

# Guidelines for Juvenile Information Sharing

## -Tool Kit-

### *Privacy and Security Impact Assessment*

---



## Information Sharing to Prevent Juvenile Delinquency Project



The project is supported by Grant No. 2006-JF-FX-0077 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions expressed in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Guidelines for Juvenile Information Sharing  
-Tool Kit-  
*Privacy and Security Impact Assessment  
Template*



Prepared by Jennifer Mankey  
Center for Network Development  
Denver, Colorado  
January 2008

# Table of Contents

Introduction .....	5
How to Use the Template .....	7
Completing Part 1 .....	7
Completing Part 2 .....	7
Part 1 .....	9
Individual JIS Participating Agency Assessment .....	9
1. Purpose.....	9
2. Collection limitation .....	10
3. Data quality .....	11
4. Use limitation.....	12
5. Security safeguards .....	13
6. Openness and transparency.....	14
7. Individual participation.....	15
8. Accountability.....	15
Assessing the JIS Participating Agency Answers.....	16
Part 2 .....	17
Integrated System Privacy and Security Assessment .....	17
1. Purpose.....	17
2. Collection .....	18
3. Data quality .....	19
4. Use limitation.....	20
5. Security .....	21
6. Openness and transparency.....	22
7. Individual participation .....	23

8. Accountability.....	24
9. Additional Considerations - Disclosure.....	25
10. Additional Considerations – Personal Information.....	26
11. Additional Considerations - Protection of Privacy .....	27
12. Additional Considerations - Computer Matching.....	27
Assessing the Integrated System Answers.....	28
Links to Juvenile Justice and other Youth Service Agency Flow Charts .....	29
Juvenile Justice Flow Charts.....	29
Mental Health.....	29
Victim/Offender Remediation .....	29
Child Welfare Flow Chart.....	29

## Introduction

The **Guidelines for Juvenile Information Sharing** provide a course of action for States and local jurisdictions involved in efforts to improve information sharing among the key agencies that work with at-risk youth and juvenile offenders. In addition to publishing the Guidelines, [Guidelines for Juvenile Information Sharing: An OJJDP Report](#), the Office of Juvenile Justice and Delinquency Prevention (OJJDP) is supporting development of a toolkit to assist juvenile justice and other youth serving agencies implement the Guidelines.

This template was designed to guide juvenile justice and other youth serving agencies in conducting a Privacy and Security Impact Assessment for Juvenile Information Sharing (JIS) as recommended in Guideline #15, “Assess the impact on privacy and security when deciding what information may be shared through juvenile information sharing.” A Privacy and Security Impact Assessment is invaluable for both **assessing potential risks to privacy** that can occur with information exchange, and **identifying solutions and policies** that minimize those risks.

A model Privacy Impact Assessment for criminal justice information sharing systems was developed by a task force of expert federal department and criminal justice professionals convened by the National Criminal Justice Association (NCJA), and supported by the Bureau of Justice Assistance, U.S. Department of Justice.<sup>1</sup> This template presents guiding questions for completing a PIA that were formulated by that group, and adds other relevant questions and considerations that are adopted from Roger Clarke’s discussions of privacy impact assessments.<sup>2</sup> Materials from both sources are included with their permissions.

The *Justice Information Privacy Guidelines* identifies three components to a Privacy and Security Impact Assessment (PIA) including a map of the flow of information within and between agencies; a privacy analysis of the information flow; and an analysis of privacy issues. As this

---

<sup>1</sup> *Justice Information Privacy Guideline*, Privacy Impact Assessment, Chapter 7, National Criminal Justice Association, <http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/default.htm> 2002. The predominant PIA methodology, instructions, and guiding questions are from the *Justice Information Privacy Guideline - Privacy Impact Assessment*. As appropriate, language has been altered for application to youth-serving agencies. Otherwise, descriptions, instructions and questions are as found in the referenced documents. Task force members represented the National Criminal Justice Association, the United States Department of Justice, Office of Justice Programs (OJP), and the Office of the Ontario Information Privacy Commissioner.

