BJA
Bureau of Justice Assistance
U.S. Department of Justice

Global Justice Information Sharing Initiative

U.S. Department of Homeland Security

Establishing a Privacy Officer Function Within a Justice or Public Safety Entity

Global Advisory Committee Recommended Responsibilities and Training

Integrated justice systems and advancing information sharing technologies and initiatives enable state, local, tribal, and territorial (SLTT) justice or public safety agencies to collect, use, store, and share information more efficiently than ever before. These efficiencies, however, can be quickly undermined by misuse, unauthorized access, or the entity's failure to adhere to privacy, civil rights, and civil liberties laws, regulations, and policies. Headline-grabbing stories demonstrate that an entity's reputation and perceived effectiveness may depend, to a significant extent, on whether the entity has a sound privacy, civil rights, and civil liberties (privacy) policy and is following privacy protection best practices. Violations may damage the relationship between citizens and those sworn to protect them.

Adopting a privacy policy is a positive and proactive step toward mitigating risks and preventing violations, but the policy alone is just a first step. To adequately ensure that the organization, its personnel, and the personally identifiable information (PII) it collects are managed in compliance with privacy laws and the entity's privacy policy, responsibility needs to be assigned for oversight and execution of these tasks. This role is traditionally performed by the agency's privacy officer, although the function is sometimes only one among many responsibilities that are performed by an individual staff member in smaller entities.

A privacy officer is a person (or persons, within larger justice organizations) whose job, whether a full- or part-time responsibility, is to manage and monitor compliance with privacy laws and the entity's privacy policy; respond to public access and corrections requests or complaints; ensure that agency personnel receive appropriate training; serve as a knowledgeable resource on privacy, civil rights, and civil liberties for the entity; and enforce adherence to the provisions of the privacy policy.

Considerations

Do I Need a Privacy Officer Function?

The function of a privacy officer for a justice or public safety agency is to manage the policies and procedures of the entity as it handles and protects PII and other sensitive information. This is a critical role, since a privacy officer can play a proactive role in helping to prevent privacy-related problems and avoid further problems, thus saving expense in the future. For example, if there is a complaint regarding a breach of PII, the privacy officer can step in to help evaluate, educate, and manage the issue and help ensure that appropriate procedures are followed in addressing the complaint.

You may already have a person or persons in your organization who handle many of these tasks. For example, a court administrator may not be designated as the privacy officer but may be assigned appropriate responsibilities related to the information privacy function.

Your entity may already have a privacy policy in place, in which case the privacy officer will be responsible for policy implementation and training on the policy, as well as compliance and enforcement of the policy. However, if your organization does not yet have a privacy policy, the privacy officer may be designated and tasked with its development, either in coordination with a privacy committee (generally chaired by the privacy officer) or through collaboration with relevant departments, such as the agency's legal counsel.

Whether it is a full-time privacy officer or an individual with multiple job responsibilities who takes on these tasks, it is important that your organization encourage longevity in the role and provide the privacy officer with senior management support, as well as the authority to intervene on privacy, civil rights, and civil liberties issues related to the entity's operations. Organizations also need to professionalize this role to reduce turnover.

The decision of whether to appoint a privacy officer requires a careful assessment, not only of the costs associated with funding this role but also of your entity's ability to mitigate privacy risks and reap the benefits of agencywide privacy policy compliance.

It Is Recommended That You Have a Privacy Officer If:

- **You collect personally identifiable information**
- **You collect medical information**
- **You collect or gather sensitive law enforcement or criminal justice information**
- **You collect, gather, or analyze criminal intelligence information**
- **You participate in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)**
- **Your state has a data breach notification law**
- **You are a fusion center**

Heightened alarm over identity theft, reports of misuse, and frequent high-profile media reports of data security breaches have prompted federal and state legislators to enact legislation designed to protect persons whose sensitive PII, such as social security numbers (SSNs), has been collected. For example, an agency must follow numerous laws put in place prior to collecting SSNs and protect the SSNs,[1] once collected.

