Guidelines for Juvenile Information Sharing

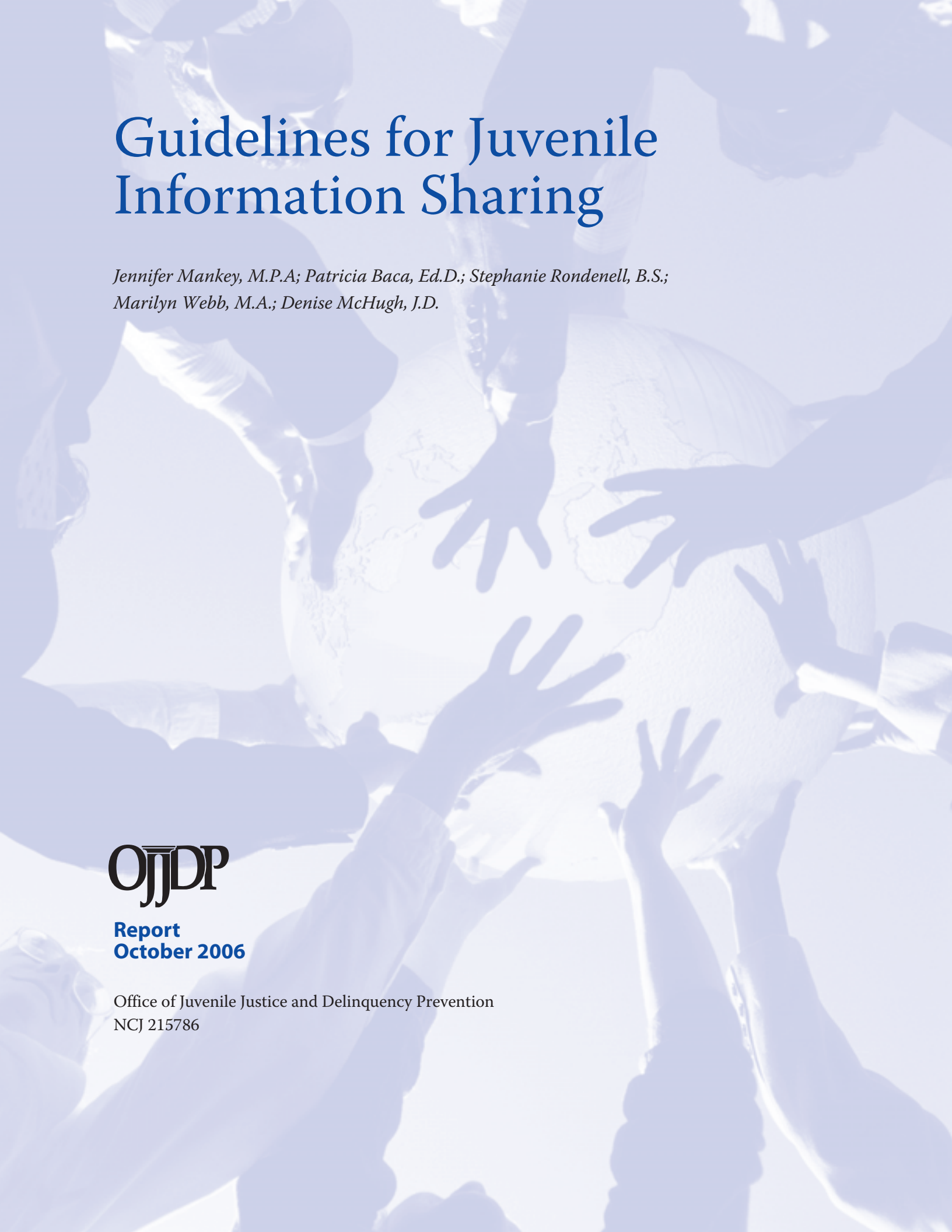
OJJDP

report

U.S. Department of Justice
Office of Justice Programs
Office of Juvenile Justice and Delinquency Prevention

Guidelines for Juvenile Information Sharing

Jennifer Mankey, M.P.A; Patricia Baca, Ed.D.; Stephanie Rondenell, B.S.; Marilyn Webb, M.A.; Denise McHugh, J.D.



OJJDP

Report
October 2006

Office of Juvenile Justice and Delinquency Prevention
NCJ 215786

Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Alberto R. Gonzales
Attorney General

Regina B. Schofield
Assistant Attorney General

J. Robert Flores
Administrator
Office of Juvenile Justice and Delinquency Prevention

Office of Justice Programs
Partnerships for Safer Communities
www.ojp.usdoj.gov

Office of Juvenile Justice and Delinquency Prevention
www.ojp.usdoj.gov/ojjdp

These guidelines were prepared by the Center for Network Development, and supported by grant number 2000-JN-FX-K004 from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice.

The Office of Juvenile Justice and Delinquency Prevention is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, and the Office for Victims of Crime.

Table of Contents

Acknowledgments

The juvenile information sharing (JIS) guidelines were prepared by the Center for Network Development (CND) for the Office of Juvenile Justice and Delinquency Prevention (OJJDP). The 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.

The JIS guidelines draw on the experience and expertise of many who work in youth-serving agencies and information technology initiatives throughout the United States.

Gratitude is extended in particular to the professionals who have served on the Juvenile Information Sharing Advisory Group and to those who served as peer reviewers of the draft guidelines.

Appreciation also goes to J. Robert Flores, Administrator, Office of Juvenile Justice and Delinquency Prevention (OJJDP), who has set an example for cross-agency collaboration and communication, and to Gwendolyn Dilworth, Program Manager, Demonstration Programs Division, OJJDP, who has worked steadfastly in support of juvenile information sharing as a means to improve services to youth.

JUVENILE INFORMATION SHARING ADVISORY GROUP

Paul Embley
G&H International Services, Inc.

Anne Gardner
Assistant United States Attorney, U.S. Attorney's Office, Eastern District, Arkansas

Julie Spence Gefke
Former Privacy and Security Officer, State of Colorado, Department of Health Care Policy and Financing

Ken Gill
Former Technology Advisor, Bureau of Justice, Office of Justice Programs

Jim Ham
Information Technology Juvenile Justice Manager, Arizona Supreme Court

Blake Harrison
Program Principal, Criminal Justice, National Conference of State Legislatures

Emmitt Hayes
SASD Director, Travis County, Texas, Juvenile Probation Department

Bill Hughes
Information Technology Programming Specialist, Arizona Office of the Courts

Bernie Martinez
Director, Migrant Education Program, Colorado Department of Education

James McMillan
Principal Court Technology Consultant, National Center for State Courts

Richard Morris
Project Coordinator, U.S. Department of Labor, Office of Youth Services

Carolyn Nava
President, Youth Leadership International

Leroy Rooker
Director, Family Policy Compliance Office, U.S. Department of Education

LaChundra Thomas
Child Welfare Program Specialist, U.S. Department of Health and Human Services

Gary Waint
Division Director, Juvenile and Adult Court Programs, Missouri Office of State Courts Administrator

Jennifer Zeunik
Project Manager, Law Enforcement Technology Standards Council Technology Center, International Association of Chiefs of Police

JUVENILE INFORMATION SHARING GUIDELINES PEER REVIEWERS

Bobbie Chinsky
Program Manager, Juvenile Justice Services Division, Arizona Administrative Office of the Court

Paul R. Eik
Program Manager, State of New Mexico Children, Youth and Families Department

Doug Engle
Director, Office of Technology and Information Services, Georgia Department of Juvenile Justice

Honorable Ernestine S. Gray
Judge, Orleans Parish (Louisiana) Juvenile Court

Denise Hotopp
Director, Polk County (Iowa) Decategorization

Nicole Lievsay
Director, Juvenile Justice Initiatives, Harris County (Texas)

William Lutz
Director, Juvenile Assessment Center, 18th Judicial District (Colorado)

Eileen Madigan
Juvenile Justice Information System Coordinator, Crime Prevention and Justice Assistance Division, Hawaii Department of the Attorney General

Michael Overton
Project Manager, Nebraska Crime Commission

Tricia Schlechte
Deputy Department Director, Health and Public Health, Missouri Department of Health and Senior Services

Julie Slayton
Chief Research Scientist, Program Evaluation and Research Branch, Los Angeles Unified School District

Wansley Walters
Director, Miami-Dade Juvenile Assessment Center

Introduction

State and local jurisdictions across the United States are working to improve information sharing among key agencies responsible for community safety and the health and wellbeing of at-risk youth and juvenile offenders. These juvenile justice and other youth-serving agencies often have difficulty receiving timely and reliable information needed for conducting assessments and determining appropriate supervision, sanctions, incentives, and services for youth.

