GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

Guidelines for Information Sharing

State of Colorado

2010

601 E. 18TH AVENUE, STE. 250, DENVER, CO 80203

This page left intentionally blank

Table of Contents

Introduction

There are many efforts across the State of Colorado by agencies at the state and local level to leverage information technology to improve information sharing for a variety of purposes and across a wide spectrum of domains, including criminal justice, public safety, education, health, social services, and transportation. It is recognized by the State Chief Information Officer, Governor, and the Colorado General Assembly that in order to more effectively serve citizens, improve the efficiency and effectiveness of state government, and to inform policy making, a strong program of information sharing is required across all lines of business the state serves.

Successful information sharing initiatives don't just happen; they require much work and dedication from the agencies and people involved in these efforts. Information sharing also requires a cultural adjustment by agencies, in terms of viewing things from a broader perspective and creating trust and meaningful dialogue across agency boundaries. Often, there is a strong need for a collaborative multi-agency partnership, but it dies because of lack of participation, poor project management, or no clear path forward to achieving the stated goals of the project.

These guidelines have been developed as an effort to standardize the approach for information sharing initiatives and to bring best practices to bear on these efforts. All OIT technical, policy and process standards that apply to the collaborative's information sharing initiative must be followed. The collaborative must submit documentation, including project charter, business requirements, technical requirements, regulatory information, and proposed system implementation and technology plan, to OIT's Enterprise Architect and Chief Data Officer for review and approval *prior* to beginning implementation

The target audience for this document includes agency directors, program managers, project managers, technology managers, and any stakeholder participant in an information sharing initiative. The Governor's Office of Information Technology hopes that the reader finds these guidelines helpful and useful.

Acknowledgement

This guide is based on the juvenile information sharing (JIS) guidelines prepared in 2006 by the Center for Network Development (CND) for the Office of Juvenile Justice and Delinquency Prevention (OJJDP). Those original guidelines suggest a course of action for key agency and organization stakeholders involved in a state or local effort to implement and sustain juvenile information sharing.

CND is partnering with the State of Colorado on the Colorado Children and Youth Information Sharing initiative, and we are appreciative of their efforts and guidance. We thank OJJDP for allowing us to use the JIS guidelines as a model for creating our own guidelines.

How the Guidelines are Presented

The guidelines are presented in four chapters that integrate the three critical components of information sharing – collaboration, confidentiality, and technology – into an effective developmental framework. Each chapter includes a brief introduction, guidelines, and a summary discussion of each guideline.

Chapter One provides direction for establishing an effective information sharing collaborative, as well as the governance structure and necessary project management.

Chapter Two guides agencies through assessment, strategic planning, and policy and procedure development to ensure the protection and security of private information, and achieve cross-agency integration and interoperability.

Chapter Three recommends the implementation of policies and procedures, training, and continuous quality improvement to ensure effective information sharing.

Chapter Four suggests policies for transparency, openness, and public communication regarding policies and procedures.

Chapter One: Establish the Collaborative

This chapter explores how to establish an information sharing collaborative responsible for developing, implementing, and maintaining an information sharing initiative focused on a specific domain area. An effective collaborative relies on key stakeholders instituting evidence-based collaborative principles, providing appropriate structure, ensuring project management, and following state enterprise standards.

Collaborations arise from the need to solve complex problems. Agencies and individuals participate in an information sharing collaborative when they perceive that they can accomplish more by working together than they can on their own. Although information sharing may be just one of several goals of the collaborative, for the purposes of these guidelines, this stakeholder group is referred to as the collaborative.

Guideline 1 – Establish a collaborative that includes key decision-makers from all relevant stakeholder groups who have the authority to make decisions on behalf of their agency or organization.

A. The stakeholder groups should represent the core services and systems integral to the primary outcomes desired by the collaborative. Leaders of these agencies and organizations should appoint a person of influence within their organization to champion information sharing. Some jurisdictions may also need to recruit decision makers from other agencies as needed to be members of the collaborative.

For example, in a juvenile justice information sharing collaborative, representative agencies should include:

- Child welfare
- Community services
- Education
- Juvenile justice and corrections
- Law enforcement
- Mental health
- Primary health care
- Substance abuse
- Technology

B. Engage representatives from the target population group in the collaborative.

It is critical to involve representatives from the community of interest (COI) on which information is being shared in the planning and development of the information sharing collaborative. By participating, these groups assume an active role and are included in the development of solutions that that affect their lives.