Health information collected by the justice system can include confidential medical and mental health records. The Health Insurance Portability and Accountability Act (HIPAA)[2] applies only to HIPAA-covered entities,[3] since such covered agencies are prohibited from using or disclosing protected health information (PHI). However, an agency must be familiar with HIPAA in order to determine when covered organizations may disclose PHI to criminal justice agencies without an individual's written authorization (for example, when an individual is in lawful custody).[4] Covered entities are also required by HIPAA to designate privacy officials[5] to enforce the HIPAA Privacy Rule.

Many state and local law enforcement agencies (Illinois State Police, Los Angeles Police Department, etc.) and entities with responsibility for criminal justice information systems (Indiana Data

Considerations (continued)

Exchange [IDEx], Connect South Dakota [Connect SD], Hawaii Integrated Justice Information Sharing [HIJIS] Program, etc.) have worked to ensure that the role of privacy officer, which is responsible for implementing privacy policies, has been fulfilled.

Many intelligence organizations, including the Regional Information Sharing Systems® (RISS)[6] Centers, have privacy policies that implement Code of Federal Regulations (CFR) Title 28, Part 23 (28 CFR Part 23).

One of the requirments of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)[7] is that fusion centers include provisions in their privacy policies that include the appointment of privacy officers[8] as part of their adoption of the NSI Privacy Protection Framework.[9]

As of August 20, 2012, 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, but they do not all deal with notifications in a standard way. Lawmakers in recent years have attempted to pass a national data breach notification law but so far have been unsuccessful.

The Information Sharing Environment (ISE) Privacy Guidelines require SLTT agencies, including fusion centers, that receive terrorism-related information from federal agencies to adopt a privacy policy that is at least as comprehensive as the ISE Privacy Guidelines,[10] including the designation of a privacy officer. In addition, the U.S. Department of Homeland Security (DHS), as a condition of Homeland Security Grant Program (HSGP) funding, requires that all fusion centers have an approved privacy policy at least as comprehensive as the ISE Privacy Guidelines. To date, all designated fusion centers have completed their privacy policies and appointed privacy, civil rights, and civil liberties (P/CRCL) officers.

Do I Need a Full-Time Privacy Officer?

In larger justice and public safety organzations, the tasks of a privacy officer may require an individual who is devoted full-time to the position. However, particularly for smaller agencies, there are alternatives to hiring or designating a full-time privacy officer, such as the following:

- **Part-time role:** The responsibilities of a privacy officer may be assigned as a function of another already established position or an individual with privacy expertise. For example, the entity's legal counsel may assume privacy officer duties, or the chief of police of a small police department may, because of limited staffing and resources, assume these tasks as part of his or her leadership position.
- **Shared responsibilities/team approach:** A team may be appointed to share day-to-day privacy officer responsibilities; however, it is important that one individual be designated to have the lead and, ultimately, the responsibility and accountability for the privacy officer function.
- **Privacy committee:** An agency may create a privacy committee consisting of representatives from the departments or organizations that have a particular interest and/or expertise in privacy, especially those that should have input into the privacy policy. Senior leadership, however, must take charge of finalizing and implementing the privacy recommendations of the committee or appoint a committee chair who will serve, in a practical sense, as the liaison to a part-time or full-time privacy officer.
- **Positions within parent agency:** Some agencies may wish to request that a relevant position or individual within the entity's parent organization or a support office assume the privacy officer responsibilities. For example, an attorney within the general counsel division of a state's department of public safety may be able to assume privacy officer tasks for the state highway patrol.

It is important, however, to note that privacy officers cannot perform their tasks alone. They must draw upon the knowledge, skills, and experience of various entity personnel, such as the security officer or perhaps an individual within the agency's parent organization. This individual may be a legal counsel, an information technologist, a security officer, a human resources manager, or other professional.

Considerations (continued)

What Qualifications Are Recommended for the Privacy Function?

