initiatives. Any collaborative arrangements must be in alignment with the mission, values, and enterprise architectures of the participating parties. See the NASCIO Enterprise Architecture Value Chain.[3] They include:

- What is the context within which this new need, issue, or purpose exists?
- What is the purpose and intended outcomes?
- What is the duration?
- Who is involved in the agreement and in what capacity are they involved?
- What data and information will be shared?
- What is the sensitivity of such data and information?
- What is the perceived and necessary level of quality and reliability?
- How often will such agreement be re-evaluated for either continuation for termination?
- What conditions would suspend or actually terminate such an agreement?
- What remedies are prescribed for breach of terms?
- What individuals and roles will carry responsibility and accountability for the agreement?
- Would such agreement benefit from periodic assessment such as a privacy impact assessment (PIA)?

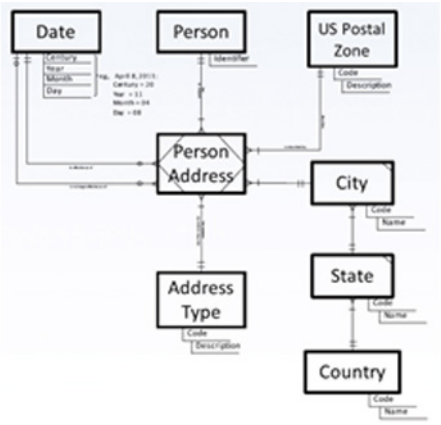
Such are examples of basic terms that should be considered in most agreements in order to ensure the participants know their commitments, and ensure the data and information being shared is properly handled, shared and protected.

We're Data Modeling Again!

The data and information being shared may have, and should have, an associated data and/or domain model that describes the embodied semantics, definitions, terms, and the business rules of the data. That data model will not necessarily be shared with all partners, but the provider of the data and information must employ proper data management, clearly understand what data is being shared either in entirety or as a

Key Question

Who should be responsible for a data agreement portfolio?



"view" of the data, and properly evaluate privacy and security implications. Doing so will assist in developing proper discipline on both the sender and recipient side of a data sharing relationship and help avoid unintended outcomes.

There must be the necessary meta data – or data about the data – such as classification and associated necessary security measures that must be in place on both the provider and recipient side of the data sharing relationship, and the transmission in between. This may be particularly important when agencies are not only sharing data, but they making policy decisions together. There must be agreement on business terms and definitions.

A Legal Review

Legal review must be carried out by qualified legal staff who are familiar with relevant statutes and regulations. The most qualified legal staff come from the agencies that are the keepers of the data – the authoritative source of the data. These are the experts in the specifics of a particular government line of business and are the experts that maintain vigilance of current and forthcoming relevant laws and regulations.

This staff must be part of the team that constructs the agreement and periodically reviews such agreement to ensure they are in line with current applicable law.

Possible Conflicts in Terms and Conditions

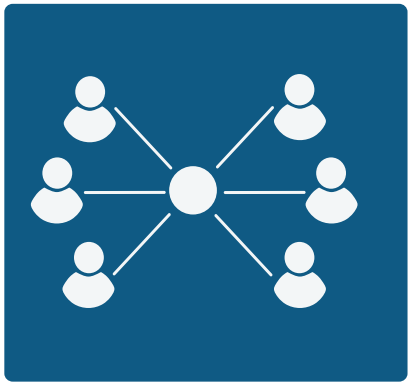
When beginning to build the structure of a data sharing agreement, or a memorandum of understanding, it is necessary to understand the applicable laws, and the terms and conditions specified in those laws. A requester of information must meet the terms and conditions specified by the provider. As well, the requester may have terms and conditions that must be met by the provider.

Each agency or department has their responsibilities, commitments and obligations. Any data sharing agreement must be in alignment with those elements. This is where challenges may arise. There may be conflicts in terms, definitions, data models. Those conflicts must be reconciled through efforts such as data mapping. There may be conflicts of laws, regulations, data classifications, security, and privacy protocols. Such conflicts will need to identified and addressed in the DSA or MOU.[4]

Key Question

How often should data agreements be reviewed?