To continue the example of juvenile justice information sharing, representatives from youth and family groups should be invited to participate. Engaging and learning from youth and families also results in better collaborative decision making. Based on their experience navigating between various systems and agencies, youth and families can advise decision makers about effective information sharing practices. Typically, at-risk and delinquent youth and their families are engaged with multiple agencies, each of which collects similar information as part of intake and processing. They know that when agency decision makers have the information needed to make good decisions, they receive the services and assistance they need. For example, if a judge has accurate information from schools and services, court orders reflect a youth's current school performance and involvement in behavioral health treatment.

C. Consider other possible stakeholders in the information sharing collaborative.

The information sharing collaborative should examine gaps in resources or expertise and consider how involving other potential stakeholders may contribute to accomplishing their mission and performance goals. Other potential stakeholders could include:

- Businesses
- Elected officials
- Faith-based organizations
- Legal advisors
- Other collaborations serving the same COI
- Other agencies and organizations serving the same COI

For example, in juvenile justice information sharing, an elected official with a known interest in improving juvenile justice processes may bring important knowledge of policy issues that may impact juvenile information sharing. Given the range of federal, state and locally funded projects within a jurisdiction, it is also possible that other agencies or groups of agencies have made some progress towards cross-agency information sharing that is relevant to the goals of a juvenile justice information sharing collaborative.

Guideline 2 – Agree on and institute elements of effective information sharing.

Elements of effective information sharing should assist in creating a collaborative culture that embodies trust, mutual respect, direct and open communication, and responsiveness to the varied organizational and cultural perspectives represented. These elements could include items such as:

- Broad-based representation
- Commitment
- Communication and decision making
- Leadership and institutional support
- Mutual benefit
- Process and workflow
- Enterprise architecture standards
- Shared information models

- Resources
- Rewards and incentives
- Rules of engagement
- Shared ownership
- Shared vision
- Training
- Trust and respect

In addition, it is useful to keep in mind that:

- Collaboration is the process by which multiple stakeholders make a formal, long-term commitment to sharing resources to accomplish their vision. This process involves effective problem solving, negotiation, and willingness to compromise and commit to developing and implementing information sharing.
- Agencies and individuals collaborate when there are benefits and incentives to do so, such as improved organizational effectiveness and efficiency, and increased capacity and skills for the COI.
- Even though many of the collaborative agency members may maintain contact with some of their partner agencies, they rarely have a clear understanding of those agencies' legal mandates, policies, procedures, and resources. Cross-training increases understanding of agencies' mission, goals, and operations; contributes to a willingness to work together, and builds mutual processes and procedures.
- Trust is central to information sharing decision making and needs to be strategically nurtured. Before addressing confidentiality and information sharing issues, for example, members should have worked together long enough to have established mutual trust and understanding.
- Engaging collaborative members in determining how decisions are made contributes to building trust and shared ownership. Consensus and voting are two decision making methods used. Some collaborative find it useful to engage the initial assistance of an outside facilitator to help create decision making processes.

Guideline 3 – Establish a governance structure for the planning, implementation, and maintenance of the information sharing initiative.

The collaborative must institute a formalized governance structure to provide oversight and management of the development, implementation, maintenance, performance, and sustainability of information sharing. Members of the governing body may be a subset of a larger collaborative, and may also include additional ad hoc members with specific knowledge and expertise needed to achieve the information sharing goals and objectives.

Some collaboratives use a multiple committee structure (e.g., executive, operational, and technical committees) to focus members' skills and resources in their areas of expertise, and to ensure participation of end users in planning, testing and implementation.

To be effective, the governance structure employs procedures that facilitate information sharing. Such procedures include how decisions are made; incentives for sustaining key stakeholder participation; and the frequency and management of meetings procedures. Effective structure and procedures provide an operational framework for addressing issues of funding, investment, commitment, and sustainability, and for reconciling the diverse confidentiality practices and technology systems of the participating agencies.

The Government Data Advisory Board created through HB 09-1285 is one example of such a governance body.

Guideline 4 – Develop and agree on a shared vision, mission, goals, objectives, and outcomes for the information sharing initiative.

A shared vision is vital to the information sharing effort in the following ways:

- It establishes the ideal as the standard toward which to aspire.
- It helps improve upon existing conditions or creates a new way of doing business.
- It serves as motivation for change.
- It precedes success that is significant and lasting.
- It creates conditions for having an aligned information sharing collaborative.
- It drives the mission and goals.