The following is a list of recommended qualifications for the individual or individuals designated to handle privacy function responsibilities. One individual may not need all of these qualifications, especially if the role is shared across several individuals.

- Knowledge of relevant privacy, civil rights, and civil liberties laws, including, when appropriate, intelligence-related laws and regulations, such as 28 CFR Part 23 and data security and public records laws.
- A general understanding of technology, particularly those areas that are especially related to privacy, such as user authentication and credentialed role-based access.
- An understanding of the agency's justice-related activities, particularly its information management practices—how the entity collects, stores, accesses, uses, disseminates, and purges or destroys PII and other sensitive information.
- Adequate project management skills, because the creation, implementation, and revision of privacy policies, as well as compliance, auditing, enforcement, and training, are ongoing activities of a privacy program cycle.[11]

What Responsibilities Are Recommended for a Privacy Officer?

In order to ensure appropriate access to justice or public safety information while also implementing privacy, civil rights, and civil liberties protections, a privacy officer should be appointed to fulfill key duties and responsibilities identified by the organization. Recommended privacy officer responsibilities include the following:

- Performs a privacy, civil rights, and civil liberties impact assessment to identify privacy risks and vulnerabilities.
- Guides the development of the agency's privacy policy (if none is in place) in coordination with the entity's legal counsel and/or a privacy committee (which is recommended and, when in place, generally is guided by the privacy officer). Ensures an appropriate breadth of input and feedback from other justice or public safety practitioners (stakeholders) on the privacy policy.
- Is familiar with all federal, state, and local laws and regulations concerning the sharing of justice information and information sharing technologies and ensures that the sharing of information and utilization of these technologies comply with the law and address privacy concerns.
- Reviews new or enhanced information and technology programs for privacy issues before they are implemented and shapes policies, directives, and agreements for the information systems.
- Serves, if the agency shares terrorism-related information, as the privacy liaison for the ISE.[12]
- Monitors changes in the data privacy landscape that may warrant updates to the agency privacy policy and annually reviews (or leads the review of) the entity's privacy policy to ensure that it is comprehensive and up to date (i.e., incorporates changes in applicable law, technology, the purpose and use of agency information systems, and public expectations).
- When additional or revised procedures may be called for, works with relevant entity offices in the

Considerations (continued)

consideration, adoption, and implementation of such procedures.

- Oversees the implementation of privacy protections in personnel procedures and information system processes.
- Reviews and approves analytical products for appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the organization.
- Mitigates agency risk related to the release of sensitive information determined to be necessary to protect the public.
- Manages the evaluation, at least annually, of user compliance within information and intelligence systems (for example, through the use of system audits), including logging access to and periodic auditing of these systems.
- Handles reported errors and deficiencies in information and suspected or confirmed violations of the entity's privacy policy provisions.
- Ensures that enforcement procedures and sanctions are adequate and enforced.
- Receives and responds to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the organization.
- Responds to or ensures the proper handling of public records requests for information.
- Handles individuals' requests for corrections, under the agency's redress policy, involving information that the entity has disclosed and can change because it originated the information and complaints related to information that is not subject to disclosure.
- Assists in the development of interagency agreements or memoranda of understanding between the agency and state and local participating agencies for the purpose of enhancing and fostering the responsible exchange of information while ensuring that all privacy concerns, requirements, and responsibilities are addressed.
- Ensures that data breach notification policies and mitigation procedures are adequate and followed in the event of a data security breach.
- Serves as a community liaison regarding the organization's privacy policies and practices and maintains an outreach policy.
- Develops a training curriculum to support the institutionalization of privacy policies and practices for protecting privacy, civil rights, and civil liberties.
- Trains all staff annually and trains new staff members on the agency's privacy, civil rights, and civil liberties policy.
- Ensures that privacy protections are implemented agencywide through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

Resources

The following are some of the key privacy resources developed for state, local, and tribal (SLT) justice and public safety entities by the Global Justice Information Sharing Initiative (Global), Global partners, and DOJ collaborations with other federal agencies, such as the U.S. Department of Homeland Security (DHS).

