National Governors Association

Issue Brief

A System of Trust: Privacy Policies for Justice Information Sharing

Executive Summary

Privacy policies are the lynchpin of a system of trust that allows agencies and states to share information. States need privacy policies to govern their justice information systems to ensure that personal information is protected and only accessed by authorized users at appropriate times. In fact, for many states, privacy policies serve as the fundamental concept of operations for the entire justice information system. Without strong privacy policies, states and their component justice agencies leave themselves open to liability.

Recognizing the need to protect sensitive information and employ fair information practices the NGA Center for Best Practices (NGA Center), in partnership with the Bureau of Justice Assistance of the U.S. Department of Justice (BJA), worked to help five states create and implement privacy policies for their integrated justice information systems. State teams from **Alabama**, **Hawaii**, **Kansas**, **Nebraska**, and **Wyoming** received technical assistance from a national faculty of privacy experts during the Privacy Policy Academy and were able to develop privacy policies that conform to best practices.

This report builds on the lessons of the academy, identifies common challenges that states face when developing privacy policies for justice information sharing systems, and provides a roadmap for states to implement privacy policies based on the experiences of the states participating in the policy academy.[1] Governors can achieve public trust and confidence by ensuring that justice agencies establish adequate privacy protections and enforce limitations on how personal information is accessed and utilized at all points within the justice system through the following actions:

- Empower a team of key stakeholders to coordinate all aspects of the development and implementation of a privacy policy for the justice information sharing system;
- Conduct a legal analysis of extant privacy laws and regulations;
- Assess the privacy risks and vulnerabilities of the various components of the justice information sharing system via a privacy impact assessment;
- Write and review the privacy policy; and
- Establish auditing, security, and enforcement mechanisms in the justice information sharing system to ensure system accountability.

An Overview of Privacy in Justice Information Sharing

What Is a Privacy Policy?

Justice information systems contain information from across states' justice enterprises— including court data, criminal histories, victims' personal information, criminal intelligence, mental health records, presentencing investigations, motor vehicle information, and other pertinent information.[2] Although the ability to share that information is vital to criminal justice decisionmakers, justice agencies are susceptible to lawsuits, sanctions, and reputational damage if personal information is misappropriated or shared with unauthorized users.

In the context of information sharing, the term privacy refers to an individual's interest in preventing the inappropriate collection, storage, and use of personal information.[3] A "privacy policy" is a written statement that dictates how an information sharing entity handles personally identifiable information (PII).[4] In an information sharing environment, the person or entity sharing information must balance the need for information with the expectation of privacy. A privacy policy does just that by identifying how an organization will collect, disseminate, store, and dispose of information.

Most privacy policies contain aspects of the Fair Information Principles established by the Organization for Economic Cooperation and Development (OECD) in 1980 (see Box 1). The OECD's guiding principles for protecting personal information are industry standards that provide a basic framework of several information sharing components.[5]

Box 1: Fair Information Principles

The Organization for Economic Cooperation and Development (OECD) established guiding principles for protecting personal information.

1. Purpose Specification Principle. Identify the purposes for which all personal information is collected, and keep subsequent use of the information in conformance with such purposes.

2. Collection Limitation Principle. Review how personal information is collected to ensure it is collected lawfully and with appropriate authority, and guard against the unnecessary, illegal, or unauthorized compilation of personal information.

3. Data Quality Principle. Implement safeguards to ensure information is accurate, complete, and current, and provide methods to correct information discovered to be deficient or erroneous.

4. Use Limitation Principle. Limit use and disclosure of information to the purposes stated in the purpose specification, and implement realistic and workable information retention obligations.

5. Security Safeguards Principle. Assess the risk of loss or unauthorized access to information systems, and ensure ongoing use conforms to use limitations.

6. Openness Principle. Provide reasonable notice about how information is collected, maintained, and disseminated and describe how the public can access information as allowed by law or policy.

7. Individual Participation Principle. Allow affected individuals access to information related to them in a manner consistent with the agency mission and when such access would otherwise not compromise an investigation, case, court proceeding, or agency purpose and mission.

8. Accountability Principle. Have a formal means of oversight to ensure the privacy and information quality policies and the design principles contained therein are being honored by agency personnel.

Source: Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980).

Who Do Privacy Policies Protect?