A mission statement is a clear statement of the reason the information sharing collaborative exists. Goals are general statements about what the collaborative intends to accomplish and are consistent with the mission statement. Objectives are statements of intentions that refine goal statements and are specific, measurable, achievable, and consistent. The collaborative should think about, and document, the policy questions they are trying to address by linking siloed data together.

All of these must be included in the collaborative's project charter. A project charter is a statement of the scope, objectives and participants in a project. It provides a preliminary delineation of roles and responsibilities, outlines the project objectives, identifies the main stakeholders, and defines the authority of the project manager. It serves as a reference of authority for the future of the project.

Develop a written charter that describes:

- Purposes, including policy or service questions to be addressed.
- Public policy need(s).
- Participating agencies' ability to receive and disclose information on a "need to know" basis to fulfill their agency mandates.
- Types of policy questions being addressed.
- How participating agencies will use the data that is shared.
- Expected outcomes.
- Potential risks and issues, along with a mitigation plan.

The written purpose statement identifies information to be disclosed, accessed, and used by participating collaborative agencies. Examples of juvenile justice purpose areas are improving outcomes for youth, families, and communities protecting victims and public safety. The purpose statement should be also included in a memorandum of understanding, and can be used to introduce information sharing to the COI, policymakers, and the general public.

The collaborative must determine a set of measurable outcomes for these efforts. The COI(s) assist in determining these outcomes. A primary purpose for information sharing is to improve outcomes for the COI(s). Enlisting the COI's involvement in determining these outcomes should inform the development of performance measures and benchmarks. These outcomes should be documented and included in the project charter. Architectures and data models that minimize future changes or maximize flexibility and reuse should be a goal.

Guideline 5 – Designate, or hire, an individual or team to provide centralized project management for the development and implementation of the information sharing initiative.

Project management is essential to a successful information sharing project. Good project management helps deliver the greatest possible organizational benefits by minimizing the risk of project failure, increasing productivity and efficiently using time, money, and resources. A project manager will help the collaborative to invest the time necessary to gather information, think through all the details, and write a plan that will help ensure program success within the approved schedule and budget. An effective project manager also helps to foster shared ownership, responsibility, and commitment among the collaborative.

The collaborative should designate an experienced individual (or team) dedicated to managing the process from planning through implementation. Typically the project manager should be assigned by OIT or from within an agency and not outsourced.

Chapter Two: Develop Policies, Procedures and Practices

This chapter examines the elements necessary to develop an effective collaborative that provides participating agencies with timely and accurate information on a "need to know" basis, protects confidentiality of private information, and facilitates the exchange of information through integration and interoperability. As mentioned in Chapter 1, when agencies form a collaborative and governance structure, they are faced with the challenge of reconciling the diverse confidentiality practices and technologies of the participating agencies. Assessment and analysis of the legal authority to share information and existing technology infrastructure are therefore necessary to provide a foundation for strategic planning. Practices need to be determined to support the proposed operations and protect private information, policies and procedures. Such practices are guided by legal authority, and best available and appropriate technology, and are made available to the COI.

Guideline 6 – Enter into a Memorandum of Understanding (MOU) that is signed and endorsed by each participating agency.

As the development and implementation of information sharing is a long-term endeavor, it is essential to capture participating agencies' commitment to remaining consistent through changes in administration and leadership of the collaborative.

Participating agencies will use the MOU developed by the Government Data Advisory Board and published by the Office of Enterprise Architecture as the framework for their MOU. The collaborative will still need to verify the agreed upon arrangements of policies, procedures, practice, agency responsibilities, and resources for sharing information. The MOU documents the agencies' agreements on such criteria as:

- Collaborative purpose
- Governance
- Collaborative participating agencies and their responsibilities
- Shared funding and costs
- Legal authority for and restrictions on disclosure of information
- Common consent form
- Access to and use of information
- Information that will be shared
- Privacy policies and notification requirements
- Infrastructure for information sharing
- Information security
- Penalties for improper disclosure or use
- Auditing requirements
- Continuous quality improvement
- Maintenance of technology and software
- Training

- Resources to support information technology for participating agencies
- Communications support and resources
- Conflict resolution process

Guideline 7 – Assess the existing data systems infrastructure.

The existing data sharing infrastructure must be baselined to begin the development process. An inventory of all the types of information collected by participating agencies is needed. This analysis identifies which participating agencies collect which information needed to achieve the purpose. It also reveals redundancies and gaps in information collected.