General

Global Privacy Resources Booklet

A variety of privacy awareness, policy development, and implementation products are available to the justice community today. To help these agencies know which privacy product(s) to use when and for what purpose, Global published this roadmap to help justice entities, particularly privacy officers, navigate these resources. The roadmap illustrates the stages an agency naturally goes through when embarking on such an endeavor (such as education and awareness, self-assessment, policy development, policy evaluation, technical implementation, and more). Together, these stages comprise a privacy program cycle. This booklet graphically illustrates this cycle and guides agencies to the resources they need for each particular stage. Global recognizes that state, local, and tribal (SLT) justice entities come in all sizes, with a variety of roles and with varying degrees of available resources. The resources presented in this booklet are flexible and designed to meet a spectrum of privacy protection needs. In addition to this downloadable booklet, Global has developed an online version of this information available at www.it.ojp.gov/privacy.

Education/Awareness

Executive Summary for Justice Decision Makers: Privacy, Civil Rights, and Civil Liberties Program Development

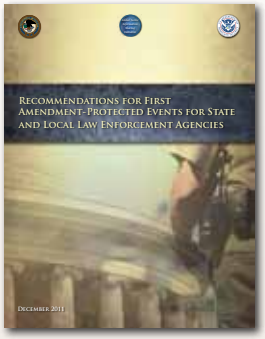
This awareness resource for justice executives is also an informational training tool. The flyer makes the case for privacy policy development and underscores the importance of promoting privacy protections within justice agencies. Included is information on basic privacy concepts; the intersection of privacy, security, and information quality; privacy risks; and steps to establish privacy protections through a privacy program cycle. This paper applies privacy principles to justice information sharing and makes recommendations on best practices. It is available online at www.it.ojp.gov/privacy.

7 Steps to a Privacy, Civil Rights, and Civil Liberties Policy

Designed for both justice executives and agency personnel, this document raises awareness and educates readers on the seven basic steps involved in the preparation for development of a privacy, civil rights, and civil liberties policy. Each step describes the practical tasks associated with preparing for, drafting, and implementing a privacy policy. Also featured is an overview of the core concepts that an agency should address in the written provisions of a privacy policy. It is available online at www.it.ojp.gov/privacy.

Resources (continued)

Recommendations for First Amendment-Protected Events for State and Local Law Enforcement



This resource provides guidance and recommendations to law enforcement agency personnel in understanding their roles and responsibilities in First Amendment-protected events. It is divided into three stages—Pre-Event, Operational, and Post-Event—with each stage identifying the recommended actions of law enforcement. The resource also provides an overview of how fusion centers can support law enforcement in its public safety mission in regards to these types of events. It is available online at http://it.ojp.gov/documents/First_Amendment_Guidance.pdf.

Role of State and Local Law Enforcement in First Amendment Events

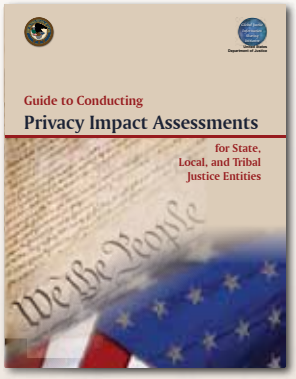
This pocket-sized reference card is designed for line officers who are responding to a First Amendment-protected event. It provides an overview of officers' roles and responsibilities and the rights of the participants at First Amendment-protected events. It is available online at http://it.ojp.gov/documents/First_Amendment_Reference_Card.pdf.

DHS/BJA Privacy and Civil Liberties Web Portal

Through a joint effort between BJA and DHS, this collaborative Web portal, accessible at www.it.ojp.gov/PrivacyLiberty, provides access to a wide range of resources and training materials available in the ISE that address privacy and civil liberties protections, including many of the Global-recommended products described within this overview. Although intended for fusion center use, these resources can easily be adapted by law enforcement, criminal justice, public safety, and homeland security communities nationwide.