The Business Case - Value Determination



As with any project, program and management initiative, there must be a business case. There must be an economic value to putting in place a data sharing agreement. The business case should explore alternatives to a data sharing agreement. For instance, *access* to certain data may be an alternative to physically *sending* or *transmitting* data. The business case must evaluate the cost, benefits and associated risks. The business case must also include addressing the validation of the business case once the data sharing agreement is in place. In other words, are the parties involved harvesting the value presenting in the business case? And if not, why not?

Deidentification and Reidentification, A Moving Target!

Depending on the data, the intended use of the data, and potential secondary use of the data, it may be necessary to remove personal as well as organizational identification. This is called *deidentification*. *Deidentification* is the action of removing explicit identifiers from a database or dataset. This entails removing explicit identifiers, generalizing data, or replacing identifying information with fictitious data. Deidentification of data is not the same as anonymizing data. *Anonymous data* is a stronger discipline that precludes the manipulation of the data in order to actually reidentify the subject(s) of the data.[5]

The whole subject area of deidentification and reidentification is a moving target. The technical know-how and technology capabilities for re-assembling identities are continually emerging in data analysis. This creates a significant challenge to preventing reidentification. On the other hand, as data is manipulated to remove the risk of reidentification, the counter effect is the creation of synthetic datasets, potential confounders and bias in the data. The process of deidentification can in fact mask the existence, or the strength, of a causal determinant. It may be that the statistical study design must necessarily influence the approach to deidentification in order to avoid any bias or confounders. The study may have to include strategy and techniques that take into account the actual effect of data modification used to protect identities.

If deidentification is a requirement, then it must be properly ensured. Why is this so important? Because state government is in a position of trust. The citizens of this country

Key Question

How often are your data sharing agreements reviewed and then either renewed and terminated?

have entrusted government with one its most valuable and personal assets – their information. For that reason, NASCIO's work emphasizes privacy as a key ingredient in data sharing agreements. And, for that reason, we have made special emphasis on privacy principles, borrowing from some of the best references including the American Institute of Certified Public Accountants and the Office of the New Zealand Privacy Commissioner.

Privacy Principles

As with most things there are applicable principles here as well. Principles that should guide the discipline of data sharing agreements include the following.[6] These are general principles of data sharing adapted from the Center for Disease Control (CDC) which in turn references the citation given.

Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality Adapted from CDC

1. State government data should be acquired, used, disclosed, and stored for legitimate purposes.
2. Programs should collect the minimum amount of personally identifiable information necessary to achieve the intended purpose of the data sharing agreement.
3. Programs should have strong policies to protect the privacy and security of personally identifiable data.
4. Data collection and use policies should reflect respect for the rights of individuals and community groups and minimize undue burden.
5. Programs should have policies and procedures to ensure the quality of any data they collect or use.
6. Programs have the obligation to use and disseminate summary data to relevant stakeholders in a timely manner.
7. Programs should share data for legitimate state government purposes and may establish data-use agreements to facilitate sharing data in a timely manner.
8. State government data should be maintained in a secure environment and transmitted through secure methods.
9. Minimize the number of persons and entities granted access to identifiable data.
10. Program officials should be active, responsible stewards of state government data.

Key Question

Is there either an executive order or statutory support for data sharing?

"Ohio Governor John R. Kasich is committed to taking data analytics to the next level in Ohio, by better interconnecting and correlating the state's many separate data resources that feed the analytical process to tackle complex problems with outcomes that improve Ohioans' health, security and well-being. In concert with this data sharing priority, Gov. Kasich and his agency directors are then also committed to ensuring that data is analyzed and applied in ways that fully protect individual identities and preserve the confidentiality of personal information.