Privacy policies protect the public from unauthorized use of personal information contained in justice information sharing systems. They also protect authorized individuals or entities that are handling personally identifiable information (PII).

PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[6]

PII can be compromised in two ways: (1) an unauthorized person gains access to PII; or (2) an authorized person uses the PII in a way that is beyond the scope of their occupational duties. The misappropriation of PII can lead to identify theft, physical harm, personal embarrassment and lack of trust in the entity storing and exchanging the information. A privacy policy reduces the chances of those outcomes by providing accountability and legal recourse for information breaches, whether negligent or intentional. Justice information sharing systems that do not have privacy policies are effectively operating without a safety net.

What Is the Global Justice Information Sharing Initiative?

The Global Justice Information Sharing Initiative—referred to as "Global"— serves as a federal advisory committee that advises the U.S. Attorney General on advances in information sharing.[7] Consisting of group of groups representing more than 30 independent law enforcement, judicial, correctional, and related organizations, the initiative was created to support the broad exchange of pertinent justice and public safety information.

The Office of Justice Programs of the U.S. Department of Justice provides assistance to Global's member organizations and facilitates several working groups of the Global Advisory Committee. These working groups have developed several technology tools and best practices to assist states in improving their capabilities to share justice information. The Global Privacy and Information Quality Working Group, for example, has created a set of standards and products that tackle common privacy issues and assist with the development of privacy policies. Some of the resources developed by that working group are highlighted in the "Resources" section in Appendix A of this issue brief.

The NGA Center Privacy Policy Academy

In an effort to assist states, the NGA Center, in partnership with BJA, launched a multi-state policy academy designed to help states develop and implement privacy policies conforming to best practices established by Global.

Five states participated in the policy academy—**Alabama**, **Hawaii**, **Kansas**, **Nebraska**, and **Wyoming**—and received technical assistance from a national faculty of privacy experts to create privacy policies for their integrated justice information systems. Many of the resources developed by the Global Privacy and Information Quality Working Group of the Global Justice Information Sharing Initiative were used to engage participating state teams during the creation and implementation of their policies. Key questions that states or other entities developing a privacy policy should consider are identified in Box 2.

As discussed below, four of the five states participating in the NGA Center's Privacy Policy Academy developed their privacy policy for justice information sharing as a component of a multistate initiative. The fifth state focused on developing a privacy policy to govern information sharing within the state.

The Consortium for the Exchange of Criminal Justice Technology (CONNECT) Project: A Multi-Jurisdictional Approach to Information Sharing

In 2007, **Alabama, Kansas, Nebraska,** and **Wyoming** founded the Consortium for the Exchange of Criminal Justice Technology (CONNECT) in the hope of eventually linking their justice information systems—the Alabama Criminal Justice Information Center, the Kansas Criminal Justice Information System, the Nebraska Crime Commission, and the Wyoming Division

Box 2: Questions to Consider When Developing a Privacy Policy

What type of governance structure does the information sharing initiative follow?

What statutes or local laws, related to privacy, govern your information sharing initiative?

How will information exchanges be monitored?

What kind of information will be shared, stored and retained?

How will information be shared, stored and retained?

of Criminal Investigation—to allow authorized users to obtain state and local criminal justice information across state lines.[8]

At the end of 2009, with support from the U.S. Department of Justice and the National Governors Association, and the National Criminal Justice Association, the CONNECT project initiated a proof-of-concept capability, including a secure information sharing federation and technology framework built upon the information sharing standards created by the Global Justice Information Sharing Initiative. The first data set to be shared among CONNECT member states was drivers' license information, which can now be securely shared by authorized criminal justice officials in compliance with the privacy and operating policies of the consortium and participating states.

At the NGA Center's Privacy Policy Academy, representatives of the four states that founded CONNECT sought to develop a privacy policy for justice information sharing that would (1) meet the legal requirements of all four member states; (2) define authorized purposes for accessing information via the portal; (3) establish policies for secondary dissemination; (4) detail logging and auditing requirements; and (5) describe enforcement policies for misuse. In addition, CONNECT members wanted to design a privacy policy that would be extensible to other states**.**

The Hawaii Integrated Justice Information Sharing (HIJIS) Program: An Intrastate Sharing Approach

Key justice officials in Hawaii have long recognized the need to build integrated information sharing and access capabilities among justice agencies and other governmental entities throughout the State of Hawaii. The Hawaii Integrated Justice Information Sharing Program (HIJIS) was initiated in 2007 to build statewide information sharing capabilities to enable real-time access and automated data exchange throughout the whole of the state's justice and public safety system. To address the growing demand for justice information by government agencies to support employment screening, firearms purchases, licensing, victim notification, and other applications, HIJIS shares information for both justice and nonjustice purposes.