Tools—Privacy Impact Assessment

Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities (PIA Guide)



Privacy policies emerge as a result of the analysis performed during a Privacy Impact Assessment (PIA) process. In this PIA guide, practitioners are provided with a framework with which to examine the privacy implications of their information systems and information sharing collaborations so they can design and implement privacy policies to address vulnerabilities identified through the assessment process. In addition to an overview of the PIA process, this guide contains a template that leads policy developers, such as privacy officers, through a series of appropriate PIA questions that evaluate the process by which personally identifiable information is collected, stored, protected, shared, and managed. The PIA questions are designed to reflect the same policy concepts as those recommended in the policy development tools listed here, further supporting privacy policy development. It is available online at www.it.ojp.gov/privacy.

Tools—Policy Development

Privacy, Civil Rights, and Civil Liberties Policy Development Template for State, Local, and Tribal Justice Entities (SLT Policy Development Template)

This SLT Policy Development Template was developed to assist SLT agencies in drafting privacy policies. The provisions suggested are intended to be incorporated into an agency's general operational policies and day-to-day operations. Each section represents a fundamental component of a comprehensive privacy policy that includes baseline provisions on information collection, information quality, collation and analysis, merging, access and disclosure, redress, security, retention and destruction, accountability and enforcement, and training. Sample language is included for each recommended provision, as well as a glossary and a listing of relevant federal law. It is available online at www.it.ojp.gov/privacy.

Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template (FC Privacy Template)

The FC Privacy Template was developed by DOJ in collaboration with DHS in the joint DHS/DOJ Fusion Process Technical Assistance Program. This template was designed specifically to assist fusion center personnel in developing privacy policies related to the information, intelligence, and suspicious activity report (SAR) information their centers gather, collect, receive, maintain, archive, access, disclose, and disseminate to center personnel, governmental agencies, Information Sharing Environment (ISE) participants, and other participating criminal justice and public safety agencies, as well as to private contractors and the general public. Provisions contained in this template help centers comply with requirements of the DHS Homeland Security Grant Program Guidance and the ISE Privacy Guidelines. It is available online at www.it.ojp.gov/privacy.

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations

This resource provides law enforcement and justice agencies with guidance and recommendations on issues to consider when developing a social media policy (or updating other relevant policies), focusing on access, use, storage, and dissemination of information obtained from social media sites for investigative and criminal intelligence purposes. The document includes recommended elements of the related policy, focusing on potential privacy, civil rights, and civil liberties implications. It is available online at https://it.ojp.gov/gist/132/Developing-a-Policy-on-the-Use-of-Social-Media-in-Intelligence-and-Investigative-Activities--Guidance-and-Recommendations-.

Resources (continued)

Tools—Policy Evaluation

Policy Review Checklist

The checklist is a companion piece to Global's SLT Policy Development Template and serves two purposes. First, it is a self-assessment tool to assist privacy officers in evaluating whether the provisions contained within their draft privacy policies have met the core concepts recommended in the Global SLT Policy Development Template. Second, it is a tool for performing the annual privacy policy review. The checklist is structured according to policy provision categories with section references that correlate with the Global SLT Policy Development Template. It is available online at www.it.ojp.gov/privacy.

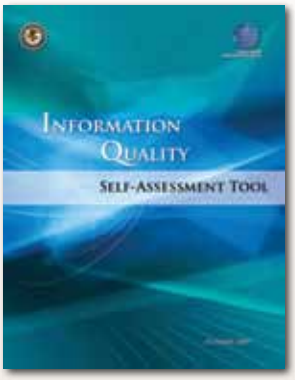
Tools—Analytic Product Evaluation

Checklist for the Development, Review, and Dissemination of Analytic Products and Resources

This resource is designed to be used as a checklist for personnel operating in an intelligence enterprise (including fusion centers and agency intelligence units), to ensure that privacy, civil rights, and civil liberties protections are upheld in the development and release of analytic and intelligence products. It is available online at https://it.ojp.gov/gist/133/Checklist-for-the-Development--Review--and-Dissemination-of-Analytic-Products-and-Resources