In concert with the U.S. Department of Education (DOE) and the Substance Abuse and Mental Health Services Administration (SAMHSA), the Office of Juvenile Justice and Delinquency Prevention (OJJDP) identified juvenile information sharing (JIS) as an essential tool to assist juvenile justice, education, health, and other youth-serving agencies in their efforts to improve services for at-risk and delinquent youth and their families. JIS benefits jurisdictions by:

- Enabling decisionmakers to electronically access and exchange critical information at key decision points.
- Facilitating more efficient access to data and information from multiple locations.
- Improving data quality.
- Eliminating redundant data collection and entry.

Achieving effective juvenile information sharing, however, requires a significant shift in the information sharing practices of many agencies. JIS institutes new processes and procedures for information sharing and requires the development and application of new knowledge and skills.

In 2000, OJJDP awarded a cooperative agreement to the Center for Network Development (CND) to increase the capacity of jurisdictions to plan and implement juvenile information sharing through the Information Sharing to Prevent Juvenile Delinquency: A Training and Technical Assistance Project. A national needs assessment of JIS practices revealed that a variety of approaches were being used with varying degrees of success. Agencies typically were challenged in their efforts to:

- Build effective collaborations of multiple agencies responsible for developing juvenile information sharing.
- Develop and agree on confidentiality practices to protect private information based on statutes and policies relating to juvenile information exchange.
- Employ appropriate technology to facilitate access to and secure information.

Instructional training and followup assistance were delivered to help multiple agency teams across the country implement strategies to meet those challenges.

Participants in regional JIS training workshops and other youth-serving professionals affirmed the need for assistance and further emphasized the value of a standardized approach for JIS development and implementation to bridge diverse information sharing practices and policies.

In response, OJJDP endorsed the development of JIS guidelines as a critical step toward achieving agreement on appropriate information to share within jurisdictions and as mechanisms for effective and efficient information sharing.

Background

The emergence of electronic information sharing for justice purposes began in the 1990s, when advances in technology made it possible to automate the collection of and access to information by various related justice agencies such as courts and probation. Arizona, a pioneer in automating juvenile justice information exchange, implemented the Juvenile Online Tracking System (JOLTS), a statewide juvenile probation and dependency system, in 1993.

Concurrently, policies and service approaches for at-risk youth and juvenile offenders increasingly were moving toward the coordination of multiple agency efforts. The Office of Juvenile Justice and Delinquency Prevention (OJJDP), and other federal departments such as the Substance Abuse and Mental Health Services Administration and the U.S. Department of Education, were promoting information sharing among juvenile justice, education, and other youth-serving agencies to support a comprehensive continuum of care and services. State legislatures were endorsing information sharing to streamline services and protect communities. From 1993 to 2000, 35 states enacted new legislation regarding juvenile records. For example, laws allowing information sharing among juvenile justice agencies and school districts were enacted in response to incidents of lethal violence in schools and communities nationwide. In addition, policymakers requested that agencies provide accurate data to measure program effectiveness, costs, gaps, or redundancy.

As integrated information technology was evolving, so was the potential for its application to information sharing that included multiple youth-serving agencies outside of justice systems. Nevertheless, jurisdictions experienced other significant barriers to the sharing of multiple agency information including concerns of confidentiality and privacy of information, blurred lines of authority, gaps in data integration, service fragmentation, and distrust among different agencies. Through the OJJDP Information to Prevent Juvenile Delinquency: A Training and Technical Assistance Project, CND provided training and technical support to multiple agency jurisdictional teams who demonstrated interest in enhancing their information sharing capabilities.

The scope and array of agencies that participated in the CND training and technical assistance activities illustrates that, despite the challenges of juvenile information sharing, youth service agencies are committed to improving information sharing and are searching for ways to implement it across agencies. One-hundred-seven (107) teams of youth service agencies from state and local jurisdictions across the country participated in JIS trainings, including: judges and court administrators, law enforcement, probation and parole officers, defense attorneys, prosecutors, school administrators, technology staff, child welfare administrators and case workers, government officials, state juvenile justice specialists, medical and mental health service providers, diversion program managers, juvenile corrections administrators and staff, prosocial service providers, family advocates, substance abuse treatment counselors, detention and institutional agency administrators, community-based prevention program administrators, and community representatives. There were also representatives of collaborations involved in a continuum of service programs; for example, Juvenile Accountability and Incentive Block Grant, Serious and Habitual Offender Comprehensive Action Program, Safe Schools/Healthy Students, Safe Start, and Safe Kids/Safe Streets programs.

The Need for JIS Guidelines

Because of the challenges posed by the diversity of information sharing practices and policies, agency representatives have requested a promising, research-based blueprint for JIS development, to include protocols and examples of practices for effective collaboration, confidentiality, and technology.

To keep JIS training and follow-up assistance current, CND tracked developments in both adult criminal and juvenile justice information integration initiatives, resources, and programs. Over the past decade, the adult sector benefited from new technology, privacy protocols, and policies that facilitated the development of integrated models for adult criminal justice information sharing. In contrast, less attention and fewer resources were devoted to the development of standardized practices for the juvenile sector. Youth service agencies attempted to develop juvenile information sharing without the benefit of a framework specific to the principles of youth-serving agencies. As a result, juvenile information sharing approaches neither the level of practice nor prevalence of integrated information sharing found in adult criminal justice. Furthermore, the technology advances, protocols, and policies recommended for the adult sector cannot be adopted without significant modification for the juvenile sector due to differences in processes and scope.

OJJDP made the development of JIS guidelines a priority for the Information Sharing to Prevent Juvenile Delinquency project, ensured coordination with the Office of Justice Programs' Information Technology Initiatives, provided resources, and actively participated in the JIS Advisory Group deliberations.

The Development of JIS Guidelines

In January 2004, CND convened a JIS Advisory Group of professionals from various agencies and disciplines, and a family programs' advocate to ensure that the guidelines incorporated the breadth of youth-serving agencies. The Advisory Group used a comprehensive guide of principles and practices compiled by CND through an extensive assessment of existing information sharing principles, practices, and standards of youth-serving agencies.

The investigation of collaboration principles and practices included:

- Models for delinquency prevention.
- Education.
- Juvenile justice.
- Mental health systems of care.
- Adult criminal integrated justice policies and governance.
- Community and nonprofit collaboration.

The investigation of confidentiality practices and privacy protections included federal and state confidentiality laws relevant to:

- Child welfare records.
- Substance abuse treatment records.
- Runaway and homeless youth records.
- Mental health records.
- Public records acts.
- Juvenile court and juvenile probation records.
- Child protection records.
- Prosecution records.
- Law enforcement records.
- Public education records.
- Medicaid.
- Interstate compact records.
- Federal youth offender records.
- Self sufficiency program records.
- Medical and behavioral health records (e.g., Health Insurance Portability and Accountability Act).