Sorting through computer loads of seemingly obscure numbers and unemotional statistics, data analytics may appear far removed from the lives and concerns of everyday Ohioans. Yet the clues it reveals can help the state address some of Ohio's greatest challenges, such as infant mortality, child welfare, opiate addiction, persistent poverty, and school dropout rates. By addressing challenges like these in a more focused, purposeful way, the next level of data analytics will give state policymakers and stakeholders a deeper understanding of those issues, pointing toward strategic areas of focus and lasting solutions."

~Statement from the Office of the Governor, State of Ohio, December 2016[11]

Then there are certain specific privacy principles for government.

As discussed, state governments hold an enormous amount of information on citizens, private corporations and non-profits. As such, state government is expected to carefully manage such information in such a way as to maintain and protect privacy rights of its constituents. Therefore, any data sharing agreement must consider privacy implications and determine what discipline will be put in place to protect privacy. Various state government analytics initiatives have demonstrated the value of data sharing. The benefits and the potential for future benefits is impressive. As state government matures its capabilities to share data in order to inform analytics which in turn inform decision making, it must also mature its ability to anticipate and address privacy issues. That endeavor begins with principles. And we do emphasize this aspect of data sharing.

To emphasize the importance of privacy we present yet another set of principles. These are the Generally Accepted Privacy Principles from the American Institute of Certified Public Accountants.

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection. The entity collects personal information only for the purposes identified in the notice.
5. Use, retention, and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. Access. The entity provides individuals with access to their personal information for review and update.
7. Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).

Key Question

Who should be involved in constructing a data sharing agreement?

9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

See additional references regarding privacy in the reference section of this report.

Conclusion

Data sharing agreements enable the sharing of data across agencies and across jurisdictions. Shared data and information contribute toward informing the decision-making process. Data sharing is a foundational enabler of digital government. 21st Century Government is a digital government that will continue to mature in its capabilities for delivering citizens services through decision making and policy making that is more informed than any time in our history. With adequate, appropriate and timely information decision makers are enabled to make well informed decisions and achieve well vetted outcomes. The end result is better outcomes for citizens. Data sharing agreements must be carefully crafted in alignment with the principles of data sharing including applicable laws and regulations, data management, and privacy.

Recommendations

1. Establish a discipline for creating data sharing agreements.
2. Create a set of proforma templates for data sharing agreements.
3. Put in place appropriate enterprise data governance for data sharing agreements and memorandums of understanding related to data sharing.
4. Ensure those crafting data sharing agreements test their agreements against aforementioned principles, especially those concerned with data governance, metadata management, data quality, and data integration.
5. Review all data sharing agreements with state and/or agency legal, records management, enterprise data management, data governance, data security, and privacy functions.
6. Manage data sharing agreements within a portfolio and data management structure that includes discipline for periodically reviewing such agreements regarding duration, changing needs, compliance with current standards and statutes, security and privacy.
7. Ensure data sharing agreements are updated as needed as new technology and new data management standards emerge for re-identification.
8. Ensure data sharing agreements are terminated and data is properly

Key Question

Under what circumstances does government employ enterprise-wide MOUs in lieu of individual data sharing agreements?

destroyed according to legal and other protocols once the data sharing is no longer needed.

9. Test whether a data sharing agreement is really needed. Determine if an enterprise wide MOU can serve most data sharing needs, thus resolving the resource demand of managing 100's or 1000's of data sharing agreements.
10. Train employees and contractors on the principles and necessary terms and conditions of data sharing including data security, physical security, and privacy.
11. Stay tuned to NASCIO for publications on data sharing agreements, analytics, records management, privacy and security.