Tools—Information Quality Evaluation

Information Quality Self-Assessment Tool



Justice information of the highest quality is the cornerstone for sound entity decision making. Gathering and providing access to inaccurate information can be a public and personal injustice. Information quality (IQ) plays an extremely important role in the protection of privacy rights of individuals, since both concepts are inherently linked, influencing the appropriate treatment of personally identifiable information. Comprehensive privacy policies proactively address the quality of entity information. The purpose of this tool is to provide practitioners with guidance in evaluating the IQ of justice information. Structured as a self-administered worksheet, this tool will assist practitioners in identifying gaps in roles and responsibilities, policies and procedures, and information technology that beget IQ problems. The matrix of self-assessment questions can be tailored to meet the specific needs of each entity. This Global IQ resource and others are available online at www.it.ojp.gov/iq_resources.

Tools—Privacy Compliance Evaluation

Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise

This document assists agencies in determining whether they are in compliance with applicable privacy-related policies, procedures, rules, and guidelines. The document includes a suggested methodology for conducting the review of an agency's intelligence enterprise and identifies the high-liability areas of concern that should be included when performing the review. The document also contains a suggested list of questions to answer when conducting the compliance process but may not cover all laws, policies, and procedures that are applicable to a particular state or agency. It is available online at https://it.ojp.gov/gist/86/Privacy--Civil-Rights--and-Civil-Liberties-Compliance-Verification-for-the-Intelligence-Enterprise.

Training

The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety

This short training module was developed and supported by Global's Criminal Intelligence Coordinating Council as a training tool to educate viewers, particularly line officers during roll call, on the privacy and civil liberties issues they may confront in their everyday work. The training also addresses the liabilities associated with the failure to adhere to sound policy and practice. This short overview reviews and proactively emphasizes the role line officers have in the ongoing protection of citizens' and community members' privacy, civil rights, civil liberties, and other associated rights in the course of officers' daily activities and calls for service. It is available online at www.ncirc.gov/privacylineofficer/lineofficer.swf.

Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Online Training

Criminal intelligence plays a vital role in the safety and security of our country. The Code of Federal Regulations, Title 28, Part 23—Criminal Intelligence Systems Operating Policies (or 28 CFR Part 23) was issued to ensure the privacy and constitutional rights of individuals during the collection and exchange of criminal intelligence information. 28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. To facilitate greater understanding of 28 CFR Part 23, BJA developed the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) online training, which focuses on the requirements of 28 CFR Part 23 and includes topics such as compliance, privacy, inquiry, and dissemination requirements; storage requirements; and review-and-purge requirements. The training is available online at www.ncirc.gov/Training.aspx or www.ncirc.gov/28cfr/.

Resources (continued)

Criminal Intelligence Sharing: Protecting Privacy, Civil Rights, and Civil Liberties

This training is designed to present effective information sharing tools, examine the principles of 28 CFR Part 23, and address the importance of privacy, civil rights, and civil liberties in the context of information sharing. Its purpose is to enhance information sharing by clarifying the various rules and regulations to ensure that agencies are more confident as they collect and share information, particularly criminal intelligence information. In addition, technical assistance can be provided through on-site system reviews, policy reviews, and other specialized problem resolution. Training and technical assistance for this project are provided through funding from BJA. For more information on this training, visit www.iir.com/Justice_Training/privacy101/default.aspx.

Responding to First Amendment-Protected Events—The Role of State and Local Law Enforcement Officers

These training modules are designed to assist law enforcement personnel in understanding their roles and responsibilities as they prepare for and respond to a First Amendment-protected event; protect the privacy, civil rights, and civil liberties of persons and groups participating in a First Amendment-protected event; and reinforce fundamental concepts learned at law enforcement training academies and during in-service programs. These trainings are available online at www.ncirc.gov/Training_First_Amendment.aspx.