The first step should be to review the existing agency data inventory contained in OIT's metadata repository. Next, non-inventoried data should be collected and entered into the central metadata repository via OIT's system and online tool. Finally, a gap analysis should be complete to identify what data that might be needed is missing or not collected, and determine availability from another source (internal or external) or develop a plan to begin collecting that data.

Then, the architecture of the participating agencies' information technology systems must be documented. The development and design of information sharing maximizes use of the overall architecture of the participating agencies, and must use enterprise architecture, policies, and standards developed by OIT. Technical and architectural decisions must be made from an enterprise-wide perspective to have the greatest long-term value for the state, rather than from any one particular organizational perspective. If possible, agencies will leverage existing technologies that have been implemented for other data sharing initiatives.

Guideline 8 – Identify information sharing opportunities and needs, as well as the information or data that is commonly exchanged between the members of the collaborative.

After completing the technology review, participating agencies can identify information sharing opportunities and needs using standard methods that will foster the exchange of information from disparate systems.

It is necessary to identify those who need access to the collected information, including those who will actively use the information sharing system. An understanding of who the users are provides a cursory level definition of the types of data that might be incorporated into the information sharing system Conceptual frameworks for these information sharing opportunities, business processes, and key events that trigger the need to share data should be detailed in documentation.

Collaborative participants should also take advantage of business process re-engineering when possible to modernize business processes as appropriate. This work will also help determine high-level policy and privacy issues at the planning stage.

Guideline 9 – Designate technology decision makers from each participating agency to participate in the information sharing system development.

It is important that key technologists from each participating agency be active in the planning and development processes. This involvement provides the collaborative with technical support and a well-rounded knowledge base of the existing technologies and systems.

Guideline 10 – Define data exchange points.

The initial development of data exchange points for information sharing should be modeled using the tools and services from OIT, and beginning with the OIT standards. If the collaborative wishes to use a new technology or methodology not covered by OIT standards, it should submit a written request to the Office of Enterprise Architecture.

Guideline 11 – Conduct a legal analysis and privacy impact on data needed for information sharing.

Each agency has a distinct mix of federal, state, and local legal authorities that guide the collection, disclosure, and use of personal information found in participating agency records. The collaborative must analyze the interaction of the relevant legal authorities to put appropriate protections in place for information sharing. For some agencies, both federal and state legal authorities may dictate information sharing practices (e.g., public education, child welfare, and health). In other agencies, information sharing practices such as law enforcement, courts, and probation, are primarily directed by state legal authority.

In our example of juvenile justice information sharing, in general, legal authority identifies:

- What information in a record is protected, such as name, address, school attendance, treatment status, and mental health diagnosis.
- Under what circumstances information can be released, such as imminent danger, suspected child abuse, or delinquency sentencing.
- Which individuals or agencies have access to protected information, such as parent, legal guardian, or court.
- “Mechanisms” that allow release of information, such as a signed consent to release by the client, or guardian, or a valid court order.
- Description of the responsibilities of recipients of information, such as a non re-disclosure of information.
- Legal mandates, if any, for release of certain information to certain agencies or the public, such as, sex offender records.

This information should be well-documented and written as part of the project management team’s files. This information should also be reviewed and updated annually for currency.

To ensure that privacy rights are protected, this assessment analyzes security practices regarding the types of data to be shared and maintained by participating agencies. The collaborative must ensure that OIT’s Office of Cyber Security’s policies are reviewed as part of this process. The results of the privacy

and security assessment inform the development of policies and procedures for managing potential privacy risks.

As the collaborative further examines and documents privacy and security requirements, it is important that technology representatives assist. Technology representatives should pay particular attention to how informed consent and security of personal information fit into the information sharing system design. These determine an agency's accessibility to the needed information when it is appropriate.

The end result of this assessment process is documented assurance that all privacy issues have been appropriately identified, and either adequately addressed, or, in the case of outstanding privacy issues, brought forward to senior management for further direction. When in doubt on an issue, the Office of the Attorney General should be consulted for a definitive opinion.

Guideline 12 – Formulate a strategic plan to achieve information sharing.

The strategic plan provides a roadmap for joint action and includes operations, performance, and monitoring. The plan delineates purpose, resource, milestones, timelines, a set of measureable outcomes, project management, actions, and the agencies and individuals responsible for executing the determined actions. The plan is realistic in scope and responsive to the available resources and capacities of the collaborative. To measure progress and sustain commitment, it is important that the actions, timeline, and milestones are designed to realize both short- and long-term objectives with measurable outcomes. To promote flexibility and responsiveness, the plan should incorporate strategies for a continuous improvement process to generate ideas, make decisions, and execute plans.