<sup>2</sup> Clarke R. (1998) 'Privacy Impact Assessments' Xamax Consultancy Pty Ltd, Canberra, February 1998, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html> Links to PIA Handbooks and privacy discussions are also available through this website.

PIA template focuses agencies' efforts on the second and third areas, [Links to examples of Juvenile Justice and other Youth Service Agency Flow Charts](#) are listed at the end of this document.

The following are the definitions of the PIA components as described by the *Juvenile Information Privacy Guidelines*.

1. "A map of the information flows associated with the participating agency's and the integrated system's business activity to determine information decision points and privacy vulnerabilities;
2. A privacy analysis of the information flow that examines whether agreed-upon privacy policies are firmly adhered to, whether there is technical compliance with a jurisdiction's statutory or regulatory privacy requirements, and whether these policies and laws are affording the desired privacy protection;
3. An analysis of privacy issues raised by the system review, including a risk assessment and a discussion of the options available for mitigating any identified risks." <sup>1</sup>

## How to Use the Template

The template is in two sections to correspond with the two part process for completing a PIA. The [first](#) section guides individual juvenile justice and other youth serving agencies through an assessment of their information privacy methods and protections. The [second](#) section guides the collaborative of agencies involved in developing JIS, through an assessment of the potential impacts of the proposed JIS on privacy, and evaluation of the security methods.

### **Completing Part 1**

Each agency administrator assigns responsibility for conducting the PIA to the individual(s) with knowledge and familiarity of their agency's privacy protection methods, policies and procedures.

The questions in this section guide each JIS participating agency in an assessment of the information privacy and security measures that are in place in their agency. The instructions and guiding questions from the *Justice Information Privacy Guidelines* allow each JIS participating agency to document a "yes" or "no" response, and directs agencies to provide further description when necessary.

### **Completing Part 2**

The JIS project management coordinates responses, taking into consideration the results of each participating agency's PIA. The JIS Collaborative assigns individual(s) to assist project management with Part 2, and each participating agency commits the expertise of the individuals who were responsible for their agency's assessment in Part 1.

The instructions and guiding questions are again from the *Justice Information Privacy Guidelines*, with additional questions and considerations by Roger Clarke. "Yes" or "no" responses are documented, and the assigned individuals or group completing the PIA are directed to provide further description when necessary.

A **written summary report** of the assessment results is used to guide JIS development and to assure agencies, policy makers, the public, youth and parents or legal guardians of JIS information privacy and security protections. *Elements of a Privacy Impact Report*, Chapter 9, <http://www.privacy.org.nz/privacy-impact-assessment-handbook/?highlight=PIA> provides a good description and outline of a PIA report. In addition, to gain a fuller understanding of the PIA process, please refer to Chapter 7 in the *Justice Information Privacy Guidelines*.

To learn how to link the PIA to policies, a discussion on the application of the PIA results for privacy policies development is provided in *Justice Information Privacy Guideline*, page 93, and the *Privacy Policy Development Guide* section 7

[http://it.ojp.gov/documents/Privacy\\_Guide\\_Final.pdf](http://it.ojp.gov/documents/Privacy_Guide_Final.pdf) .

Copies of the template may be distributed to members of a JIS Collaborative for the purposes of developing or assessing Juvenile Information Sharing. Other copying or uses may be done with permission of the Center for Network Development.

The Center for Network Development (CND) provides support, training, and technical assistance to agencies, collaboratives, and project managers on JIS. To share your comments or for more information, please direct your feedback or questions to: Jennifer Mankey, Center for Network Development 303-893-6898 [jennifer.mankey@thecnd.org](mailto:jennifer.mankey@thecnd.org).

## Part 1

### Individual JIS Participating Agency Assessment

<b>1. Purpose</b>	<b>Yes</b>	<b>No</b>
a. Is there a written purpose statement for the JIS? Set out the purpose statement(s).		
b. Is the written statement(s) publicly available prior to the time of information collection?		
c. If available publicly, is the written statement(s) set out in the organization's information collection form(s) in a comprehensive and prominent manner?		
d. Is the written purpose statement periodically reviewed and updated?		
e. Has a clear relationship been established between the personal information being collected, and the system's functional purpose and operational requirements?		
f. Is the personal information collected pertinent to the stated purposes for which the information is intended for use?		
g. Are there limits on subsequent (secondary) use of the information?		
h. Are there limits on third party and/or private sector partnerships or relationships where personal information is or will be disclosed?		
i. If not, do these secondary use(s) conform to the stated purpose?		
j. Are there mechanisms in place to inform youth, parent, guardian (data subjects) of third party, secondary use disclosure?		