A Road Map to Data Sharing: Key Questions

- Is there benefit to using a framework to manage data and information at an organizational level to ensure data sharing capabilities?
- Is there value in managing data sharing agreement centrally?
- What governance structure should be in place for managing data sharing agreements?
- What statutes or executive directives exist or should exist for supporting data sharing agreements?
- Should data sharing agreements be managed as a portfolio?
- Who should be responsible for a data agreement portfolio?
- How often should data agreements be reviewed?
- How often are your data sharing agreements reviewed and then either renewed and terminated?
- Is there either an executive order or statutory support for data sharing?
- Who should be involved in constructing a data sharing agreement?
- Have your data sharing agreements been reviewed by counsel?
    - Breach Liability
    - Statute review
    - Legal terms
- Have your data sharing agreements been reviewed by cybersecurity staff?
- Have your data sharing agreements been reviewed by privacy staff?
- Should agreements have standardized (pre-written) sections?

Key Question

What messaging and marketing might be required to move the culture to more data sharing?

- How do you store and keep track of Data Sharing Agreements? (internal and external)
- What procedures do you have in place to destroy data after the termination of a data sharing agreement?
- Does the culture of state government have established trust to support agency to agency data sharing?
- What messaging and marketing might be required to move the culture to more data sharing?
- Under what circumstances does government employ enterprise-wide MOUs in lieu of individual data sharing agreements?

Contributors:

- Lily Alpert, Analyst, State Child Welfare Data Center, Chapin Hall, University of Chicago; Analytics Committee, National Collaborative for Integration of Health & Human Services, APHSA
- Monica Carranza, Chief Information Officer, State of Illinois Department of Employment Security
- Allison Davis, Chief Information Security Officer, Department of Human Services, State of New Jersey; Analytics Committee, National Collaborative for Integration of Health & Human Services, APHSA
- Stu Davis, Chief Information Officer, State of Ohio
- Gale Given, former Chief Technology Officer, State of West Virginia
- Amy Glasscock, Senior Policy Analyst, NASCIO
- Kelly Harder, Director, Community Services Division, Dakota County, Minnesota; Co-Chair, Analytics Committee, National Collaborative for Integration of Health & Human Services, APHSA
- Jack Harris, Director, Enterprise Architecture and Network Strategies, State of Michigan
- Jeffrey Jordon, Director, Enterprise Warehousing and Analytics, State of Maine
- Andrew Laing, Enterprise Business Architect, Agency of Human Services, State of Vermont
- Emily Lane, Program and Brand Manager, NASCIO
- Megan Lape, Director, National Collaborative for Integration of Health and Human Services, American Public Human Services Association (APHSA); Co-Chair, National Collaborative's Analytics Committee

- Michelle Lavallee, Organization Change Management Director, Enterprise Service Office, Agency for Human Services, State of Vermont; Analytics Committee, National Collaborative for Integration of Health & Human Services, APHSA
- Sean McSpaden, Principal Legislative IT Analyst, Administrator - Joint Legislative Committee on Information Management and Technology, Administrator - Transparency Oregon Advisory Commission, Oregon Legislative Fiscal Office
- Sallie Milam, Executive Branch Chief Privacy Officer, West Virginia Health Care Authority
- Dewand Neely, Chief Information Officer, State of Indiana
- Dr. Steve Nichols, Chief Technology Officer, Georgia Technology Authority, State of Georgia
- Mark Raymond, Chief Information Officer, State of Connecticut
- Doug Robinson, Executive Director, NASCIO
- Ellena Schoop, Enterprise Data Architect, State of Minnesota
- Anne Marie Smith, Ph.D., VP of Education, Chief Methodologist, EWSolutions, Inc.
- Cy Smith, Geospatial Information Officer, State of Oregon
- Jim Sparks, Indiana Geographic Information Officer, Indiana Office of Technology

References

Examples from the States

Michigan – A Standardized Data Sharing Template

The State of Michigan has in place an Executive Order that established the Enterprise Information Management (EIM) program. One of the program goals is "promoting efficient cross-agency data sharing, within a "share first" environment, while taking all necessary and appropriate steps to ensure personal privacy and safeguard personal information."