Online SAR Training for Law Enforcement and Hometown Security Partners

These online training deliveries support frontline officers and hometown security partners in understanding their roles and responsibilities regarding documented and verified behaviors and indicators which, when viewed in the totality of circumstances, may indicate terrorism-related criminal activity. Both the SAR Line Officer Training and the sector-specific SAR Hometown Security Partners Trainings discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens' privacy, civil rights, and civil liberties. SAR training modules are available for line officers and private sector security, fire/EMS, probation/parole/corrections, public safety telecommunications, emergency management, and maritime personnel. The modules are available online at http://nsi.ncirc.gov/training_online.aspx.

Additional Resources/End Notes

1. Most states have statutes that restrict the collection and dissemination of SSNs. Additionally, a recent case out of the Seventh Circuit (*Gonzalez v. Village of West Milwaukee*, 671 F.3d 649, C.A.7 [Wis.] 2012) applies Section 7 of the federal Privacy Act of 1974 to local governments. Section 7 prohibits local government agencies from denying an individual a right, a benefit, or a privilege because of the individual's refusal to disclose an SSN and requires the agency to inform the individual whether disclosure is mandatory or voluntary, the statutory or other basis for which it is requested, and what uses will be made of the number.
2. Health Insurance Portability and Accountability Act (HIPAA) of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191, www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.
3. Per 45 CFR Part 160 General Administrative Requirements, Subpart A, § 160.103, a covered entity is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a covered transaction (relating to health claim report, status, payment, etc.).
4. Per 45 CFR Part 164 § 164.512(k)(5), "HIPAA-covered entities are permitted to disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object for specialized government functions, such as to a correctional institution or other law enforcement official having lawful custody of an inmate or other individual when the PHI is about such inmate or individual and if the correctional institution or such law enforcement official represents that such protected health information is necessary" for the conditions stated in this regulation.
5. Code of Federal Regulations, Title 45 Public Welfare (45 CFR), § 164.530(a)(1), www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/xml/CFR-2011-title45-vol1-sec164-530.xml.
6. www.riss.net.
7. Nationwide SAR Initiative (NSI), http://nsi.ncirc.gov.
8. The NSI requires "each site to fully adopt the NSI privacy protection framework prior to participation in the NSI. To expedite privacy policy development and implementation, it is strongly recommended that the sites have access to the services of a trained privacy officer who is available to provide ongoing advice and assistance regarding privacy, civil rights, and civil liberties." *Final Report, Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Evaluation Environment*, p. 23, January 2010.
9. Nationwide SAR Initiative Privacy Fact Sheet, http://nsi.ncirc.gov/documents/SAR_Privacy_Fact_Sheet_2012.pdf.
10. Privacy, Civil Rights, and Civil Liberties Protection Framework, Information Sharing Environment (ISE), http://ise.gov/privacy-civil-rights-and-civil-liberties-protection-framework, and ISE Privacy Guidelines, http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf.
11. Privacy Program Cycle, Global Privacy Resources, Global Justice Information Sharing Initiative, U.S. Department of Justice, www.it.ojp.gov/privacy.
12. Information Sharing Environment (ISE), www.ise.gov.

Where to Locate These Resources

The recommended Global privacy resources featured within this guide and others are available online at www.it.ojp.gov/privacy. To request printed copies, send requests to GLOBAL@iir.com.

About the Global Advisory Committee

www.it.ojp.gov/global

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment.

GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts to help address critical justice information sharing issues for the benefit of practitioners in the field.

Acknowledgement

www.it.ojp.gov/privacy

BJA wishes to acknowledge the support of Global and the Global Privacy and Information Quality Working Group (GPIQWG) in the development of this resource. For more information on BJA's Global privacy resources, refer to www.it.ojp.gov/privacy.

This project was supported by Grant No. 2009-DB-BX-K105 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative and the U.S. Department of Homeland Security. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice or the U.S. Department of Homeland Security.

Issued 07/2013
Revised 06/2014