Guideline 13 – Identify and direct staff and funding resources that will be used for the information sharing collaborative.

Sustainability is critical for information sharing initiatives and discussion and planning for long-term sustainability should begin early in the collaborative's process. As the collaborative plans for cross-agency information sharing, it is important to address the costs to be shared among agencies, such as building and testing the application, training staff, and providing supportive services. In addition, the collaborative needs to consider how the information sharing system will be maintained, managed, and supported.

Guideline 14 – Develop the technical business requirements for information sharing, including all functions, businesses, processes and improvements to operations.

Technical business requirements provide direction for the information sharing system technology design. Business requirements encompass the practices necessary to perform daily operations. They include procedures for new information systems and services as well as new or updated policies and procedures that enhance new technologies. One phase of developing business requirements is reviewing and modernizing processes related to the information that the information sharing initiative is attempting to incorporate.

Security requirements tied to data security and privacy laws must be included. After assessing the threats to privacy and security of private information, the collaborative can determine appropriate and effective safeguards to address those risks. Administrative safeguards may include security clearance and pass codes, prohibiting attachment of unauthorized hardware to the system, and audits. Examples of physical security safeguards are secured desktop workstations, alarm systems, locking computer areas, and restricting access to authorized users within an agency. User access codes, firewall, multi-factor authentication, encryption, and automatic logoff are all examples of technical security safeguards. The collaborative will review all Office of Cyber Security and Office of Enterprise Architecture policies to ensure compliance with State enterprise security policies and technical standards.

Guideline 15 – Disclosure agreements.

Based on the legal analysis conducted in Guideline 11, the relevant laws the disclosure and mechanisms needed to authorize the disclosure (e.g., a legal mandate to share certain information between agencies, informed consent by the individual(s) whose information is to be disclosed, or a court order) will be known. Collaborative participants should agree that the information to be disclosed by each participating agency is based on legal authority and/or informed consent to release information by the individual and/or the individual's parent or legal guardian. They should also agree that participating agencies will not, without good cause, refuse to disclose the information necessary to achieve the information sharing initiative's purposes.

It is advisable that participating agencies agree to disclose all specified information, unless good cause exists to refuse. Examples of good cause are that federal and/or state law prohibits disclosure or the individual refuses to consent to the release of the information. In Colorado, agencies have explicitly been given statutory authority to share information, except where specifically prohibited by federal or state laws. C.R.S. **24-37.5-705** states:

> **Data sharing - authorization.** (1) WITH THE IMPLEMENTATION OF THE INTERDEPARTMENTAL DATA PROTOCOL, EXCEPT AS SPECIFICALLY PROHIBITED BY STATUTE, EACH STATE AGENCY IS AUTHORIZED, IN ACCORDANCE WITH THE PROVISIONS OF THE INTERDEPARTMENTAL DATA PROTOCOL, TO SHARE WITH THE FOLLOWING ENTITIES DATA COLLECTED IN THE COURSE OF PERFORMING ITS POWERS AND DUTIES:
>
> a) OTHER STATE AGENCIES;
> b) AGENCIES WITHIN THE LEGISLATIVE AND JUDICIAL DEPARTMENTS;
> c) POLITICAL SUBDIVISIONS; AND,
> d) NONGOVERNMENTAL ENTITIES AND INDIVIDUALS.

Collaborative agencies should also prohibit re-disclosure of personal information accessed through information sharing unless required or allowed. Members should also agree on the consequences for improper re-disclosure to third parties. Relevant legal authorities discourage re-disclosure of confidential information to third parties without client consent. Disclosure and re-disclosure policies will be contained in the collaborative MOU.

Guideline 16 – Design procedures to ensure that information disclosed by participating agencies is accurate and complete.

To achieve the collaborative's purpose(s), the information that is accessed and used must be accurate and complete. The policies and procedures developed by the Data Management Program and the Data Stewards Action Council within the Office of Enterprise Architecture will be put into place by all collaborative entities sharing data sets, and monitored to ensure information accuracy. These will address training, data validation, data updates, and quality assurance of data inputs and outputs. It is the responsibility of the agencies and data stewards to ensure the quality of the data within their systems.

Guideline 17 – Access agreements.