In 2014 the EIM project surveyed the 8 Steering Committee departments and found that those departments alone had 161 Data Sharing Agreements (DSA) with State of Michigan (SOM) departments. The format and content across the agreements varied

considerably. One of the early deliverables of the EIM project was development of a standardized Data Sharing Agreement template. This template is used by all SOM agencies to document data sharing. The most frequently shared data element is address.

The state has not yet established a central repository of DSAs so there is not a current count of how many DSAs exist. It is believed that the current portfolio of DSAs is numbered in the thousands. The aforementioned 161 agreements only encompasses 8 Michigan departments within the bounds of State government. In total there are 25 departments/agencies, and many departments share data with local units of government, researchers, and other states.

Probably the biggest success story from a data sharing perspective is the use of an enterprise Master Data Management (MDM) solution, which Michigan has branded Master Person Index (MPI), to match data across multiple programs. Today MPI matches participant data across about 25 DHHS programs, and can authoritatively identify that an individual is indeed the same individual enrolled in multiple DHHS programs/services. EIM is in the process of adding data sources other than DHHS to the MPI solution.

Examples of data sharing facilitated through MPI include:

- Matching educational and workforce data to evaluate public education and workforce training programs
- Matching driver, vehicle, and emergency services data with road conditions and crash data in order to reduce traffic fatalities
- Matching electronic death records with a variety of payment data to reduce fraud

Illinois – Enterprise Memorandum of Understanding

In April 2016, thirteen State Agencies that are members of the State's Health and Human Service enterprise signed an Enterprise Memorandum of Understanding (eMOU) to encourage inter-agency data sharing. At the time of the signing, state agencies operated within a "siloed" data structure that only allowed agencies to view customer information related to Agency-specific programs. Illinois realized that the most valuable insight comes from analyzing data across systems and programs, both at the aggregate level for policymaking and on the frontlines for immediate decision support.

ILLINOIS

Illinois had operated under a "siloed" data structure which prevents agencies from sharing data. This impeded the ability to aggregate and synthesize information or

employ predictive analytics for early intervention and prevention. Under this model, residents had to contact multiple agencies to find information or sign up for services. Often they would fill out a paper form, and then physically travel to the offices of another agency to fill out another paper form with identical information. This was an inefficient system that wasted the limited resources of the state and created a frustrating experience for residents.

To address this problem a team from Illinois looked to other states for examples of how to encourage inter-agency data sharing. Indiana had implemented a new inter-agency data sharing model, but their approach was time-consuming. The team then looked to Virginia, which had implemented an enterprise-wide data sharing agreement. Illinois' current version of the eMOU used the Virginia model as a platform to build upon. After several months of collaboration by the Agency General Counsels, CIOs, and the Office of the State Chief Information Security Officer, the state was able to refine the model for Illinois.

In order to address these problems, Illinois built an enterprise wide data sharing agreement between Illinois agencies that was designed to:

- enable customer-centric service delivery, providing information tailored to a citizen's needs;
- assist effective strategic policymaking, offering executives and front-line staff trustworthy data to make informed decisions; and
- encourage efficient program management, leading to increased productivity of State employees.

In order to accomplish these goals, the agreement established an operational committee that facilitates data sharing requests among the agency partners. The committee is comprised of the State's Chief Data Officer and Chief Information Officers from signatory agencies. The agreement was created and signed in the state of Illinois within seven months. The speed at which the agreement was completed can be attributed to the strong support from the Office of the Governor, Illinois Department of Innovation & Technology executive leadership, and agency directors. The agreement was viewed as instrumental in Illinois' IT transformation.

The creation and signing of this agreement was a positive step forward for the State of Illinois and highlighted the desire of the Governor's Office, state leaders and the agencies to improve the lives of Illinois residents. Since implementation, Illinois has seen 5 distinct benefits from the eMOU on data sharing. Specifically, the eMOU: (1) provides structure and consistency around data sharing; (2) increases the speed of information sharing; (3) creates an internal clearinghouse for data; (4) delineates timelines for sharing of information; and (5) uses National Institute for Standards and Testing (NIST) security standards to ensure the highest level of data protection.