At the NGA Center's Privacy Policy Academy, representatives from Hawaii sought to develop a privacy policy focused on the exchange of arrest information. A step-by-step description of HIJIS's privacy policy development process is presented in Appendix B of this report.

Challenges in Creating Privacy Policies for Justice Information Sharing

The states participating in the NGA Center's Privacy Policy Academy identified a number of common challenges in developing and implementing privacy policies for justice information sharing systems. One over-

arching theme that emerged from the academy was the importance of balancing law enforcement's need for access to information with protection of individuals' privacy rights. The National Association of State Chief Information Officers reiterated the point in a recent publication: "One of the major factors unique to government is the inherent openness that is expected of government at all levels. That has created a challenge of balancing that expectation of openness and transparency with the need to protect the privacy of personal or sensitive citizen information."[9]

States also noted a number of other challenges in developing and implementing privacy policies, which include the following:

Multiple stakeholders involved in the creation of a privacy policy. A key challenge in implementing a privacy policy in an integrated justice information sharing system is managing the large number of stakeholders involved in the policy development process. **Hawaii's** HIJIS, for example, includes information from over 20 agencies, each with its own leadership, culture, funding sources, technologies, legal constraints, and missions. For the CONNECT project, the geographic distance between member states (**Alabama, Kansas, Nebraska,** and **Wyoming)** created additional challenges related to communication and data governance. To manage such challenges, states should create and execute a memorandum of understanding (MOU), joint powers agreement, or other formal agreement that details how information is to be shared and governed.

The need to identify a project "champion" for the privacy initiative. Another challenge in developing privacy policies in justice information sharing is identifying an individual or agency to oversee the privacy development process and to ensure that the all of the correct players are involved—that is, a project "champion." A project champion is likely to come from the executive branch of government (e.g., be a governor's policy advisor) and should be tasked with establishing buy-in from key players in all branches of government and educating personnel about the importance of enacting privacy protections. Creating a privacy policy requires personnel to complete thorough policy and legal analyses and conduct capabilities assessments. The project champion must facilitate that process from start to finish and ensure that stakeholders are aware of all privacy concerns.

Multiple and conflicting privacy laws. Privacy policies in integrated justice information sharing systems must align with existing laws and regulations, some of which themselves may conflict, overlap or contain gaps. Existing laws and regulations must be taken into account in the final privacy policy that will govern the information sharing system. For that reason, entities seeking to develop a privacy policy must perform a legal analysis of all pertinent laws and regulations pertaining to privacy. CONNECT representatives conducted an in-depth legal review that was inclusive of all of the four member states' laws prior to developing their privacy policy. They decided to operate under the legal authorities of the CONNECT member state with most stringent privacy protections for cross-jurisdictional information sharing, ensuring that all four member states would be able to share information without violating any member state's laws or regulations.

Creating auditing, security, and enforcement mechanisms. To prevent the unwarranted use and misappropriation of PII, justice information sharing systems must have security mechanisms, frequent auditing, and sanctions for violations of privacy policies. The "failure to develop, implement, and maintain appropriate protections for both information and use of technology can result in: harm to individuals; public criticism; loss of confidence in and cooperation with the agency; and lawsuits and liability."[10] Existing agency security systems must be strengthened and agencies must make sure that regular audits are conducted to ensure that information is being used for the purposes specified in the privacy policy and MOU. The geographic distance between states in CONNECT made cross-jurisdictional auditing and enforcement difficult.

Recommendations for Creating Privacy Policies for Justice Information Sharing

The states that participated in the NGA Center's Privacy Policy Academy were asked to identify key lessons from developing and implementing their privacy policies for justice information sharing. The following five recommendations from those states will prove useful to other states as they move forward in developing privacy policies for their justice information sharing initiatives.