<b>2. Collection limitation</b>	<b>Yes</b>	<b>No</b>
a. Is the collection of personal information limited to the agency/system's stated purpose?		
b. Is personal information obtained by lawful and fair means? Document the relevant law(s) that provides authority to collect information.		
c. Where appropriate, is personal information obtained with the knowledge or written consent of the youth, parent or guardian (data subject)?		
d. Is relevance considered when collecting personal information on individuals without their knowledge or consent, or when the individual is not charged with a crime (i.e. under investigation, or when an investigative body is "information gathering")?		

<b>3. Data quality</b>	<b>Yes</b>	<b>No</b>
a. Is the personal information collected for stated purposes accurate, complete, current, and verified?		
b. Does the agency/system collect “original” or “new” information?		
c. Is the personal information collected directly from the youth, parent, or guardian (data subject)?		
d. Is there a procedure for tracking requests to modify information, determining the requests to modify, modifications made based on the requests, the source of the information that is used to modify the information, and when the last modification occurred?		
e. Is there a procedure to provide notice of correction (modification) to subsequent system users and third parties (secondary users)?		
f. Where appropriate, does the youth, parent or guardian (data subject) have some means of accessing the information to ensure it is accurate and up to date?		
g. Where personal access by the youth, parent or guardian (data subject) is not appropriate, are there other methods to ensure that the information held is accurate and up to date?		
h. When a data subject challenges the accuracy of a record, is he/she provided with information about the agency personnel responsible for the record and administrative procedures governing inquiries?		
i. Are there procedures for addressing data management issues and record retention issues?		

<b>4. Use limitation</b>	<b>Yes</b>	<b>No</b>
a. Is the use of the information relevant to the purpose for agency/system operations?		
b. Does the system limit the use or disclosure of personal information to the stated purpose(s)?		
c. Are any secondary uses limited to those with the written consent of the youth, parent, or guardian (data subject), by the authority of law, for the safety of the community (including victims and witnesses), or pursuant to a public access policy?		
d. If personal identifiers are used for purposes of linking across multiple databases, do these multiple databases have consistent purposes?		
e. Are there procedures to ensure a “record of use” is maintained? Is it attached to each piece of personal information?		
f. Does the system prevent the derivation of new information or creation of previously unavailable information about an individual through aggregation from the information collected? Is an agency or the system itself prevented from making determinations about individuals that would not be possible without this new information?		
g. Are procedures in place to verify the new information for relevancy and accuracy?		
h. Is it prohibited to sell or release personal information under public access policy to private information gatherers (resellers)? If not, is the released information “publicly accessible” pursuant to your public access policy? If sold to private information gatherers (resellers), are there any contractual agreements between you that would prevent the unintended use, or misuse, of the personal information provided by the system?		
i. Does the agency/system have mechanisms to inform data subjects of third party (public), secondary use disclosure?		

<b>5. Security safeguards</b>	<b>Yes</b>	<b>No</b>
a. Does the system have security safeguards?		
b. Is there documentation of the system's security safeguards that protect personal information against loss, unauthorized access, destruction, use, modification, and disclosure?		
c. Are security safeguards provided according to sensitivity of the information and risks to all involved parties?		
d. Has there been an expert security review?		
e. Are JIS participating agencies' staff trained in requirements and ethics for protecting personal information?		
f. Is staff aware of policies and consequences regarding breeches of security?		
g. Are there controls in place over the processes that grant authorization to modify (add or delete) personal information?		
h. Does the system allow user access and changes to personal information to be audited by date and user identification?		
i. Are user accounts, access rights, and security authorizations controlled and recorded by systems or records management processes that provide accountability?		
j. Are access rights provided only to users who actually require access for the system's stated purposes?		
k. Are there contingency plans and mechanisms in place to identify security breaches and disclosures of personal information in error?		
l. Are there mechanisms in place to communicate violations or errors to subsequent users to mitigate collateral risks?		
m. Are adequate, ongoing resources budgeted in maintenance plans for security upgrades with measurable performance indicators?		
n. Are the system's security safeguards comprehensive enough to include all system back-up mechanisms?		