The agreement provides a legal foundation by which participating Agencies can easily share data across State programs. By signing the agreement Agencies adopt the legal, security and data governance framework in advance of any data sharing requests. Unlike Agency-to-Agency Data Sharing Agreements, once a data request is made, participating Agencies can focus on the technical components of data sharing; as the legal components have already been agreed upon.

To ensure support for the agreement, educating the workforce and managing change is essential. Taking the time to educate all levels of staff before an agreement is signed helps lay the foundation for swift adoption from State and agency executive leaders to managers and front-line staff.

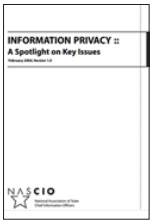
Listed below are external and internal resources that were used to accomplish the data sharing agreement:

- The State of Indiana - Article[7]
- The State of Virginia – Presentation[8]
- The Illinois Department of Employment Security - Article[9]
- The State of Washington - Article[10]

NASCIO

Information Privacy: A Spotlight on Key Issues

www.nascio.org/Publications/ArtMID/485/ArticleID/258/Information-Privacy-A-Spotlight-on-Key-Issues



This publication highlights key issues in the following areas of privacy: Children's Information, Drivers' Information, Health Information, Financial Information, Education Information, Social Security Numbers, Homeland Security-Related Information, Website Privacy Policies, and Government Data Matching Activities and Agreements.

Think Before You Dig: The Privacy Implications of Data Mining & Aggregation

www.nascio.org/Publications/ArtMID/485/ArticleID/254/Think-Before-You-Dig-The-Privacy-Implications-of-Data-Mining-Aggregation

This publication highlights key issues in the following areas of privacy: Children's Information, Drivers' Information, Health Information, Financial Information, Education Information, Social Security Numbers, Homeland Security-Related Information, Website Privacy Policies, and Government Data Matching Activities and Agreements.

Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications

www.nascio.org/Publications/ArtMID/485/ArticleID/254/Think-Before-You-Dig-The-Privacy-Implications-of-Data-Mining-Aggregation

This brief examines the business benefits and privacy issues related to government's use of data-mining technologies. It also takes a look at high-profile government data-mining programs and suggests ways to infuse privacy protections and transparency into government's use of data-mining technologies.

Managing Change: How the Indiana County/State Data Sharing Initiative Mapped Its Way to Success (webinar)

www.nascio.org/Publications/ArtMID/485/ArticleID/466/Managing-Change-How-the-Indiana-CountyState-Data-Sharing-Initiative-Mapped-Its-Way-to-Success-webinar

All 92 Indiana counties have voluntarily provided key geospatial data with the Indiana Geographic Information Office. One hundred percent cooperation was not easy and it took several years to accomplish. This presentation focuses on the drivers that encouraged the effort and the resistors that hampered success and how managing both sides of the change equation worked in Indiana.

Data Strategy: Essential for State Governments (webinar)

www.nascio.org/Publications/ArtMID/485/ArticleID/463/Data-Strategy-Essential-for-State-Governments-webinar

All state governments need a guided approach to managing their data and information to obtain the maximum value for success in a challenging environment. An Enterprise Data/Information Management (EDM/EIM) initiative provides the framework for a state to deliver real information knowledge and provide true value to their citizens. This session provides the framework of the domain known as enterprise data / information management, explains its essential components, gives the reasons that state governments should create a sustained data management program, and demonstrates some benefits that successful state EDM/EIM programs have achieved.

State of Washington: Privacy Modeling Demo (webinar)

http://www.nascio.org/Publications/ArtMID/485/ArticleID/472/State-of-Washington-Privacy-Modeling-Demo-webinar

Government is using more data than ever in rendering services to citizens, yet government has few tools to enforce privacy rules or considerations and can't simply hire enough to meet the demand for expertise. After consulting with academic and legal experts form the privacy community in Seattle, the state's Chief Privacy Officer,

Alex Alben, retained a software firm to create a web application which returns relevant search requests based on the intended use of personal information in a product or service.