In addition, recommended standards of practice included:

- Information sharing principles and standards for multiple agency collaborations.
- Professional licensing protocols.
- Professional codes of ethics or conduct.
- Specialized services standards of practice (e.g., pre-trial release, detention).
- Standards for multiple agency information sharing.

The investigation of technology protocols, methods, and applications included:

- Standards for specific process areas within justice and public safety (e.g. Probation Functional Protocols and Law Enforcement Functional Protocols).

- Technology standards produced for local and state government and for the justice and public safety environment (e.g., Court Functional Protocols).
- Extensible markup language (XML) applications in justice and other environments.
- At-risk youth and juvenile justice specific data reference models.
- Statewide Automated Child Welfare Information System.
- Health Insurance Portability and Accountability Act.
- State technology standards.

The JIS Advisory Group contributed local, state, and federal expertise in such areas as: multiple agency partnerships, confidentiality, technology, juvenile justice, behavioral health, law and policy, child welfare, youth and families, law enforcement, labor, and information systems management, design and implementation. The Group reviewed information sharing practices of youth-serving agencies and disciplines; deliberated relevant laws, policies, and practices; investigated various resources and technology advances in the adult and juvenile sectors; and identified essential principles for collaboration, confidentiality and technology. Members vetted and approved draft recommendations for JIS guidelines, and used the results of expert peer review to recommend modifications for the final version of the guidelines.

How the Guidelines are Presented

The guidelines are presented in four chapters that integrate the three critical components of juvenile 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. A glossary of relevant terms and references is provided at the end of the Guidelines.

Chapter One provides direction for establishing an effective JIS 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 about youth, families, and victims, and achieve cross-agency integration and interoperability.

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

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

Chapter 1. Establish the JIS Collaborative

This chapter explores how to establish a juvenile information sharing (JIS) collaborative responsible for developing, implementing, and maintaining juvenile information sharing. An effective JIS collaborative relies on key stakeholders instituting evidence-based collaborative principles, providing appropriate structure, and ensuring project management.

Collaborations arise from the need to solve complex problems. Agencies and individuals participate in a JIS collaborative when they perceive that they can accomplish more by working together than they can on their own. Although juvenile 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 JIS collaborative.

Guideline 1

Establish a JIS collaborative that includes key decisionmakers from the following groups who have the authority to make decisions on behalf of their agency or organization:

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

The groups listed above represent the core services and systems responsible for the health and wellbeing of youth and their families. Leaders of these agencies should appoint a person of influence within their organization to champion juvenile information sharing. Some jurisdictions may also need to recruit decisionmakers from other agencies, (e.g., domestic violence) as needed to be members of the JIS collaborative.

Guideline 2

Engage youth and family representatives in the JIS collaborative.

It is critical to involve youth and families in the planning and development of a juvenile information collaborative. By participating, youth and their families assume an active role and are included in the development of solutions that affect their lives. Sources for youth and family representatives include JIS collaborating agencies and youth or family advocacy organizations.

Engaging and learning from youth and families also results in better JIS decisionmaking. Based on their experience navigating between various systems and agencies, youth and families can advise decisionmakers 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 decisionmakers 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.

For youth and families involved in juvenile information sharing, it is important that confidentiality continue to be recognized and maintained within the collaborative. Any disclosure of youth- and family-specific information needs to be based on appropriate legal authorization.

Guideline 3

Consider other possible stakeholders in the JIS collaborative, such as:

- **Businesses.**
- **Elected officials.**
- **Faith-based organizations.**
- **Legal advisors, e.g., general counsels, prosecutors, defense attorneys.**
- **Other collaborations serving youth.**
- **Other youth-serving agencies and organizations.**

The JIS collaborative should examine gaps in resources or expertise and consider how involving other potential stakeholders may contribute to accomplishing their mission and performance goals. For example, 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 the JIS collaborative.

Guideline 4

Agree on and institute elements of effective JIS collaboration. For example:

- **Broad-based representation.**
- **Commitment.**
- **Communication and decision-making.**
- **Leadership and institutional support.**
- **Mutual benefit.**
- **Process and workflow.**
- **Resources.**
- **Rewards and incentives.**
- **Rules of engagement.**
- **Shared ownership.**
- **Shared vision.**
- **Training.**
- **Trust and respect.**

The elements listed above assist in cultivating a collaborative culture that embodies trust, mutual respect, direct and open communication, and responsiveness to the varied organizational and cultural perspectives represented. 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 juvenile 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 youth and families.
- Even though many of the JIS 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' missions, goals, and operations; contributes to a willingness to work together; and builds collaborative processes and procedures.
- Trust is central to JIS decisionmaking 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 JIS collaborative members in determining how decisions are made contributes to building trust and shared ownership. Consensus and voting are two decisionmaking methods used. Some collaboratives find it useful to engage the initial assistance of an outside facilitator to help create decisionmaking processes.

Guideline 5

Establish a governance structure for the planning, implementation, and maintenance of JIS.

The JIS collaborative institutes a formalized governance structure to provide oversight and manage the development, implementation, maintenance, performance, and sustainability of juvenile 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 juvenile information sharing.

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

To be effective, the governance structure employs procedures that facilitate juvenile 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 JIS participating agencies.

Guideline 6

Designate, or hire, an individual or team to provide centralized project management for the development and implementation of JIS.

Developing juvenile information sharing requires dedicated and expert project management. The designated individual or team is responsible for managing the process from planning through implementation. Project management helps to foster shared ownership, responsibility, and commitment, and is effective and successful when it is performed:

- According to accurately defined and agreed upon objectives.
- On schedule.
- Within an approved budget.

Guideline 7

Initiate a planning agreement that articulates the purpose and agreed-upon actions for the development of juvenile information sharing.

JIS collaboratives enter into a planning agreement to formalize the purpose of juvenile information sharing and each agency's commitment to developing a collaborative. This planning agreement differs from the Memoranda of Understanding (MOU) discussed in Chapter 3, which relates to JIS participating agency commitments with regard to implementation and operations. Each of the following elements is essential to a complete planning agreement:

- General covenants: what all JIS collaborating members agree to do collectively to develop juvenile information sharing.
- Specific covenants: what each JIS collaborative member agrees to do individually to develop juvenile information sharing.
- Administrative provisions: the effective date of the agreement, procedures for monitoring and modifying it, etc.
- List of JIS collaborative members and their signatures.

Chapter 2. Develop JIS Policies, Procedures, and Practices

This chapter examines the elements necessary to develop an effective JIS 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 youth-serving agencies form a JIS 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 youth and families.

Guideline 8

Determine and agree on the purpose(s) for juvenile information sharing. Develop a written statement that describes:

- **Purposes.**
- **Public policy need(s).**
- **Participating agencies' ability to receive and disclose information on a "need to know" basis to fulfill their agency mandates.**
- **How participating agencies will use the data that is shared.**
- **Expected outcomes.**

The written purpose statement identifies information to be disclosed, accessed, and used by JIS participating agencies. Examples of JIS purpose areas are improving outcomes for youth, families, and communities protecting victims' and public safety. The purpose statement is included in the JIS collaborative's Memorandum of Understanding as described on page 22 in Chapter 2, and can be used to introduce juvenile information sharing to youth, families, policymakers, and the general public.

Guideline 9

Conduct an analysis of what information is currently collected by JIS participating agencies, and what additional information is necessary for agencies to achieve the JIS purpose(s).

An inventory of all the types of information collected by JIS participating agencies is needed. This analysis identifies which JIS participating agencies collect which information needed to achieve the JIS purpose. It also reveals redundancies and gaps in information collected.