Empower a team of key stakeholders to coordinate all aspects of the development and implementation of a privacy policy for the justice information sharing system.

Understanding what makes an effective privacy policy requires a grasp of foundational privacy issues that the average justice practitioner may not have.[11] Consequently, it is important for justice information sharing system officials to empower a team of stakeholders through a committee, working group, or development team and to give this team the responsibility of coordinating all aspects of the development of a privacy policy.

The responsibilities of the privacy team should include (1) creating a governance structure for how information will be shared, stored, and disposed of; (2) appointing a privacy officer[12]; (3) developing a mechanism to train personnel on procedures described in the privacy policy; and (4) ensuring that the privacy policy is vetted and reviewed regularly.

The team should be comprised of stakeholders who will oversee the development of the state's privacy policy for sharing justice information should include legal counsels, policymakers, privacy policy analysts or advisors, consultants from privacy advocacy groups, and justice decisionmakers (e.g., department of corrections official, judges, sheriffs). The team should include members that are familiar with both technical and policy related components of the justice information sharing system. In Hawaii, for example, HIJIS created both an operational working group and a technical working group to draw on expertise in those interrelated areas.

Conduct a legal analysis of extant privacy laws and regulations.

Conducting a thorough legal analysis of extant privacy laws and regulations is a crucial step that should be completed in the initial stages of privacy policy development. A thorough legal analysis can help to ensure the privacy policy that is developed complies with all relevant privacy statutes and regulations in the jurisdiction(s) where information exchanges will occur. Such an analysis will also give policymakers a sense of the legal issues likely to be encountered when exchanging information.

The privacy team must define the scope of the privacy policy it plans to develop before examining relevant statutes, as some laws and regulations may or may not be applicable. Sources of legal authority include, but are not limited to, federal and state case law, federal and state constitutions, executive orders, local ordinances, and data collection laws.[13] Although there are several approaches to completing a legal analysis, privacy teams should focus on the basics, such as the types and quality of information (e.g., intelligence, incident reports) that will be collected and exchanged and how the information will be disseminated.

Assess the privacy risks and vulnerabilities of the various components of the justice information sharing system via a privacy impact assessment.

Before beginning to draft a privacy policy, participating agencies must conduct a "privacy impact assessment" to identify the risks and vulnerabilities that exist within the justice information sharing system and any information exchanges that will occur. A privacy impact assessment is a series of questions that "evaluate the processes through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application."[14]

Such an assessment contains multiple sections of detailed questions that address the following: the system architecture, type(s) of information shared and stored within the system, uses of the information in the system, disclosure practices, internal and external sharing, notification, accessibility and redress, and technical access and security.[15]

A privacy impact assessment will give agency participants, privacy analysts, and outside technical assistance consultants a better understanding of the particular needs of the justice information sharing system and how to address those needs. Assessing those vulnerabilities allows states and participating agencies to put remedial measures in place. Additionally, states can mitigate the risks created by those vulnerabilities by ensuring they are addressed in the privacy policy and/or through technology improvements.

All of the states involved in the Privacy Policy Academy were required to conduct privacy impact assessments. The privacy impact assessment was especially important for the CONNECT project to determine the differences and similarities in participating states' policies and the need to resolve potential challenges related to differing state statutes and policies regarding use and access to data in the member states.

Write and review the privacy policy.

Once a governance agreement is in place and a legal analysis and a privacy impact assessment has been conducted, the state team is ready to write a privacy policy for justice information sharing. Team members may appoint an individual with a legal background to draft the policy, but that is not required. Existing privacy policies from other states that have similarities in governance and the type of information that will be shared may be used as a starting point for creating an outline or initial draft.

Team members should also consult the following resources developed by the Global Privacy and Information Quality Working Group when drafting their policies:[16]

- *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities*. This is a hands-on guide for justice practitioners that provides sensible guidance for articulating privacy obligations in a manner that protects the justice agency, the individual, and the public. The guide provides an approach to the planning, education, development, and implementation of agency privacy protections. Also included are drafting tools, such as a policy template a glossary, legal citations, and sample policies.
- *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities*. This is a template with provisions that are intended to be incorporated into the agency's day-to-day operations. Sample language is included for each provision.
- *Policy Review Checklist*. This checklist is a companion piece to the policy development template and serves both as a self-assessment tool to assist privacy policy authors, project teams, and agency administrators in evaluating whether the provisions contained within their draft policy have met the core concepts recommended in the policy development template and as a resource for use during the annual policy review.