<b>6. Openness and transparency</b>	<b>Yes</b>	<b>No</b>
a. Does the system have a general policy of openness about developments, practices, and policies with respect to the <i>management</i> of personal information (apart from the actual information)?		
b. Does openness include public access to the management practices of the information?		
c. Does openness require clear communication to affected individuals where justice records are requested, sold, or released to third parties?		
d. Does openness require clear communication to affected individuals where justice records are requested, sold, or released under the system's public access policy?		

<b>7. Individual participation</b>	<b>Yes</b>	<b>No</b>
a. Does the system allow a youth, parent, or guardian to obtain confirmation of whether or not the data collector has information relating to him or her?		
b. Does the system allow a youth, parent, or guardian (data subject) to receive information relating to him or her within a reasonable time, at a charge, if any that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him/her?		
c. Does the system provide for an explanation if a request is denied? Is a youth, parent or guardian able to challenge a denial?		
d. Is the system designed to afford the above access rights with minimal disruption to day-to-day operations?		

<b>8. Accountability</b>	<b>Yes</b>	<b>No</b>
a. Is there an individual or agency body that is accountable for complying with measures that give effect to the privacy design principles, the public access policy, and applicable law or regulation?		

## ***Assessing the JIS Participating Agency Answers***

“Questions 1-8 above are phrased to help identify any vulnerability in possible areas of information privacy within an agency system. Where a question is answered in the negative (“No”), agency representatives should document the following items for each such answer:

1. What is the reason(s) that you answered “No”?
2. Regarding this question, is there a law, regulation, or articulated policy that excludes the system from compliance with a particular policy suggested by the privacy design principle?
3. Is there a logical exception related to the purpose of the agency system, e.g., law enforcement investigation or intelligence gathering?
4. What can be done to the agency system to make the answer to this question, “Yes”?
5. If you must retain the identified privacy risk, what plans or procedures are in place to mitigate possible effects of the identified risk?”

“Agency representatives should keep in mind that although there may be a legal, regulatory, or traditional policy exception for their information system, implementation of additional privacy protections may be appropriate. This is especially relevant given the public’s interest in and growing concern about information privacy. The documentation as to why the system has not answered affirmatively (“Yes”) to any one of the questions in the PIA should be retained and become a formal part of the impact assessment.”

“Additionally, [each JIS participating agency] in cooperation with the project management, should weigh its responses to the questionnaire against the agreed-upon “privacy baseline” of the [JIS participating agencies and collaborative]. Where the agency’s system falls short of meeting the privacy objectives, these areas should be brought to the attention of the [JIS] project management and governance and receive additional consideration.” *Justice Information Privacy Guidelines*

## Part 2 Integrated System Privacy and Security Assessment

1. Purpose	Yes	No
a. Are the purpose statements of the JIS participating agencies' systems compatible?		
b. Have all of the JIS participating agencies agreed to a common purpose for which information will be shared through the JIS application?		
<b>Purpose- Additional Considerations <sup>2</sup></b>		
c. Are there any additional purposes for which the information to be included in the proposed [JIS] application could be used? Are these additional uses absolutely necessary?		
d. If yes, should the additional purposes be defined as a primary, rather than as consistent purposes, and the youth/parent or guardian (data subjects) notified of its existence at the outset?		
e. Will the JIS be maintained for the purpose of creating a record that is available to the general public? What is the authority for creating a public record? Even if the records are public in nature, is the information managed in accordance with <i>fair information practices</i> because of potential public privacy concerns related to that information?		