Other Resources

The American Institute of Certified Public Accountants (AICPA)

http://www.aicpa.org

The AICPA is the national professional organization of Certified Public Accountants (CPAs) in the United States, with more than 400,000 members in 145 countries in business and industry, public practice, government, education, student affiliates and international associates. The AICPA sets ethical standards for the profession and U.S. auditing standards for audits of private companies, non-profit organizations, federal, state and local governments.

See Generally Accepted Privacy Principles

Business Version:

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf

Practitioners Version:

http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_PRAC_%200909.pdf

National Neighborhood Indicators Partnership (NIPP)

http://www.neighborhoodindicators.org

The National Neighborhood Indicators Partnership (NNIP) is a collaborative effort by the Urban Institute and local partners to further the development and use of neighborhood information systems in local policymaking and community building.

See NNIP Guide, *NNIP Lessons on Local Data Sharing.*

National Electronic Interstate Compact Enterprise - NEICE

Expediting the placement of children in safe, permanent families across state lines and reducing administrative paperwork and costs. The National Electronic Interstate Compact Enterprise is a cloud-based electronic system for exchanging the data and documents needed to place children across state lines as outlined by the Interstate Compact on the Placement of Children (ICPC). Launched in November 2013 as a pilot project with six states, NEICE significantly shortened the time it takes to place children

across state lines, and saved participating states thousands of dollars in mailing and copying costs. At this time, the NEICE project is expanding nationwide, with the goal of serving all states.

www.aphsa.org/content/AAICPC/en/actions/NEICE.html

The Privacy Commission of New Zealand

www.privacy.org.nz

The Privacy Commissioner's Office works to develop and promote a culture in which personal information is protected and respected. The Privacy Commissioner administers the Privacy Act 1993. The Privacy Act applies to almost every person, business or organization in New Zealand. The Act sets out 12 privacy principles that guide how personal information can be collected, used, stored and disclosed. The Privacy Commissioner's Office has a wide range of functions. Some of these include investigating complaints about breaches of privacy, running education programs, and examining proposed legislation and how it may affect individual privacy.

See e-Learning Modules at www.privacy.org.nz/further-resources/online-e-learning-privacy-modules/

An A To Z of Approved Information Sharing Agreements (AISAs)

Guidance on what constitutes an approved information sharing agreement provided by the New Zealand Privacy Commissioner's Office.

https://privacy.org.nz/assets/Files/AISAs/Approved-Information-Sharing-Agreement-guidance-March-2015.pdf

Linking Data across Agencies: States That Are Making It Work

The Forum for Youth Investment

forumfyi.org/files/States.That.Are.Making.It.Work.pdf

This report presents:

- The current status of states' ability to link data across agencies;
- Processes to foster a culture of data-driven decision making:
  - Prioritize critical policy questions to drive development and use
  - Ensure interoperability by adopting common standards, definitions and language
  - Protect personally identifiable information to reinforce that information is private and secure and data can be shared

- Federal support for cross-agency data sharing;
- The role governance structures play in linking data systems;
- Four states that are creating critical linkages between data systems to answer key policy questions:
  - Connecticut, Florida, Maine and Washington
- Further reports and resources on sharing data across agencies to improve research and student success

The University of Chicago, University Research Administration

Data-sharing Agreements

https://ura.uchicago.edu/page/data-sharing-agreements

This reference provides a list of necessary elements that should be addressed in a data sharing agreement.