To ensure that a privacy policy for justice information sharing is correctly drafted and includes all privacy nuances and legal intricacies, state teams should consult with subject matter experts or technical assistance providers.

When the state team is satisfied with the policy resulting from the line-by-line review, it should vet the policy to a wider net of stakeholders ensuring that there is agreement and buy-in. Once the privacy policy is vetted and completed, the project champion or privacy officer must ensure that the policy is reviewed annually to account for changes in law, policies, and procedures within the system.

Establish security, auditing, and enforcement mechanisms in the justice information sharing system to ensure system accountability.

Fully operational security and auditing mechanisms are crucial to ensure the protection of information in the justice information sharing system. Minimum security functions implemented in justice information sharing systems, in accordance with existing federal security policy and guidance from the National Institute of Standards and Technology, should include the following: (1) data encryption; (2) controlling and limiting remote access to the information; (3) using a time-out function that requires re-authentication after 30 minutes of inactivity; (4) implementing a log and verify system that requires any information that is extracted from the system to be logged in a database and verified by an auditor or supervising official; and (5) ensuring understanding of responsibilities.[17] Participating states and agencies must monitor use and regularly create audit trails that describe who is accessing the information and for what purposes.

Beyond imposing security and auditing requirements, state entities should impose and enforce sanctions for misuse of information from the justice information sharing system. Sanctions can be punitive, ranging from reprimanding the unauthorized user to disallowing the offending agency from participating in further information exchanges and criminal prosecution. The MOU or joint powers agreement should describe, in detail, the procedures and recourse for access violations.

Conclusion

The main objective of the NGA Center's Privacy Policy Academy was to aid participating states in developing effective privacy policies that adhere to established best practices for justice information sharing systems. The successful development of such privacy policies by the multistate CONNECT project and Hawaii's HIJIS demonstrates that states can develop policies that protect the privacy without compromising the efficiency and quality of information shared. If states follow the policy development recommendations of the five states that participated in the policy academy, they will improve justice outcomes while ensuring that personal privacy rights have not been violated.

Contact: Anne-Elizabeth Johnson
Policy Analyst, Homeland Security and Public Safety
202/624-7854
ajohnson@nga.org

Appendix A: Resources

There are many resources that governors and other policymakers can turn to for additional information and assistance on privacy policy development and implementation in justice information sharing systems.

Working Groups of the Global Justice Information Sharing Initiative

The Global Justice Information Sharing Initiative is a group of groups representing more than 30 independent law enforcement, judicial, correctional, and related independent organizations that serves as a federal advisory committee that advises the U.S. Attorney General on justice information sharing integration services. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete and accessible information in a secure and trusted environment."[18]

Some of the resources available from two standing committees of the Global Justice Information Sharing Initiative—the Global Privacy and Information Quality Working Group (GPIQWG) and the Global Security Working Group (GSWG)—are discussed below. All of these products are available for download at the following website: http://www.it.ojp.gov/privacy.