Whereas Guideline 15 deals with the disclosure of information, this guideline focuses on who may access this information. Participating agencies need to be fully informed on all sources of legal authority regarding confidentiality and information sharing, in order to determine who may access the information. These include federal or state laws, regulations, court order, court rules, case law, other legal authority, or by informed written consent. Documentation on every type of legal requirement should accumulated early in the process, reviewed and updated at least annually, and provided to all stakeholder groups. This information must be used to inform the data security classifications assigned to all data elements for access management provisioning. The state's data security classification policies can be found on the Office of Cyber Security's website.

Collaborative members should agree that participating agencies access and use only the information that is necessary to achieve the collaborative's purpose(s) and to support defined activities. Disclosure of, and access to, information that supports the collaborative's purpose is further limited to only the information needed to achieve the collaborative's goals. In statutes and regulations, limiting access to the "minimum necessary" information to effectively conduct activities is intended to control broad and unnecessary disclosure of private information.

Guideline 18 – Informed consent processes.

Privacy and information sharing policies provide transparency, protect participating agencies, and facilitate information sharing. These policies strengthen public confidence in the collaborative and its participating agencies' ability to handle information appropriately and support automated information sharing systems. Further, attention given to the development and implementation of these policies may prevent possible harm to individuals, public criticism, lawsuits, and legal liability.

Members should agree on a common process for obtaining informed consent for information release that provides adequate verbal and written notice and is linguistically appropriate. Most laws regarding confidentiality of agency records allow disclosure of personal information with written informed consent of the individual, youth, parent(s), or legal guardian. The collaborative's analysis of relevant legal authority governing release of information determines the need for informed consent. Whenever possible, written, informed consent is the preferred method for obtaining authorization to disclose confidential information.

"Informed consent" requires that the individual provide consent with a full understanding of what information is likely to be shared, with whom and under what circumstances, what information can be released to whom without their consent, and consequences for unauthorized disclosure. A common informed consent process provides adequate written and verbal notice and a consistent approach among the participating agencies. To ensure that the consent is "informed", participating agencies need to be aware of any cultural or linguistic factors that may impact the individual's ability to understand the consent process, including the need for interpretive services.

A common consent form used by all participating agencies reinforces the common informed consent process. Included in the consent form should be items such as:

- Identifies the individual(s) who the information is about.
- Identifies the agency that is disclosing the information.
- Clarifies the information sharing purposes – to include language broad enough for all collaborative members' needs.
- Defines the reasons for disclosing the information.
- Identifies the agencies that will access or receive the information.
- States the expiration date of the consent to release information or the circumstances upon which the consent automatically expires.
- Identifies the ways that the disclosed information will be used – again, to cover all collaborative members' needs.
- Delineates the limitations on the disclosure and/or use of the information.
- Describes agency practices regarding sharing of non-confidential, as well as confidential information.
- Explains the manner in which consent can be revoked.
- Policies for the individual to review their information.
- Lists the grievance procedures for suspected unauthorized disclosure or use of the information.
- Outlines the penalties for unauthorized disclosure or use of the information.

The elements noted above are a common set found in relevant statues and regulations. The consent form can also include language explaining that once an agency discloses information to another pursuant to the individual's written consent, the original agency is not responsible for any subsequent disclosures. However, participating agencies need to agree on the penalties and processes for any such unauthorized disclosure or use of confidential information. Once agreed upon, a copy of these penalties and processes must be provided to the individual.

Despite assurance of privacy protection, an individual may not want specific personal information disclosed. When an individual refuses to provide consent, in part or in total, they should not be denied services based on their refusal unless the information is necessary to determine eligibility for services. It is the participating agencies' responsibility to ensure that the individual understands that they are not required to consent to the release of any personal information; the consequences, if any, of not providing consent; and, if their refusal may hinder the delivery of services.

Regardless of the collaborative's composition, a minimum level of confidentiality needs to be set and agreed to by all participating agencies. The collaborative should have the Office of the Attorney General's Chief Privacy Officer review and approve these policies.

Guideline 19 – Develop accessible processes and procedures for individuals to review information that is collected about them and that may be disclosed. Provide them with the procedures and opportunity to approve and/or amend their information.

Laws and other legal authority regarding confidentiality of agency records generally afford individuals the right to see and have copies of their information. Additionally, providing opportunities for review and amend that information can help ensure that it is accurate and current. Participating agencies should follow the Office of Enterprise Architecture's procedures for review and amending information, unless there is a superseding federal requirement, and notify individuals of these procedures. Information regarding these procedures is typically provided through agency notices required by federal and state laws.