<b>2. Collection</b>	<b>Yes</b>	<b>No</b>
a. Are the collection policies of the JIS participating agencies' systems compatible?		
b. Has it been determined which agency bears responsibility for protecting the privacy rights of individuals affected by the collection of information when it is shared among JIS participating agencies?		
c. Has an agency been identified as responsible for data quality of the collected information?		
d. Is there a process in place to evaluate the possible cumulative effects on individual privacy due to sharing information collected by different JIS participating agencies' systems?		
<b>Collection - Additional Considerations <sup>2</sup></b>		
e. Could there be adverse consequences for the youth/parent or guardian (data subject) from the collection of personal information? If so, should that information be collected or used? Can the same results be accomplished with anonymous aggregate information?		
f. What is the minimum information necessary and relevant to the purposes of the proposed application? Why is that information needed? Is any additional information being collected or used? If so, why is it necessary?		
g. Will there be collection of any new personal information? What is the authority for the collection? Is new legislation/regulation/policy required or appropriate? What are the purposes of the collection? Will the information be collected directly from the youth, parent or guardian (data subject), if not, why not?		

<b>3. Data quality</b>	<b>Yes</b>	<b>No</b>
a. Are the data quality assessments of the JIS participating agencies compatible?		
b. If they are not compatible, can you identify the weakest “link(s) in the chain”?		
c. Is there a procedure in place to address (improve) data quality at the weakest point(s)?		
<b>Data Quality - Additional Considerations <sup>2</sup></b>		
d. What steps will be taken to ensure that the information needed for the proposed [JIS] application is accurate and up-to-date?		
e. What procedures are in place to verify information and to ensure that information will not be used if it is inaccurate or out-of-date?		

<b>4. Use limitation</b>	<b>Yes</b>	<b>No</b>
a. Are the use limitation policies of the JIS participating agencies compatible?		
b. Are the public access policies of the JIS participating agencies compatible?		
c. Is information “publicly accessible” under one JIS participating agency’s public access policy also “publicly accessible” under all the other’s public access policies?		
d. Does the JIS have mechanisms to inform data subjects of third-party (public), secondary use disclosure?		
e. Does the use of information throughout the JIS derive <i>new</i> information (such as a compilation)?		
f. Are the JIS participating agencies only using this information according to the agreed purpose of the JIS?		
g. Are JIS participating agencies aware that their decision-making may be based on “new” (aggregated) information?		
h. Do the JIS participating agencies have safeguards, or review procedures, at these decision-making points?		
i. Does the JIS limit the release of this new information to secondary sources such as scientific, educational, or other government organizations; private industry; the media; information resellers; and private individuals?		
<b>Use Limitation - Additional Considerations <sup>2</sup></b>		
a. How is information from the [JIS] application to be used? Who will be using the information? What technological or policy restrictions should be in place to ensure that there are no unrelated or unauthorized uses or users?		
b. How long will information need to be kept in order to achieve the purpose of the proposed [JIS] application? What provisions are in place to ensure information is not retained for too long or disposed of too soon?		
c. How will the information used in the proposed [JIS] application be disposed of?		

<b>5. Security</b>	<b>Yes</b>	<b>No</b>
a. Are security levels of the JIS participating agencies' systems compatible?		
b. Can the weakest "link(s) in the security chain" in the integrated system be identified?		
c. Is there a procedure in place to address (improve) security at this weakest point(s)?		
d. Are there procedures in place that allow improvement (upgrade) in security while still maintaining the interagency flow of information in the integrated system?		
<b>Security - Additional Considerations <sup>2</sup></b>		
e. How will the information to be used in the proposed [JIS] be secured? What procedures are in place to determine that the proposed methods of security are appropriate for the type of records and the nature of any possible risks?		
f. What safeguards against such risks as unauthorized access, destruction, modification, use, or disclosure are necessary and appropriate? How will these be tested and monitored?		

<b>6. Openness and transparency</b>	<b>Yes</b>	<b>No</b>
a. Are the openness standards of the JIS participating agencies compatible?		
b. Are there openness standards for the JIS itself?		
c. Does the JIS have a general policy of openness about developments, practices, and policies with respect to the <i>management</i> of personal information (apart from the actual information)?		
d. Does openness include public access to the management practices for the information?		
e. Does openness require clear communication to affected individuals if agencies within the integrated system sell or release personal information to third parties?		
f. Does openness require clear communication to affected individuals if agencies within the integrated system sell or release personal information pursuant to public access policies?		
<b>Openness and Transparency – Additional Considerations <sup>2</sup></b>		
g. Will the design of the proposed [JIS] permit the severance of selective personal information from the database? If not, why not?		