Guideline 10

Determine who needs the information (JIS users).

It is necessary to identify those who need access to the information collected, including those who will be actively using

the JIS system. An understanding of who the users are provides a cursory level definition of the types of data that might be incorporated into the JIS system. It also helps determine high-level policy and privacy issues at the planning stage.

Guideline 11

Designate technology decisionmakers from each JIS participating agency to participate in JIS development.

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

Guideline 12

Conduct a technology review of all available modeling tools and methodologies to capture detailed information of the JIS participating agencies.

To begin the initial development of data exchange points for juvenile information sharing, the technology representatives should review all of the tools and services available. New technologies and methodologies now provide foundational practices for information sharing, and there are several tools developed specifically for use in the justice community (e.g., Global Justice Extensible Markup Language Data Model).

Guideline 13

Identify data exchange points and the information or data that is commonly exchanged between the members of the JIS collaborative.

After completing the technology review, JIS participating agencies can create data

exchange points using standard methods that will foster the exchange of information from disparate systems. Conceptual frameworks for these data exchange points have been developed for adult criminal justice and help define key events that trigger the need to share data, and to identify those agencies involved in the information sharing event (e.g., Justice Information Exchange Model [JIEM] developed by Search). A definition of JIEM can be found in the Glossary, see page 33.

Guideline 14

Conduct a legal analysis to identify private information that can be disclosed to and accessed by certain JIS participating agencies.

Each state has a distinct mix of federal, state, and local legal authorities that guide the collection, disclosure, and use of personal information found in JIS

participating agency records. The JIS collaborative must analyze the interaction of the relevant legal authorities to put appropriate protections in place for juvenile 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 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.
- What 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 no re-disclosure of information.
- Legal mandates, if any, for release of certain information to certain agencies or the public, such as, sex offender records.

Guideline 15

Assess the impact on privacy and security when deciding what information may be shared through juvenile information sharing.

Based on the legal analysis performed in Guideline 14, a privacy and security assessment should be conducted to determine if juvenile information sharing meets basic privacy requirements. This assessment includes an examination of all relevant legislation, policies, and business practices that support electronic information sharing among JIS participating agencies.

To ensure that privacy rights are protected, this assessment analyzes security practices regarding the types of data to be shared and maintained by JIS participating agencies.

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

"The end result of the 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." (Treasury Board of Canada, 2002)

Guideline 16

Assess the enterprise architecture of the JIS participating agencies' information technology systems.

The development and design of juvenile information sharing maximizes use of the overall enterprise architecture of the JIS participating agencies. Decisions made from an enterprise-wide perspective will have a greater long-term value than decisions made from any one particular organizational perspective.

Guideline 17

Develop and agree on a shared vision, mission, goals, objectives, and outcomes for juvenile information sharing.

A shared vision is vital to the JIS 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 JIS collaborative.
- It drives the mission and goals.

A mission statement is a clear statement of the reason the JIS collaborative exists. Goals are general statements about what the JIS 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.

Guideline 18

Formulate a strategic plan to achieve juvenile information sharing.

The strategic plan provides a roadmap for collaborative action and includes operations, performance, and monitoring. The plan delineates purpose, resources, milestones, timelines, a set of measurable 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 JIS 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 can incorporate strategies for a continuous improvement process to generate ideas, make decisions, and execute plans.

Guideline 19

Identify and direct staff and funding resources that will be used for the JIS collaborative.

As the JIS 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 JIS collaborative needs to consider how JIS will be maintained, managed, and supported.

Guideline 20

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

Technical business requirements provide direction for the JIS 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 JIS is attempting to incorporate. It is important to solicit input from the identified users on how this system will function, what events will trigger information sharing, and what will trigger data protection.

Guideline 21

Include technology representation in all discussions regarding legal issues and privacy concerns, and include security and privacy concerns in all technical planning and development for juvenile information sharing.

As the JIS 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 JIS design; these determine an agency's accessibility to the needed information when it is appropriate.

Guideline 22

a. **Agree that the information to be disclosed by each JIS participating agency is based on legal authority and/or an informed consent to release information by the youth and/or the youth's parent or legal guardian.**

b. **Agree that JIS participating agencies will not, without good cause, refuse to disclose the information necessary to achieve the JIS purposes.**

"The general rule of law as to disclosure of youth-serving agency records is that they are closed to both public dissemination and interagency sharing unless statutory exceptions apply." (James, Bernard, 2005) Accordingly, an analysis of relevant laws identifies information that can be shared and what mechanisms are 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).

It is advisable that JIS 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 that the youth and/or parent or legal guardian refuse to consent to the release of the information. Consent is further discussed in Guidelines 26–28 on pages 17–19.

Guideline 23

Agree that JIS participating agencies will only access information as permitted by legal authority.

Whereas Guideline 22a deals with the disclosure of information, this guideline focuses on who may access this information. JIS participating agencies need to be fully informed on all sources of legal authority regarding confidentiality and information sharing of juvenile records, 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 provided as appropriate by a youth and/or his or her parent(s) or legal guardian.

Guideline 24

Agree that JIS participating agencies access and use only the information that is necessary to achieve JIS purpose(s) and to support defined activities.

Disclosure of, and access to, information that supports the JIS collaborative's purpose is further limited to information that is needed for the purposes of community safety, and youth and family wellbeing. In statutes and regulations, limiting agency access to the "minimum necessary" information to effectively conduct their activities is intended to control broad and unnecessary disclosure of private information.

Guideline 25

Prohibit re-disclosure of personal information accessed through juvenile information sharing unless required or allowed. 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. For example, both the Family Educational Rights and Privacy Act (FERPA) and the Child Abuse Prevention and Treatment Act (CAPT) specify practice regarding re-disclosure, including prohibiting re-disclosure of confidential information without the consent of the youth, parent or legal guardian; penalties for improper re-disclosure; and limited exceptions to the consent requirement.

FERPA limits re-disclosure of education record information and establishes a penalty for its improper re-disclosure (Melaris, Campbell, James, 1997). Specifically, if a third party is found to have improperly re-disclosed personally identifiable information from an education record, the educational agency or institution may not allow that third party access to personally identifiable information from education records for at least five years (Authority: 20 U.S.C 1232g(b)(4)(B); 34 CFR §99.33(a)). There are certain exceptions to FERPA's general rule regarding re-disclosure. These are when the prior consent of the "parent or eligible student" is not required under 34 CFR Part 99 Subpart D at §99.31 and the party complies with the reporting requirements found at §99.32(b).

Re-disclosure of child welfare records is limited under Title IV-B of the Social Security Act and CAPTA. Title IV-B allows the release of confidential information contained in child welfare records only to certain persons or agencies that require the information for specific purposes. Once the information is released to these authorized recipients, they become subject to the same confidentiality rules as the releasing agency. For example, if a child welfare agency releases information to the court, the court cannot re-disclose that information except as permitted under 45 CFR 205.50. (U.S. Department of Health and Human Services, 2005) Similar limitations are set for re-disclosure of confidential child protective services (CPS) information. Authorized recipients of CPS information are bound by the same confidentiality restrictions as the CPS agency. Recipients of such information must use the information only for activities related to the prevention and treatment of child abuse and neglect, and re-disclosure is permitted only in accordance with the CAPTA standards.

In cases where re-disclosure is not prohibited, the JIS Collaborative might agree as a matter of practice not to re-disclose the information to a third party without consent. Limiting disclosure to JIS participating agencies also addresses the public's concern of uncontrolled dissemination of personal information through automated information sharing systems.