Community Health Data and Monitoring Committee

In support of community-academic partnerships

http://www.ucdenver.edu/research/CCTSI/community-engagement/resources/Documents/DataSharingCreatingAgreements.pdf

The development of these guidelines is a project of the Community Health Data and Monitoring Committee, a committee of the Colorado Clinical and Translational Sciences Institute's (CCTSI) Community Engagement Core. We appreciate the review of community and academic partners who have contributed to the presentation and content of these guidelines, and Montelle Tamez for editorial contributions. Funding for this project was provided by the Rocky Mountain Prevention Research Center (Centers for Disease Control and Prevention Cooperative Agreement U48 DP001938) and the CCTSI, which is supported in part by Colorado CTSA Grant 5UL1RR025780 from NCRR/NIH. Contents are the authors' sole responsibility and do not represent official CDC or NIH views.

http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf

EndNotes

[1] See NASCIO's Series – "Do You Think, Or Do You Know." See www.nascio.org/publications.

[2] See NASCIO's report, Destination: Advancing Enterprise Portfolio Management – First Stop: Issues Management, http://www.nascio.org/Publications/ArtMID/485/ArticleID/94/Destination-Advancing-Enterpris e-Portfolio-Management-%e2%80%93-First-Stop-Issues-Management.

[3] The NASCIO Enterprise Architecture Value Chain is presented in a number of reports including:

• DO YOU THINK? OR DO YOU KNOW? PART II: The EA Value Chain, The Strategic Intent Domain, and

Principles. Available at http://www.nascio.org/Publications/ArtMID/485/ArticleID/178/DO-YOU-THINK-OR-DO-YOU-KNOWPART- II-The-EA-Value-Chain-The-Strategic-Intent-Domain-and-Principles.

• Transforming Government through Change Management: The Role of the State CIO. Full report and brief available at http://www.nascio.org/Publications/ArtMID/485/ArticleID/214/Transforming-Government-through-Change-Management-The-Role-of-the-State-CIO.

[4] See discussion of conflicts of laws. Capitals in the Clouds, Par t III – Recommendations for Mitigating Risks: Jurisdictional, Contracting and Service Levels. NASCIO. pp. 8, 12, Appendices B and C. Retrieved on February 28, 2017, from http://www.nascio.org/Publications/ArtMID/485/ArticleID/116/Capitals-in-the-Clouds-Part-III-%e2%80%93-Recommendations-for-Mitigating-Risks-Jurisdictional-Contracting-and-Service-Levels.

[5] Ochoa, S., Rasmussen, J., Robson, C., Salib, M. Reidentificatio n of Individuals in Chicago's Homicide Database A Technical and Legal Study. Retrieved on August 17, 2016, from web.mit.edu/sem083/www/assignments/reidentification.html.

[6] "Ten Guiding Principles for Data Collection, Storage, Sharing, an d Use to Ensure Security and Confidentiality." Retrieved on August 16, 2016, from http://www.cdc.gov/nchhstp/programintegration/TenGuidingPrinciples.html. Adapted from Lee, LM, Gostin, LO. Ethical collection, storage, and use of pu blic health data: a proposal for national privacy protection. JAMA 2009; 302:82-84.

[7] Berggoetz, B., "Governor creates large data-sharing hub across all of state government." INDYSTAR, April 26, 2014.Retrieved on 1/31/2017 from http://www.indystar.com/story/news/politics/2014/04/26/governor-creates-large-datasharing-hub-across-state-government/8174939/.

[8] "Enhanced Memorandum of Understanding (E-MOU)." Commonwealth of Virginia, Virginia Information Technology Agency (VITA). Retrieved on 1/31/2017, from https://www.vita.virginia.gov/uploadedFiles/VITA_Main_Public/ITAC/HITSAC/2014/EMOUexecsummary.pdf.

[9] State of Illinois Department of Employment Security (IDES) Shared Data Agreements website. http://www.ides.illinois. gov/Pages/Shared-Data-Agreements.aspx.

[10] State of Washington Employment Security Department website. https://esd.wa.gov/newsroom/data-sharing.

[11] "Ohio Lays Out Plans for Data Analytics." Government Technology, January 4, 2017. Retrieved on 2/1/2017 from http:// www.govtech.com/data/Ohio-Lays-Out-Plans-for-Data-Analytics.html.