<b>7. Individual participation <sup>1</sup></b>	<b>Yes</b>	<b>No</b>
a. Are access- to- information policies of the individual JIS participating agencies compatible?		
b. Are challenge procedures of individual JIS participating agencies comparable?		
c. Do the access policies and challenge procedures of the JIS participating agencies have no measurable negative impact on the day to day operation of the integrated system?		
<b>Individual Participation - Additional Considerations <sup>2</sup></b>		
d. Will the proposed [JIS] provide individuals with a right of access to their information?		
e. Is there anything in the design of the proposed [JIS] that prevents any individual from being able to access or correct their personal information? If so, how will access be adapted to ensure they can?		
f. Will the design of the proposed [JIS] permit access to be provided, within reason, to requesters in a comprehensible form? Will alternative formats necessitate any additional costs? How can the costs be minimized?		
g. Will the youth/parent or guardian (data subjects) know about the existence of the proposed [JIS] and if not, why not? What reasons exist for not requiring data subject knowledge and consent for all aspects of the application?		
h. Will the youth/parent or guardian (data subject) be notified about the existence of [JIS]? If not, why not? If so, what type of notification would be appropriate?		
i. Will the sources of the [JIS] data be tracked? How will that information be communicated to the youth/parent or guardian (data subjects) if they request identification of sources?		

<b>8. Accountability</b>	<b>Yes</b>	<b>No</b>
a. Is there an information steward for the system who is accountable for complying with measures that give effect to the privacy design principles, public access policy, and any applicable law or regulation?		
b. Is the information steward accountable for (1) ensuring all the above privacy design principles have been incorporated in the technology design from the conceptual and contextual phase through implementation; (2) ensuring information systems are capable of providing access to personal information on request, and recording who has had access to the personal information and for what purpose; (3) ensuring staff managing information are trained on privacy protection requirements as detailed; (4) ensuring information systems are transparent and documented so that individuals or a proxy can be informed about the collection, access, use, and disclosure of their personal information within the context of the principles outlined above; and (5) establishing regular security and privacy compliance audits commensurate with the risks to the data subject or other individuals with a relationship to the justice system?		
c. Has the information steward been assigned responsibility for completing PIAs and conducting ongoing privacy assessments to a Privacy Project Manager or other individuals or bodies?		
<b>Accountability - Additional Considerations <sup>2</sup></b>		
d. Will there be an opportunity to test the proposed [JIS] in order to evaluate the effectiveness of privacy protective measures and to identify and address any problem?		
e. Who will be held accountable for maintaining the proposed [JIS] application and for complying with the Acts?		

<b>9. Additional Considerations - Disclosure<sup>2</sup></b>	<b>Yes</b>	<b>No</b>
<p>a. When and how should the information related to the proposed [JIS] be disclosed, and to whom? Will the public have access? If so, should the answers to these questions be reconsidered?</p>		
<p>b. What are the official duties or legitimate functions that would need information from the proposed [JIS]? Why would the information related to the JIS be necessary for that performance? What is the minimum amount of information necessary for that performance? Can it be performed with aggregate or anonymous information?</p>		
<p>c. Will the database of the proposed JIS application be sold? Should it be? What steps should be taken to minimize the negative impact on privacy?</p>		

<b>10. Additional Considerations – Personal Information</b>	<b>Yes</b>	<b>No</b>
<p>a. Will the information to be included in the proposed [JIS] fall under [state, federal, or tribal laws’] definition of personal information? If so, is it absolutely necessary to use identifiable information? Why? If not, should the information still be managed in accordance with fair information practices in order to be responsive to the public’s concern about use of advanced information technology?</p>		
<p>b. Will the proposed [JIS] enhance the privacy of individuals’ personal information currently held by the participating agencies?</p>		
<p>c. Will the proposed [JIS] make available or reveal any previously unavailable personal information? How will newly available information be protected?</p>		
<p>d. How might the public react if the information to be included in the proposed [JIS] is to be shared on the Internet? Would that estimated reaction warrant a re-thinking of the information to be included in the proposed [JIS] application?</p>		

<b>11. Additional Considerations - Protection of Privacy<sup>2</sup></b>	<b>Yes</b>	<b>No</b>
a. Will the proposed [JIS] aggregate or computerize any information, public or personal, that may alter the existing privacy interests of that information? If so, are new or special privacy safeguards to be implemented?		
b. Are there less privacy-intrusive alternatives that can produce equivalent results? What other options have been considered, what was their impact on privacy, and why were they not selected?		