Guideline 26

Agree on a common process for obtaining informed consent for information release that provides adequate verbal and written notice and is linguistically appropriate to the youth and parent(s) and/or legal guardian. The criteria might include:

- **Juvenile information sharing purpose(s).**
- **The reason(s) for disclosing the information.**
- **The way(s) that the disclosed information will be used.**
- **Any limitations on the disclosure and/or use of the information.**
- **Agency practices regarding sharing of non-confidential, as well as confidential information.**
- **The way(s) youth and/or the youth's parent/legal guardian can revoke their consent.**
- **Policies for youth and/or youth's parent/legal guardian to review their information.**
- **Grievance procedures for suspected unauthorized disclosure or use of the information.**
- **Penalties for unauthorized disclosure or use of the information.**

Most laws regarding confidentiality of agency records allow disclosure of personal information with written informed consent of either the youth, parent(s), or legal guardian, and in some cases, by court order. The JIS 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. By providing written, informed consent, families are encouraged and supported to become active participants in service planning and in making decisions for their children (Constantine, Aronson, Shannan, 1997).

"Informed consent" requires that the youth and/or parent(s), or legal guardian 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 JIS participating agencies. To ensure that the consent is "informed," JIS participating agencies need to be aware of any cultural or linguistic factors that may impact the youth and/or parent or legal guardian's ability to understand the consent process, including the need for interpretive services.

Guideline 27

Use an approved form to obtain the written consent of the youth and/or parents or legal guardian to release information that at a minimum includes the following elements:

- **Identifies the individual(s) who the information is about.**
- **Identifies the agency that is disclosing the information.**
- **Identifies the information that will be disclosed.**
- **Identifies the purpose of the disclosure.**
- **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 (e.g., when a youth is successfully terminated from probation or court supervision).**
- **Describes how a youth, parent, or legal guardian can revoke his or her consent.**
- **States the date of consent with the youth's parent(s) or legal guardian's signature.**
- **States that the subject of the information has a right to a copy of the release.**

A common consent form used by all JIS participating agencies reinforces the common informed consent process. The elements noted above are a common set found in relevant statutes and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), and 42 C.F.R. Part 2: Federal Alcohol/Drug Confidentiality Regulations. The consent form can also include language explaining that once an agency discloses information to another pursuant to the youth, parent(s) or legal guardian's written signed consent, the original agency is not responsible for any subsequent disclosures. However, JIS 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 need to be provided to the youth, parent(s), or legal guardian.

Guideline 28

Provide an option for youth and/or the youth's parent(s) or legal guardian to refuse consent when consent is required to release their private information to certain or all JIS participating agencies.

Despite assurance of privacy protection, the youth, parent(s), or legal guardian may not want specific personal information disclosed. In these cases when a

youth, parent(s), or legal guardian 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 JIS participating agencies' responsibility to ensure that the youth, parent(s), or legal guardian understand 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.

Guideline 29

Develop and agree on common privacy policies that address the disclosure, access, and use of information, and provide a threshold level of confidentiality that all JIS participating agencies agree to meet.

JIS participating agencies often bring different levels of information protection and policies to the JIS collaborative. Generally, well established child and family service agencies have fairly detailed confidentiality requirements. Community grass roots organizations may have less detailed requirements. Regardless of the JIS collaborative's composition, a minimum level of confidentiality needs to be set and agreed to by all JIS participating agencies.

Guideline 30

Determine common administrative, physical, and technical security safeguards to protect against any reasonably anticipated threats to the integrity of juvenile information and to ensure the confidentiality of private information.

After assessing the threats to privacy and security of private information, the JIS 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, firewalls, encryption, authentication passwords, unique user identification, and automatic logoff are all examples of technical security safeguards.

Guideline 31

Develop and make available privacy and information sharing policies to show the ability of JIS participating agencies to properly protect the privacy of the youth's and family's information.

Privacy and information sharing policies protect JIS participating agencies and facilitate information sharing. These policies strengthen public confidence in the JIS 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.

Guideline 32

Design procedures to ensure that information disclosed by JIS participating agencies is accurate and complete.

To achieve the JIS purpose(s), the information that is accessed and used must be accurate and complete. Reasonable policies and procedures are put into place and monitored to ensure information accuracy. These can address training, data validation, how information can be updated, changed, or destroyed, and quality assurance of data inputs and outputs.

Guideline 33

Develop accessible processes and procedures for youth, parents, and legal guardians 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 youth, parents, and legal guardians the right to see and have copies of their information. Additionally, providing opportunities for review and amendment can help ensure that information is accurate and current. JIS participating agencies should develop procedures for review and amending information, and notify youth, parents, and legal guardians of these procedures. Information regarding these procedures is typically provided through agency notices required by federal and state laws.

It is recommended that JIS 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 youth and families. A user-friendly approach should also be used for materials that inform youth and their families on how to assert their privacy rights.

Guideline 34

a. Provide youth, parent(s), and legal guardians with all JIS policies and procedures addressing confidentiality and privacy protection.

b. Provide youth, parent(s) and legal guardians with the procedures and opportunity to review and dispute these policies and procedures as well as the JIS participating agency decisions made pursuant to them.

While assessing needs and providing services, agencies often require youth and families to share intimate and private information about themselves. If disclosed, this information may be embarrassing to the youth and family and may discourage them from using the services designed to help them. Disclosure may also result in differential treatment and threaten job and personal security; such as, in disclosure about HIV/AIDS or domestic violence situations. Given the strong interest in protecting their privacy interests, youth and families need the opportunity to review and challenge policies and procedures that would result in the unnecessary disclosure of private information, (Constantine, Aronson, and Shannon, 1997) as well as any decision to share information made pursuant to them.

Guideline 35

Develop a JIS 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. Develop and maintain a process for identifying technology standards, records management practices and standards, privacy design principles, and security standards to ensure that the collaboration's information sharing practices are performed using agreed-upon industry and organizational standards.

Guideline 36

Develop a policy and procedural methodology for the incorporation of new agencies into juvenile information sharing.

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

Guideline 37

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

JIS participating agencies are accountable for the implementation of and compliance with JIS 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 JIS privacy, security, and technology.

Guideline 38

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

As the development and implementation of juvenile 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 JIS collaborative.

JIS participating agencies should use a Memorandum of Understanding (MOU) to verify the agreed upon arrangements of policies, procedures, practice, agency responsibilities, and resources for sharing information The MOU documents the agencies' agreement on such criteria as:

- JIS purpose(s).
- Governance.
- JIS 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 JIS participating agencies.
- Communications support and resources.
- Conflict resolution process.

Chapter 3. Implement JIS

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

Guideline 39

Implement JIS policies, procedures, and practices.

JIS participating agencies should implement the JIS 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, and the JIS collaborative as a whole. JIS participating agencies monitor implementation and compliance within their own agencies. JIS project management and the JIS collaborative monitor compliance across the JIS participating agencies, and address compliance issues and requests for modifications.

Guideline 40

Agree that JIS participating agency managers and staff participate in thorough and ongoing instructional training on JIS polices, procedures, and practices.

Successful JIS occurs when users are trained in all aspects of the system including purpose, benefits, expected outcomes, policies, and procedures. Training 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. Training typically includes a combination of online or CD-ROM instruction, classroom tuition, and one-on-one assistance.

Because JIS requires changes in privacy policies and procedures, it is critical to provide frequent and thorough user instruction to ensure that agency personnel including employees, contractors, volunteers, and anyone with access to youths' information adhere to the privacy policies and practices, including the common informed consent process.

Guideline 41

Determine a set of measurable outcomes for youth, their families, and their communities. Youth and families assist in determining these outcomes.

A primary purpose for juvenile information sharing is to improve outcomes for youth, families, and communities. Enlisting their involvement in determining these outcomes should inform the development of performance measures and benchmarks.