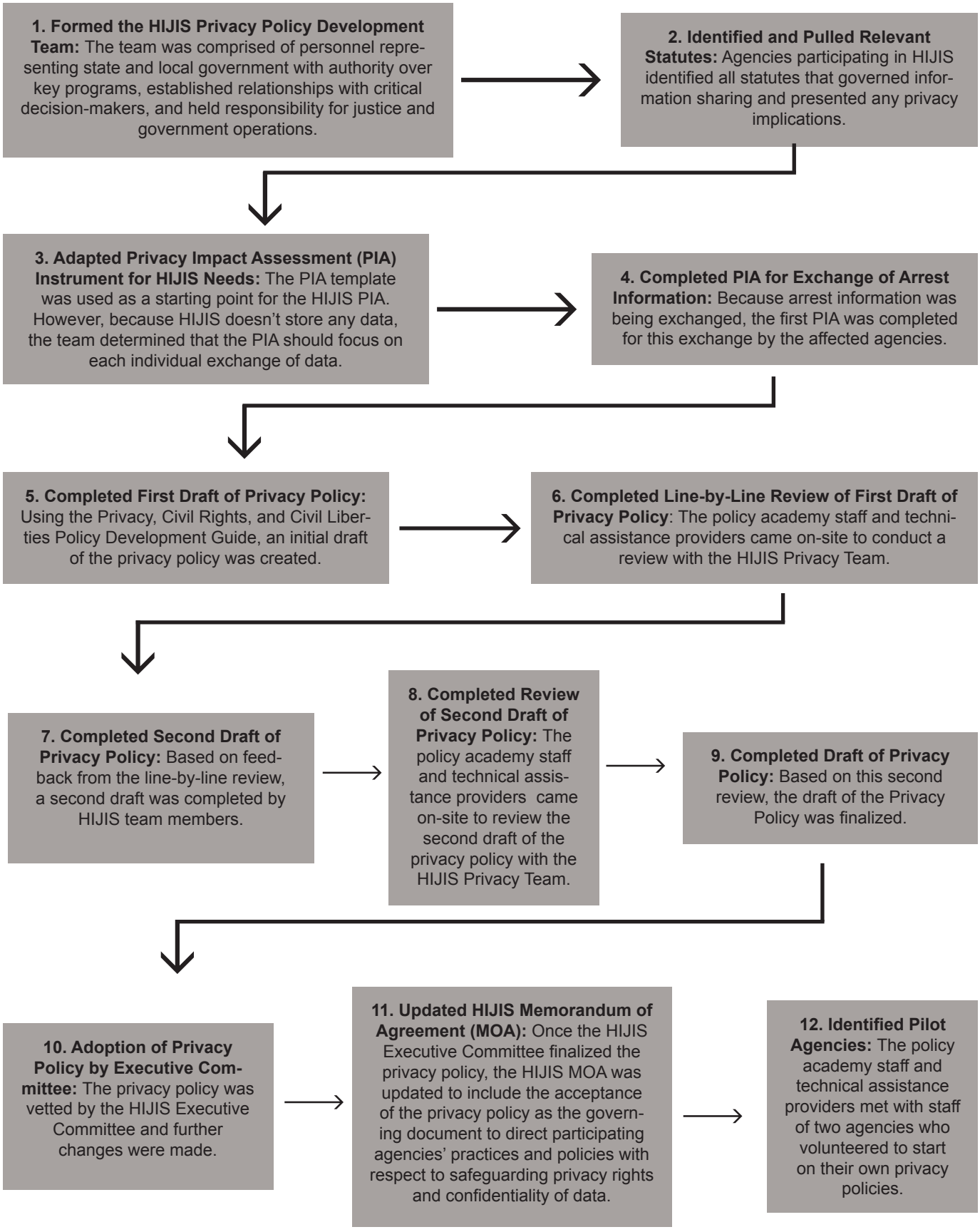
Global Privacy and Information Quality Working Group (GPIQWG). The work of the GPIQWG is designed "to assist government agencies, institutions, and other justice entities in ensuring that personal information is appropriately collected, used, and disseminated within integrated justice information systems." Of particular interest are several resources developed by the GPIQWG:

- *Guide to Conducting Privacy Impact Assessments for State, Local and Tribal Information Sharing Initiatives;*
- *Guide to Conducting Privacy Impact Assessments: Privacy Impact Assessments Template;*
- *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Entities;*
- *Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Entities;*
- *Policy Review Checklist;*
- *Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development;*
- *Global Justice Information Sharing Initiative: Privacy Policy Statement;*
- *7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy;* and
- *Global Privacy Resources.*

Sample Privacy Policies for Justice Information Sharing

The major outcome of the NGA Center's Privacy Policy Academy was the creation of privacy policies by participating state justice information sharing systems. If you would like to view the completed privacy policies, please contact the NGA Center for Best Practices in Washington, D.C. You may send inquiries to Anne Johnson at ajohnson@nga.org.

