The Fair Information Practice Principles (FIPPs)
In the Information Sharing Environment (ISE)

The Fair Information Practice Principles (FIPPs) are a set of internationally recognized principles that inform information privacy policies both within government and the private sector.

Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated in data privacy laws, policies and governance documents around the world. For example, the FIPPs are:

- at the core of the Privacy Act of 1974, which applies these principles to U.S. Federal agencies;[1]
- influential internationally, especially as articulated by the Organization for Economic Cooperation and Development;
- mirrored in many states' laws and in fusion centers' privacy policies; and
- used by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used by the Department of Homeland Security (DHS).[2]

Purpose Specification - Agencies should specifically articulate the authority that permits the collection of Personally Identifiable Information (PII). The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes *compatible* with the original collection purpose).

Implementing the Purpose Specification Principle in the ISE – Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

- Ensure that a valid lawful purpose exists and is documented for all collection of PII;
- Include the source and authority for the data so that access restrictions can be applied;
- Upon receipt of data containing PII from 3rd parties, if possible identify the purpose for which it was collected initially and limit agency use to only those uses compatible with the original purpose supporting collection;
- Ensure that metadata or other tags are associated with the data as it is shared;
- Institute a two-person review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

Data Quality/Integrity - PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up-to-date.

Implementing the Data Quality/Integrity Principle in the ISE – One important way to minimize potential downstream privacy and civil liberties concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

- Properly labeling PII;

---

[1] 5 U.S.C. § 552a
[2] 6 U.S.C..§ 142

- Determining a policy for safeguarding PII if there are "mixed" databases (those databases with personal information on U.S. persons and others, regardless of nationality);
- Instituting a source verification procedure to ensure reporting is based only on authorized data;
- Reconciling and updating PII whenever new relevant information is collected;
- Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared; and
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

Collection Limitation/Data Minimization - PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose.

Implementing the Collection Limitation/Data Minimization Principle in the ISE –Collection limitation may be implemented by:

- Designing a data storage system to pull data for review and then, if appropriate, automatically purge data after the specified retention period has been reached;
- Limiting data field elements to only those that are relevant;
- Ensuring that all distributed reports and products contain only that personal information that is relevant and necessary (nothing extraneous or superfluous)
- Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

Use Limitation - PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

Implementing the Use Limitation Principle in the ISE – While sharing information broadly is the purpose of the ISE, it should be tempered by adherence to key principles such as "authorized access." Use limitation may be implemented by:

- Limiting users of data to those with credential-based access;
- Requiring that justifications be entered and logs maintained for all queries with sensitive PII, and that an internal review process of those logs takes place at specified intervals;
- Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) PII is relevant and necessary, and (b) that the recipient is authorized to receive the information in the performance of an authorized activity;
- Prior to sharing information verify that partners have a lawful purpose for requesting information; and
- Creating multiple use-based distribution lists and restrict distribution to those authorized to receive the information.

Security/Safeguards – Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

Implementing the Security/Safeguards Principle in the ISE – This principle can be implemented by:

- Maintaining up-to-date technology for network security;
- Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable;
- Ensuring that physical security measures are in place, such as requiring an identification card, credentials and/or passcode for data access, disabling computers' USB ports, and implementing firewalls to prevent access to commercial email or messaging services;

- Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period;
- Ensuring that data system purge protocols include complete record deletion on all backup systems;
- Transitioning older repositories into more modern systems to improve access controls;
- Masking data so that it is viewable only to authorized users;
- Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals; and
- Requiring authorized users to sign non-disclosure agreements.

Accountability/Audit – Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

Implementing the Accountability/Audit Principle in the ISE – Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

- Ensuring that, upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents and/or the Constitution;
- Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII;
- Tailoring training to specific job functions, database access or data source/storage requirements;
- Conducting regular audits of all systems in which records are kept to ensure compliance with the P/CRCL policies and all legal requirements;
- Following a privacy incident handling procedure for any data breaches or policy violations;
- Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances; and
- Developing targeted and consistent corrective actions whenever non-compliance is found.

Openness/Transparency – To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints.

Implementing the Openness/Transparency Principle in the ISE – Agencies can implement the Openness/Transparency principle by:

- Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results;
- Publishing the P/CRCL policy and redress procedures;
- Meeting with community groups through initiatives (e.g., *Building Communities of Trust)* or through other opportunities to explain the agency's mission and P/CRCL protections;
- Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public; and
- Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affects PII thereby demonstrating that privacy, civil rights, and civil liberties issues have been considered and addressed.

Individual Participation - To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies

should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

Implementing the Individual Participation Principle in the ISE-- To the extent appropriate, agencies can implement the Individual Participant principle by:

- Collecting information directly from the individual, to the extent possible and practical;
- Providing the individual with the ability to find out whether a project maintains a record relating to him or her, and if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial; and
- Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.