It is recommended that the collaborative's informational materials about confidentiality policies and procedures be user-friendly, that is, written in language that is developmentally appropriate, easily understood, and available in the primary languages of most affected individuals. A user-friendly approach should also be used for materials that inform individuals on how to assert their privacy rights.

Guideline 20 – Develop a collaborative policy framework that establishes or enhances the information sharing standards and guidelines for information management.

Develop policies to guide the protection of information exchanged electronically between systems. Utilize the policies and technical standards developed by the Office of Enterprise Architecture and the Office of Cyber Security for technical standards, records management practices and standards, privacy design principals, security standards, and access management standards, to ensure that the collaboration's information sharing practices are performed using enterprise organizational and industry standards.

Guideline 21 – Develop a policy and procedural methodology for the incorporation of new agencies into the information sharing collaborative.

As the collaborative identifies new agencies to participate in information sharing, the collaborative's business model should include policies and procedures to incorporate new agencies into the overall design. It is important that new partnering agencies have a similar vision and goals to those of the existing collaborative. As part of the design strategy, this prevents redesign of the system architecture and data.

Guideline 22 – Designate representative(s) from each participating agency who will be responsible for their agency's implementation of and compliance with the collaborative's policies and procedures.

The collaborative's participating agencies are accountable for the implementation of and compliance with collaborative policies and procedures within their own agency. Each participating agency needs to identify and make known the individual(s) from their agency who will be responsible for collaborative privacy, security, and technology. This typically will be a program manager or director.

Chapter Three: Implement Information Sharing

This chapter discusses methods to effectively implement information sharing initiatives by complying with established policies, procedures and practices, training, and monitoring. Quality training and change management, both initial and ongoing, enables information sharing users to maximize the benefits of information sharing. Ongoing monitoring and assessment ensures that appropriate processes and procedures are in place to maintain the integrity and intended purpose of information sharing. Outcomes established by the collaborative are measured by benchmarks and addressed through a continuous improvement strategy.

Guideline 23 – Develop information sharing architecture.

All OIT technical, policy and process standards that apply to the collaborative's information sharing initiative must be followed. The collaborative must submit documentation, including project charter, business requirements, technical requirements, regulatory information, and proposed system implementation and technology plan, to OIT's Enterprise Architect and Chief Data Officer for review and approval *prior* to beginning implementation

Begin implementing the new technology systems architecture in a phased manner. Identify a viable pilot to include one to two agencies and one to two data exchanges. Identify best practices and lessons learned from the pilot to include in future work as the project continues to roll out.

Guideline 24 – Implement collaborative policies, procedures, and practices.

Collaborative agencies should implement the policies, procedures, and practices that were determined through strategic planning and delineated in the Memorandum of Understanding. Compliance is monitored by individual agencies, project management, the Office of Enterprise Architecture, and the collaborative as a whole. Collaborative participating agencies monitor implementation and compliance within their own agencies. The Office of Enterprise Architecture, collaborative project management, and the collaborative monitor compliance across the participating agencies, and address compliance issues and requests for modifications.

Guideline 25 – Agree that collaborative participating agency managers and staff participate in thorough and ongoing instructional training on collaborative policies, procedures and practices.

Successful information sharing occurs when users are trained in all aspects of the system including purpose, benefits, expected outcomes, policies, and procedures. Training and change management is designed to be ongoing and flexible. Effective training incorporates a combination of teaching methods to accommodate the trainees' learning styles, readiness for change, and experience with technology.

Guideline 26 – Assess and refine the performance measures and benchmarks for information sharing and agree that collaborative participating agencies provide the necessary data for measurement.

A good planning process operates continuously and links planning with results. To determine measurable outcomes, the plan needs to include process and outcome evaluation benchmarks, and

agency commitment to provide the necessary data. Examples of indicators for transparency, openness, and public communication are annual reports, public relations material, accessible minutes and reports, and newsletters. Mission and planning performance indicators could include: a written mission statement, a written strategic plan, risk management policies, and program outcome measures. Benchmarks are set to document interim achievements and demonstrate progress towards information sharing. An MOU, for example, indicates readiness to begin information sharing implementation.

Guideline 27 – Conduct periodic assessments of collaborative policies and procedures to ensure that new requirements are included within the technological frameworks of participating agencies.

Periodic assessments are conducted to ensure that policies and procedures foster an effective environment and support information sharing users. The collaborative and project manager are responsible for ensuring alignment of the collaborative's policies, procedures, and technology with periodic examinations and reviews. As policies and procedures are introduced or modified, the new requirements they present should be incorporated into the information sharing technology framework to ensure that they are supported by appropriate information exchange and security methods.