Guideline 42

Determine performance measures and benchmarks to achieve juvenile information sharing and agree that JIS 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 JIS. A Memorandum of Understanding, for example, indicates readiness to begin JIS implementation.

Guideline 43

Conduct periodic assessments of JIS 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 JIS environment and support JIS users. The JIS collaborative and project management are responsible for ensuring alignment of JIS 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 JIS technology framework to ensure that they are supported by appropriate information exchange and security methods.

Guideline 44

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

An audit trail is important to track appropriate access to JIS information and provides the JIS governance structure with information needed to monitor confidentiality and security. An audit trail records activities such as event type, date and time of event, user identification, success or failure of access attempts, and security actions taken by system administrators or security officers.

Chapter 4. Promote Public Awareness

This chapter recommends a policy of transparency, openness, and public communication regarding juvenile information sharing. Juvenile information sharing affects youth, families, and communities with regard to health, wellbeing, safety, and privacy. Educating the public and policymakers about JIS processes, policies, procedures, and impacts is critical to engendering trust and support.

Guideline 45

Approve a general policy of openness about developments, practices, and policies with respect to the management of personal information and data.

The JIS collaborative agrees on a general policy of transparency and openness that enables the public to have access to JIS 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 JIS participating agencies properly protect the privacy of youth and families.

Guideline 46

Agree that JIS 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 juvenile information sharing afford the public the opportunity to learn about JIS purposes, development, design, and outcomes. Openness can also garner public engagement and support, and is important to addressing public concerns about how juvenile information sharing complies with legal authority for information exchange and protects private information.

Guideline 47

Establish a JIS collaborative communications plan and media strategy.

A JIS communications plan determines all aspects of how information about JIS is conveyed to various audiences, including JIS collaborative agencies, other interested parties, the media, and the public. This plan covers both internal and external JIS collaborative communications and the means by which they are delivered. The JIS 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 48

Educate the public, including lawmakers and policymakers, about the purpose of juvenile information sharing, how private information is protected, and how information sharing facilitates improved wellbeing of youth and family, safety of the public and victims, and interagency collaboration.

JIS participating agencies should reach agreement on messages that are used to promote juvenile information sharing; such as on improved efficiency and outcomes. Public education communicates the JIS purpose and outcomes, and how information is gathered to achieve the goals of improved outcomes and increased community safety. Public education also covers limits on disclosure and use of information to authorized users only on a "need to know" basis.

Other reasons for juvenile information sharing, such as those identified by the California Interagency Data Collaboration Standards for Managing Confidential Data (Constantine, Aronson, and Shannan, 1997) include:

- Conduct comprehensive assessments.
- Provide all necessary services.
- Coordinate services and avoid duplication.
- Facilitate monitoring of service plans.
- Make services more family-focused.
- Serve the needs of the broader community.

Further, it is important to reach agreement on how these messages and other relevant information are disseminated. For instance, the JIS collaborative can develop an informational, public-based 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 JIS collaborative, the juvenile information sharing history, funding sources, information sharing in general, and information on and links to each JIS participating agency.

Bibliography

This bibliography is organized according to three subject areas: Collaboration, Confidentiality and Privacy Protection, and Technology.

Collaboration

Bernard, B. 1989. *Working Together: Principles of Effective Collaboration*. Oakland, CA: Prevention Forum.

Bureau of Justice Assistance. 2002. Mission Possible—Strong Governance Structures for the Integration of Justice Information Systems. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Burt, M.R., Novick, E.R., and Resnick, G., 1998. *Building Supportive Communities for At-risk Adolescents: It takes more than services.* Washington, DC: American Psychological Association.

Center for Network Development. 2000. Articulating the Vision. Juvenile Information Sharing curriculum. Denver, CO: Center for Network Development.

Center for Network Development. 2004. A Report on Key Principles, Promising Practices and Standards for Juvenile Integrated Information Sharing. Denver, CO: Center for Network Development.

Center for Substance Abuse Treatment. 2000. Changing The Conversation: Improving Substance Treatment. Rockville, MD: U.S. Department of Health and Human Services, Center for Substance Abuse Treatment, Substance Abuse and Mental Health Services Administration.

Ciancutti, A., and Steding, T.. 2001. *Built On Trust: Gaining Competitive Advantage in Any Organization.* Chicago, IL: NTC Contemporary Publishing Group, Inc.

Etten, T.J., and Petrone, R.F.,1994. Sharing Data and Information in Juvenile Justice: Legal, Ethical, and Practical Considerations. Reno, NV: *Juvenile and Family Court Journal* 45, 65–89, 1994.

Griffin, P. 2000. *Separate Tables: Interagency Information Sharing in Real Life.* Pittsburgh, PA: Center for Juvenile Justice.

Kotter, J. P. 2002. *The Heart of Change.* Boston, MA: Harvard Business School Press.

Mattessich, P., Murray-Close, M., and Monsey, B.. 1992, 2001. *Collaboration, What Makes It Work.* St. Paul, MN: Amherst H. Wilder Foundation.

Rauch, J.B., et al. 1993. Diversity Competence: A Learning Guide. Baltimore, MD: School of Social Work, University of Maryland at Baltimore.

Stein, S. 1992. Fifth Annual Conference on Restitution. Denver, CO: OMNI Research and Training, Inc.

Swan, W.W., and Morgan, J.L., Collaborating For Comprehensive Services For Young Children And Their Families. Baltimore, MD: The Local Interagency Coordinating Council. Paul H. Brookes Publishing.

Treasury Board of Canada Secretariat. 2002. Privacy Impact Assessment Policy, Preface. Ontario, Canada. Retrieved on web August 24 at http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp#Preface.

Confidentiality and Privacy Protection

Bernard J. 2004. State Statutes on Juvenile Interagency Information and Record Sharing. Washington, DC: Retrieved on Web August 2, 2006 from http://dept.fvtc.edu/ojjdp/states.htm.

Cavoukian, A., Beamish, B., and Gurski, M., et al. 2000. Policy and Technology Officer Privacy Design Principles for an Integrated Justice System, Working Paper. Washington, DC: U.S. Department of Justice, Office of Justice Programs. Retrieved on Web August 2, 2006 at http://www.ojp.usdoj.gov/archive/topics/integratedjustice/pdpapril.htm.

Center for Mental Health in Schools at UCLA. 2004. An Introductory Packet On Confidentiality And Informed Consent. Los Angeles, CA: Center for Mental Health in Schools at University of California, Los Angeles. Retrieved on Web August 2, 2006 at http://smhp.psych.ucla.edu/pdfdocs/confid.pdf.

Center for Network Development. 2001. Confidentiality Module, Juvenile Integrated Information Sharing Curriculum. Denver, CO: Center for Network Development.

Cheung, O., Clements, B., and Pechman, E. 1997. Protecting The Privacy Of Student Records: Guidelines For Education Agencies. Washington, DC: Institute for Education Sciences (IES), National Center for Education Statistics, U.S. Department of Education. Retrieved August 2, 2006 at IES Web site, http://nces.ed.gov/pubs97/p97527/.

Constantine, N., Aronson, J., Wilbur, S. 1997. Development of Uniform Standards for Interagency Data Sharing, Case Management Information Systems, and Data Confidentiality: The California Interagency Data Collaboration, July 29, 1997, Washington, DC. Retrieved on Web August 2, 2006 at crahd.phi.org/papers/nchs.pdf.

Fleming, R. and Lubin, S. 1998. Critical Issue: Addressing Confidentiality Concerns in School-Linked Service Efforts. Chicago, IL: Center for School and Community Development, North Central Regional Educational Laboratory (NCREL). Retrieved August 2, 2006 at NCREL Web site: http://www.ncrel.org/sdrs/areas/issues/envrnmnt/css/cs300.htm.