<b>12. Additional Considerations - Computer Matching<sup>2</sup></b>	<b>Yes</b>	<b>No</b>
a. Will the information to be included in the proposed [JIS] need to be linked or matched with information from other databases? Why? What steps should be taken to minimize the negative impact on privacy?		

## ***Assessing the Integrated System Answers***

“The above questions are phrased to help identify possible areas of information privacy vulnerabilities within a JIS. Where a question is answered in the negative (“No”), the JIS collaborative/governance body should document the following items for each such answer:

1. What is the reason(s) that you answered “No”?
2. Is there a law, regulation, or articulated policy that would except the JIS from compliance
3. Is there a logical exception related to the purpose of the integrated system (e.g., law enforcement investigation or intelligence gathering)?
4. What can be done to make the answer to this question “Yes”?
5. If you must retain the identified privacy risk, what plans or procedures are in place to mitigate possible effects of the identified risk?”

*Justice Information Privacy Guidelines*

### *Justice Information Privacy Guidelines*

“The documented responses become the foundation for a description of JIS privacy protections and identification of gaps or weakness. Where the JIS falls short of meeting the privacy objectives, these areas should be brought to the attention of the JIS governance body and system ‘information steward,’ receive additional consideration, and inform the development of policies to reduce gaps or weaknesses in privacy protection.”

Please refer to the discussion in *Justice Information Privacy Guideline*, page 93, and the *Privacy Policy Development Guide* [http://it.ojp.gov/documents/Privacy\\_Guide\\_Final.pdf](http://it.ojp.gov/documents/Privacy_Guide_Final.pdf) for how the PIA analysis is used to inform privacy policy development.

## **Links to Juvenile Justice and other Youth Service Agency Flow Charts**

### **Juvenile Justice Flow Charts**

<http://www.supreme.state.az.us/jisd/jolts/FlowChart.htm>

[http://www.tmcec.com/coursemats/FY05judges/charts/Juvenile\\_flowchart\\_after\\_Sept2003CA.pdf](http://www.tmcec.com/coursemats/FY05judges/charts/Juvenile_flowchart_after_Sept2003CA.pdf)

<http://www.co.honolulu.hi.us/prosecuting/juvenile.htm>

<http://www.juveniledefender.org/pdfs/scchart.pdf>

<http://mentalhealth.samhsa.gov/publications/allpubs/SMA01-3537/chp18figure1.asp>

<http://www.phila.gov/districtattorney/CriminalJusticeSystem/juvenileFlowChart.html>

[http://www.co.lancaster.pa.us/da/lib/da/vitctim\\_witness/Juvenile\\_Justice\\_Flow\\_Chart.pdf](http://www.co.lancaster.pa.us/da/lib/da/vitctim_witness/Juvenile_Justice_Flow_Chart.pdf)

[http://www.mncasa.org/svji\\_legal\\_flow2.html](http://www.mncasa.org/svji_legal_flow2.html)

<http://jja.state.ks.us/process.htm>

<http://www.cwla.org/programs/juvenilejustice/caseflowchart.pdf>

### **Mental Health**

[http://www.cimh.org/downloads/Healthyfam\\_update\\_may01.pdf](http://www.cimh.org/downloads/Healthyfam_update_may01.pdf) (page 3)

### **Victim/Offender Remediation**

<http://www.courtinfo.ca.gov/programs/cfcc/pdffiles/vorp.pdf> (page 93)

### **Child Welfare Flow Chart**

<http://www.cwla.org/programs/juvenilejustice/DCFS1.pdf>