Appendix B: The Hawaii Integrated Justice Information Sharing (HIJIS) Program's Privacy Policy Development Process



Endnotes

1. The Bureau of Justice Assistance at the U.S. Department of Justice, Bureau of Justice Assistance has made privacy and civil liberties protections a top priority in its strategic plan: *Justice Information Sharing: A 2010-2012 Strategic Action Plan.*
2. Not all justice information sharing systems include the types of data identified in this section.
3. Commonly defined as the right to be left alone, privacy is best described as a civil liberty that limits the government's ability to restrain or dictate an individual's actions. In contrast to civil liberties, civil rights are constitutionally guaranteed privileges and protections that involve affirmative government action. Both are the legal protections that safeguard individual freedom and ensure equal treatment under the law. In general, civil liberties entwine civil rights although they are distinct. See Office of Justice Programs, U.S. Department of Justice, "Privacy and Civil Liberties: Commonly Used Terms in Privacy, Civil Liberties, and Information Sharing," revised April 12, 2010. Available at: <http://it.ojp.gov/default.aspx?area=privacy&page=1268#top> (accessed March 25, 2012).
4. Global Justice Information Sharing Initiative, U.S. Department of Justice, *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities, April 2011*. Available at: <http://www.nga.org/files/live/sites/NGA/files/pdf/1106CYBERCRIMEFORUMPRIVACY.PDF> (accessed March 25, 2012).
5. Thomas MacLellan, "Protecting Privacy in an Integrated Justice World," NGA Center for Best Practices, Washington, D.C., April 12, 2006. (Note: Short descriptions of each guiding principle are provided in Box 1 on Fair Information Principles of this issue brief.)
6. Government Accountability Office, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO Report 08-536 (Washington, D.C.: May 2008). Available at: <http://www.gao.gov/new.items/d08536.pdf> (accessed March 25, 2012).
7. Office of Justice Programs, U.S. Department of Justice, "Global Justice Information Sharing Initiative," n.d. Available at: <http://www.it.ojp.gov/default.aspx?area=globalJustice&page=1019> (accessed March 31, 2012).
8. For more information on the CONNECT Consortium for the exchange of justice information technology, visit the consortium's webpage at <http://www.connectconsortium.org/> (accessed March 25, 2012). For more information on the Global Justice Information Sharing Initiative, visit the U.S. Department of Justice's webpage on the initiative at <http:// it.ojp.gov> (accessed March 25, 2012).
9. National Association of State Chief Information Officers, "Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?" Lexington, Kentucky, October 2006. Available at: <http://www.nascio.org/publications/documents/NASCIO-Keeping%20Citizen%20Trust.pdf> (accessed March 25, 2012).
10. Global Justice Information Sharing Initiative, U.S. Department of Justice, "Executive Summary for Justice Decision Makers: Privacy, Civil Rights and Civil Liberties Program Development," revised September 6, 2011. Available at: <www.it.ojp.gov/docdownloader.aspx?ddid=1462> (accessed March 25, 2012).
11. The Global Privacy and Information Quality Working Group product *7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy* identifies as the first step in developing a privacy policy the importance of "understanding foundational concepts" such as how privacy issues arise and the purpose of a privacy policy. For more information on this product, see the section on "Resources" cited in Appendix A at the end of this issue brief.
12. A privacy officer is an individual, usually appointed by the governance committee of the information sharing system, who oversees and responds to all privacy inquiries.
13. For an exhaustive list of legal authorities, see the references cited in note 4 above.
14. Bureau of Justice Assistance, U.S. Department of Justice, Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Information Sharing Initiatives. Available at: <www.it.ojp.gov/docdownloader.aspx?ddid=1181> (accessed March 25, 2012).
15. All states involved in the NGA Center for Best Practice's Privacy Policy Academy were required to complete privacy impact assessments. For samples of those privacy impact assessments, please contact the NGA Center for Best Practices in Washington, D.C.
16. All of these resources created by the Global Justice Information Sharing Initiative, and detailed descriptions are available for download the U.S. Department of Justice's webpage on the initiative at <http://it.ojp.gov> (accessed March 25, 2012).
17. Office of Management and Budget, Executive Office of the President, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," OMB Memorandum 7-16, Washington, D.C., May 22, 2007. Available at: <http://freedownload.is/pdf/safeguarding-against-and-responding-to-the-breach-of-personally--3268631.html> (accessed March 25, 2012).
18. Office of Justice Programs, U.S. Department of Justice, *Global Justice Information Sharing Initiative (Global)*. Available at: <http://it.ojp.gov/default.aspx?area=globalJustice> (accessed March 25, 2012).