Global Justice Information Sharing Initiative. Privacy and Information Quality Policy Development for the Justice Decision Maker. Washington, DC: U.S. Department of Justice, Office of Justice Programs.

Greenberg, M., and Levy, J. 1992. Confidentiality and Collaboration: Information Sharing In Interagency Efforts, Denver, CO: Education Commission of the States Distribution Center.

Harris, K. J. 2000. Governance Structures, Roles and Responsibilities, a Background Report, Integrated Justice Information Systems. Sacramento, CA: SEARCH, The National Consortium for Justice Information & Statistics.

Hodges, S., Nesman, T., and Hernandez, M. 1998. Systems of Care: Promising Practices in Children's Mental Health, Center for Effective Collaboration and Practice. Washington, DC: American Institutes for Research, Washington, DC.

Mankey, J., Baca, P. and Rondenell, S. 2002. Summary Report on the National Juvenile Integrated Information Sharing Focus Group, Denver, CO: Center for Network Development. Retrieved on Web August 2, 2006 at www.juvenileiis.org/pdf/JIISFocusGroup.pdf.

Medaris, M., Campbell, E., and James, B. 1997. Sharing Information: A Guide to the Family Educational Rights and Privacy Act and Participation in Juvenile Justice Programs—An OJJDP Program Report. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention. Retrieved August 3, 2006 on Web: http://www.ncjrs.org/pdffiles/163705.pdf.

National Association of Social Workers. Confidentiality and School Social Work: A Practice Perspective. Washington, DC: National Association of Social Workers (NASW). Retrieved August 2, 2006 at NASW Web site: http://www.socialworkers.org/practice/school/cfs0202.asp.

National Association of State Chief Information Officers. 2004. Information Privacy: A Spotlight on Key Issues. Lexington, KY: National Association of State Chief Information Officers.

National Center for Education Statistics. 1997. Protecting the Privacy of Student Records. Washington, DC: U.S. Department of Education, Institution for Education Sciences, National Center for Education Statistics.

National Criminal Justice Association. 2002. Developing, Drafting and Assessing Privacy Policy for Justice Information Systems. Washington, DC: National Criminal Justice Association.

Office of Justice Programs. 2000. Privacy Impact Assessment for Justice Information Systems. Working Paper. Retrieved August 3 on Office of Justice Programs Web site: http://www.ojp.usdoj.gov/archive/topics/integratedjustice/piaJIS.htm.

Office of Justice Programs. Justice Standards Registry for Information Sharing. Washington, DC: U.S. Department of Justice, Office of Justice Programs. Retrieved August 3, 2006 at OJP Web site: http://it.ojp.gov/jsr/public/.

Slayton, J. 2000. *Establishing and Maintaining Interagency Information Sharing*, Juvenile Accountability Incentive Block Grants Bulletin. Washington, DC: U.S. Department of Justice. Office of Justice Programs. Office of Juvenile Justice and Delinquency Prevention. Retrieved August 3, 2006 on Web at http://www.ncjrs.org/html/ojjdp/jiabg_blltn_03_1_00/13.html.

Soler, M. and Peter, C. 1993. Confidentiality and Information Sharing in Service Integration. Washington, DC: Administration for Children & Families, U.S. Department. of Health & Human Services. Retrieved August 2, 2006 from Early Head Start Web site at: http://www.ehsnrc.org/InformationResources/ResourceArticles/ftconf.htm.

West Laboratory for Educational Research and Development. 1994. Standards for Data Exchange and Case Management Information Systems In Support Of Comprehensive Integrated School-Linked Services (Version 2.0). San Francisco, CA: Youth Law Center.

Technology

Harris, K. 2000. Integrated Justice Information Systems Governance Structures, Roles and Responsibilities, Sacramento, CA: SEARCH, The National Consortium for Justice Information and Statistics. Retrieved August 3, 2006 from Web at: http://www.search.org/files/pdf/GovernanceStructures.pdf.

International Association of Chiefs of Police. 2000. Toward Improved Criminal Justice Information Sharing. Alexandria, VA: International Association of Chiefs of Police. Retrieved August 3, 2006 from Web at: http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_id=133.

National Governor's Association Addresses IT Governance Structures Within a Number of Information Sharing Publications. Washington, DC: National Governor's Association; Retrieved August 4, 2006 from NGA Web site at: http://www.nga.org/center/topics/1,1188,D_2462,00.html.

Office of Justice Programs. Information Technology Initiatives. Washington DC: U.S. Department of Justice, Office of Justice Programs. Retrieved August 3, 2006 from OJP Web site at: http://it.ojp.gov/.

Glossary

Authorization to disclose information—Permission granted by federal, state, or local legal authority; written consent to release information by the youth and/or parent or legal guardian; or court order to reveal, release, transfer, disseminate or otherwise communicate all or any part of any individual record (see "legal authority," page 33).

Access—The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Administrative safeguards—Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic information, and to manage the conduct of the agencies' workforce in relation to the protection of the information.

Agencies—Public entities funded by municipal, state, and/or federal governments or private nonprofit organizations.

Assessments—Methods that identify common factors and characteristics influencing the JIS collaborative process of gathering and interpreting information about program effectiveness.

Automatic disclosure—Authorized release of an individual's record; does not require written permission.

Audit (security)—Examines how secure a site is through systematic, measurable technical assessment of how an organization's security policy is employed at a specific site.

Benchmark—The standard by which something can be measured or judged.

Broad community representation—Representation inclusive of youth, families and their communities.

Client consent—Gives written permission to an agency or individual to release personal protected information to another agency or individual; can also be a requirement for release of personal protected information. Consent is given in writing, usually on a form provided by the agency requesting the information that complies with law and agency regulations for client consent. To release private information related to children and youth under the age of 18 years, consent by a parent or legal guardian is typically required. Exceptions include state laws related to medical, mental health, and substance abuse that might allow youth to consent prior to the age of 18 without parent or legal guardian consent (see "informed consent," page 33).

Computer security—The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (including hardware, software, firmware, information data, and telecommunications).

Confidentiality—The legal duty of someone who has received personal information in trust to protect that information and disclose it to others only in accordance with applicable legal authority. Confidentiality practices safeguard information from unauthorized disclosure to third parties.

Confidentiality laws—Federal, state, or local legal authority laws that direct practice for the collection, disclosure, access, and use of private information.

Continuous quality improvement—Knowledge-driven feedback to plan and achieve quality.

Core services—Basic services provided by agencies for youth and families to improve their outcomes for success.

Court order to disclose/access information—Under court jurisdiction, federal and state law can allow judges to issue a court order authorizing disclosure of certain information about youth and family to specified agencies and others. The court can also issue a subpoena along with the individual's consent to obtain all or any records.

Disclosure—Includes permitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, or by electronic or any other means to any person or entity.

Due process—The entitlement of a citizen to proper legal procedures and natural justice.

Duty to report—Many states require specified professionals to report to appropriate agencies and authorities whenever there is actual or suspected child abuse (physical, sexual, neglect, emotional and psychological abuse, unlawful sexual intercourse).

Education record—The Family Educational Rights and Privacy Act (FERPA) defines an education record as a compilation of records, files, documents, and other materials that contain information directly related to a student and maintained by education agencies or institutions, or by an individual acting on behalf of the agencies. A record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film microfilm, and microfiche. Sometimes referred to as a student record, an education record may include a variety of details about a student such as the birth date, date of enrollment, bus route, immunization history, achievement test scores and grades, enrollment and attendance, awards, degrees achieved, and special education plans and evaluation.

Encryption—The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Enterprise architecture—A framework for understanding all of the different elements that make up the enterprise and how those elements interrelate.

