

# Guideline 8

Develop, publish, and adhere to a privacy and civil liberties policy.

## Privacy and Civil Liberties

### Justification

The *National Criminal Intelligence Sharing Plan* (NCISP) stresses the need to ensure that constitutional rights, civil liberties, civil rights, and privacy are protected throughout the intelligence process. In order to balance law enforcement's ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be in place.

### Process

Privacy and civil liberties protection should be considered in the planning stages of a fusion center. As systems are designed, analysis should be made and protections should be developed for personally identifiable information to ensure its protection.

DOJ's Global Justice Information Sharing Initiative (Global) has developed the *Privacy Policy Development Guide* and the *Privacy and Civil Rights Policy Template for Justice Information Systems* to aid justice practitioners with developing or revising an agency's privacy policy. Furthermore, the guide assists agencies in articulating privacy obligations in a manner that protects the justice agency, the individual, and the public and makes it easier to do what is necessary—share critical justice information. These documents are contained as attachments to the guidelines.

The Global documents utilize, and any fusion center should consider, the Fair Information Practices which are the accepted baseline for privacy protection worldwide. The following is a summary of the Fair Information Practices:

1. **Collection limitation principle.** There should be limits to the collection of personal data, and any data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data quality principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date.

3. **Purpose specification principle.** The purposes for which personal data is collected should be specified no later than at the time of data collection. Its subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use limitation principle.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with Principle 3 except (a) with the consent of the data subject or (b) by the authority of law.
5. **Security safeguards principle.** Personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, misuse, modification, or disclosure.
6. **Openness principle.** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual participation principle.** An individual should have the right to (a) obtain confirmation of whether or not the data controller has data relating to him; (b) have the data related to him within a reasonable time, cost, and manner and in a form that is readily intelligible to him; (c) be given an explanation if a request made under (a) and (b) is denied and be able to challenge such denial; and (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
8. **Accountability principle.** A data controller should be accountable for complying with measures that give effect to the principles stated above.

The NCISP recommends that privacy policies should:

- ✓ Eliminate unnecessary discretion in decision making, guide the necessary discretion, and continually audit the process to ensure conformance with the policy.
- ✓ Ensure legitimacy—when an agency is developing a new policy or reviewing existing ones, interested parties and competing viewpoints should be represented.

- ✓ Clearly define the parameters of the policy.
- ✓ Acknowledge and address important issues that currently are not included in some existing criminal intelligence policies.
- ✓ Identify the decision points within the intelligence process and provide appropriate guidance and structure for each.

## Issues for Consideration

Issues to consider when drafting a privacy policy include:

- Adding introductory language that clearly states the privacy practices of the center.
- Describing the information collected and how information is stored.
- Establishing a common lexicon of terms for dealing with role-based access.
- Defining and publishing how the information will be used.
- Drafting a clear, prominent, and understandable policy. Avoid communicating in complicated or technical ways.
- Displaying the privacy policy for both center personnel and customers.
- Ensuring that all other policies and internal controls are consistent with the privacy policy.
- Establishing a business practice of notifying government agencies of suspected inaccurate data.
- Adhering to applicable state and federal constitutional and statutory civil rights provisions.
- Partnering with training centers on privacy protection requirements and conducting periodic privacy security audits.
- Consulting with a privacy committee (see Guideline 3) to ensure that citizens' privacy and civil rights are protected.
- When utilizing commercially available databases, ensuring the usage is for official business and the information obtained is not commingled with private sector data. To prevent public records disclosure, risk and vulnerability assessments should not be stored with publicly available data.
- Determining if there are security breach notification laws within the jurisdiction and following those laws, if applicable.

## Adhering to a Privacy Policy

There are a number of mechanisms that centers can develop or establish that will assist them in adhering to their privacy policy. Some of these include:<sup>49</sup>

- Establish a privacy oversight committee (see Guideline 3) or appoint a privacy officer.
- Develop or update privacy training and orientation for all employees.

- Develop a mechanism for ongoing information privacy awareness.
- Establish a process for tracking and handling privacy complaints or concerns.
- Develop a consistent sanction policy for failure to comply with the privacy policy for all individuals in the organization.
- Recognize the overlap in privacy activities and security activities, and coordinate both within the organization.
- Ensure all center personnel are adequately trained in using the privacy policy.
- Seek legal counsel.



## Available Resources on Fusion Center CD

- Audit Checklist (LEIU), [www.it.ojp.gov/documents/LEIU\\_audit\\_checklist.pdf](http://www.it.ojp.gov/documents/LEIU_audit_checklist.pdf)
- Global's *Privacy and Information Quality Policy Development for the Justice Decision Maker*, [http://it.ojp.gov/documents/200411\\_global\\_privacy\\_document.pdf](http://it.ojp.gov/documents/200411_global_privacy_document.pdf)
- National Criminal Justice Association—*Justice Information Privacy Guideline*, [www.ncja.org/pdf/privacyguideline.pdf](http://www.ncja.org/pdf/privacyguideline.pdf)
- *Privacy and Civil Rights Policy Templates for Justice Information Systems*
- Privacy Policy Sample Template
- *Privacy Policy Development Guide*

<sup>49</sup> Beth Hjort, "A HIPAA Privacy Checklist (AHIMA Practice Brief)," *Journal of AHIMA* 72, Number 6, 64A-C, 2001.