Guideline 28 – Reach agreement on participating agencies' responsibilities for auditing user activities involving information sharing. Determine how long audit logs are to be retained.

An audit trail is important to track appropriate access to information and provides the collaborative's governance structure with information needed to monitor confidentiality and security. An audit trail records activities such as event type, data and time of event, user identification, success or failure of access attempts, and security actions taken by system administrators or security officers. OIT's audit policies and procedures will be followed by the collaborative.

Chapter Four: Promote Public Awareness

This chapter recommends a policy of transparency, openness, and public communication regarding information sharing. Information sharing affects the COI(s) on many levels, possibly including health, wellbeing, safety, and privacy. Educating the public and policymakers about information sharing processes, policies, procedures, and impacts is critical to engendering trust and support.

Guideline 29 – Follow OIT's general policy of openness about developments, practices, and policies with respect to the management of personal information and data.

The collaborative agrees on a general policy of transparency and openness that enables the public to have access to the collaborative's policies. This is not to be interpreted to mean that the public has access to confidential information. Rather, the public has access to policies that explain how confidential information is protected and shared to demonstrate that the collaborative's participating agencies properly protect the privacy of the COI(s).

Guideline 30 – Agree that collaborative decision-making processes, plans, practices, policies, and evaluation results are open to the public and made available on a timely and predictable basis.

The public has an interest in agencies' effectiveness, efficiency, information privacy, and security. Open processes and policies for information sharing afford the public the opportunity to learn about the collaborative's purposes, development, design, and outcomes. Openness can also garner public engagement and support, and is important to addressing public concerns about how information sharing compiles with legal authority for information exchange and protects private information.

Guideline 31 – Establish a collaborative communications plan and media strategy.

A communications plan determines all aspects of how information about the collaborative is conveyed to various audiences, including collaborative agencies, other interested parties, the media, and the public. This plan covers both internal and external collaborative communications and the means by which they are delivered. The collaborative should periodically review, assess, and adjust the plan as needed. This will ensure that communication remains open and direct. It will also provide an opportunity to address any communication issues that may arise.

Guideline 32 – Educate the public, including lawmakers and policymakers, about the purpose of information sharing, how private information is protected, and how information sharing facilities improvements in program outcomes.

The collaborative's participating agencies should reach agreement on messages that are used to promote information sharing: such as on improved efficiency and outcomes. Public education communicates the collaboratives' purpose and outcomes, and how information is gathered to achieve

the goals of improved outcomes. Public education also covers limits on disclosure and use of information to authorized users only on a “need to know” basis.

Further, it is important to reach agreement on how these messages and other relevant information are disseminated. For instance, the collaborative can develop an information Web site to post information for the general public and potential partnering agencies. The Web site can provide information on how to participate in the collaborative, the information sharing history, policies, funding sources, information sharing in general, and information on and links to each participating agency.

Appendix: Document Checklist

List of possible stakeholder groups

Create a list of all possible stakeholder groups to engage in discussion about the initiative. This document ties to Guidelines 1.

Project charter

A project charter provides the specific purpose(s), goals, objectives, risk analysis, and key stakeholders for the information sharing initiative. This document ties to Guideline 4.

Data and systems inventory

The data and systems inventory will provide critical information regarding data that is currently being collected by the stakeholders, the systems that support the data collection efforts, and will enable a gap analysis to identify what data is missing that should be collected. This information ties to Guideline 7.

Regulatory and compliance environment inventory

The regulatory and compliance environment inventory will provide an overview of all federal and state laws that regulate the collection, storage, sharing, and destruction of each of the data elements involved in the data sharing effort. This information ties to Guideline 7, 11, and 15.

Business process workflow inventory

A business process workflow inventory should be done to identify how data is collected and used in workflow processes, as well as who needs access to data for what purposes, and how that information is being shared or routed today. This information ties to Guideline 7 and 8.

Consent notice and form

The consent form allows the re-distribution of individual's data under certain circumstances. This document ties to Guideline 18 and 19.

Memorandum of Understanding

The Memorandum of Understanding is a legal agreement that defines the stakeholders' participation in the data sharing initiative. This document ties to Guideline 6.

Metrics Sheet

Identify key performance metrics to show how the project will be baselined and how performance will be measured. This document ties to Guideline 4 and 26.