Enterprise—Any collection of organizations that has a common set of goals/principles and/or single bottom line. In that sense, an enterprise can be a whole corporation, a division of a corporation, a government organization, a single department, or a network of geographically distant organizations linked together by common objectives.

Elements—In this context, elements are all the components of the categories of people, processes, business, and technology. In that sense, examples of elements are: strategies, business drivers, principles, stakeholders, units, locations, budgets, domains, functions, processes, services, information, communications, applications, systems, infrastructure, etc.

Fair information practice principles—Widely accepted principles concerning fair information practices for collection and use of personal information. Developed for the private sector, but have been adopted for application in criminal justice information sharing as well. The principles are (1) notice/awareness (2) choice/consent (3) access/participation (4) integrity/security; and (5) enforcement/redress.

Family Educational Rights and Privacy Act (FERPA)—Family Educational Rights and Privacy Act (See "education record," above).

Global Justice Information Sharing Initiative—A group of justice professionals who work collaboratively to address the policy, connectivity, and jurisdictional issues that have hampered effective justice information sharing. The Global Justice Information Sharing Initiative Advisory Committee is an advisory body to the Assistant U.S. Attorney General, Office of Justice Programs, and the U.S. Attorney General, created to advise on issues related to broad scale exchange of justice information.

Good cause—Sufficient legal standard or reason.

Governance structure—The vehicle through which agencies, stakeholders, and users participating in juvenile information sharing strategically plan for integrated systems implementation. Governance structure is composed of a governing body, whether by executive order, statute, informal organization or a Memorandum of Understanding that establishes a mission, membership, and decisionmaking structure for the JIS collaborative to implement successful juvenile information sharing.

Health Insurance Portability and Accountability Act (HIPAA)—Provides national standards for electronic health care transactions. Entities that are covered by HIPAA are health plans, health care clearinghouses, and health care providers who electronically transmit protected health care information. HIPAA requires these covered entities to implement standards to protect and guard against misuse of individually identifiable health information.

Infrastructure—An underlying base or foundation for an organization or system; the basic foundation needed for a system to function.

Information privacy—The interest an individual has in controlling, or at least significantly influencing, the handling of data about him- or herself. Privacy in this context means "information privacy," an individual's claim to control the terms

under which personal information—information identifiable to an individual—is acquired, disclosed, and used.

Informed consent—Consent must be given by an individual voluntarily, based on his or her understanding of risk, benefits, and alternatives. The individual's ability to give informed consent depends on: adequate presentation of information in language that is understood by the individual, the individual's comprehension of presented information, freedom of choice, and his or her capacity for decisionmaking (see "client consent," page 31).

Integrity—The quality of information that has not been altered or destroyed in an unauthorized manner.

Interoperability—The ability of different information technology systems and software applications to communicate and exchange data accurately and effectively.

Justice Information Exchange Model (JIEM)—Provides a conceptual framework, methodology, and software tool to collect requirements from users for electronic information sharing, documenting both the business context and information content of information exchange as it currently exists.

Juvenile Information Sharing (JIS)—The sharing of essential information between multiple agencies and across systems using structured processes and procedures to improve outcomes for youth and families.

JIS collaborative—Youth, family, community, and agency representatives who work together to improve outcomes for youth, families, and communities.

JIS participating agencies—Those agencies that participate in, share, and receive information through juvenile information sharing.

JIS planning agreement—A means to formalize linkages and responsibilities between JIS participating agencies. The planning agreement outlines the purpose and actions necessary to develop a JIS plan.

Key stakeholders—Agencies or individuals who have a stake in the implementation of an effective JIS collaborative. Examples are youth, parents or legal guardian, child welfare, law enforcement, courts, probation, education, mental health, government, substance abuse and prevention, other youth-serving agencies, and communities.

Legal analysis—Identifies and analyzes the relationships and primacy of the relevant federal, state, and local legal authority that guides the collection, disclosure, access, and use of personal information contained in agency records.

Legal authority—Provides for the ability to disclose, access, or use information pursuant to federal, state, or local statutes, regulations, rules, case law, and court orders.

Legal guardian—An adult (not the biological parent of the child), or a licensed child caring agency, to whom a court has granted legal care and custody of a child.

Memorandum of Understanding—A written document that delineates an understanding of agreed-upon actions and responsibilities among multiple parties.

Minimum necessary—Refers to access to the minimum amount of information necessary to achieve the purpose of juvenile information sharing and the JIS participating agencies.

Mission statement—A formal statement of objectives that provides a blueprint for a group's actions and goals.

Need to know—A requirement for disclosure and receipt of private information. The information needs to be directly related to the legitimate stated purpose of the disclosure and the agency need for the information in order to perform its duties and responsibilities.

Office of Juvenile Justice and Delinquency Prevention (OJJDP)—A component of the Office of Justice Programs, U.S. Department of Justice, that provides national leadership, coordination, and resources to prevent and respond to juvenile delinquency and victimization. OJJDP supports states and communities in their efforts to develop and implement effective and coordinated prevention and intervention programs and to improve the juvenile justice system so that it protects public safety, holds offenders accountable, and provides treatment and rehabilitative services tailored to the needs of juveniles and their families.

Physical safeguards—Physical measures, policies, and procedures in place to protect the privacy of personal information, agencies' electronic information systems, and related building and equipment. from natural and environmental hazards and unauthorized intrusion.

Privacy—The interrelated values, rights, and interests that are unique to individuals, and to which the individual has a right to control or limit the access of others. Privacy interests include privacy of the person, privacy of personal behavior, privacy of personal communication, and privacy of personal data (information privacy).

Privacy impact assessment—An assessment of any actual or potential effects that an activity or proposal may have on individual privacy, and the ways in which any adverse effects may be mitigated.

Privacy protection—Protection of private information from unauthorized collection, use, and disclosure provided by security measures in information systems and agency practices and policies.

Private/personal information—Information of a personal nature about youth and families. Typically, it is protected against disclosure.

Project management—Dedicated and expert management by an individual or team who can guide the process from planning through implementation, and foster shared ownership, responsibility, and commitment among the JIS participating agencies.

Public record—The public records of some states are in the public domain; that is, juvenile records (e.g., concerning felony offenses or sex offenders) are open to everyone.

Re-disclosure—When an agency that has received personal information discloses that information to other agencies that are bound by similar confidentiality requirements. Occurs only when the client has consented to the re-disclosure of the information, or if the agency seeking the re-disclosure of the information would originally have been able to access the protected information.

Regulation—A rule issued by a public agency or administrative body that directs practice.

Statewide Automated Child Welfare Information System (SACWIS)—The Omnibus Reconciliation Act of 1993 provided states with federal financial support for the development of statewide systems that automate the collection of federally mandated child welfare data and provide support for the delivery and management of child welfare services.

Security—Encompasses all administrative, physical, and technical safeguards in an information system.

Sex offender registries—A state central registry of sex offenders, who are required to register under state law. These registries make information about offenders available to the public.

Strategic plan—A plan of action that is essential to attain a successful information sharing system which is congruent with the collaborative's mission, vision, goals, and objectives and identifies actions to reach a shared vision. The plan must address implementation and management activities.

Sustainability—The ability to keep in existence or maintain.

Systems—Normally includes hardware, software, information, data, applications, communication, and people.

Team culture—Team-related strengths, weaknesses, concerns, and expectations that encompass behavioral patterns and invisible beliefs of the group's members.

Technical safeguards—Policy and procedures regarding the use of technology that protect electronic information and control access to it.

Third party disclosure—Disclosure that occurs when an individual has received information from an agency and then provides that information to another.

User—A person or entity with authorized access to a system.

Workstation—An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, with electronic media stored in its immediate environment.