

Fair Information Practice Principles (FIPPs)

Overview

The FIPPs are a collection of widely accepted principles that agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy. The FIPPs are not requirements; rather, they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements.

Rooted in a 1973 Federal Government report from the Department of Health, Education, and Welfare Advisory Committee, "Records, Computers and the Rights of Citizens," the Fair Information Practice Principles (FIPPs) have informed Federal statute and the laws of many U.S. states and foreign nations, and have been incorporated in the policies of many organizations around the world. While the precise expression of the FIPPs has varied over time and in different contexts, they have always retained a consistent set of core principles that are broadly relevant to agencies' information management practices. To learn more, watch the Federal Privacy Council's [FIPPs video](#).

FIPPs Icons Toolkit

Guidelines for Use

- Do not add, remove, skew, or alter any elements within the icon, including the font. The name of each FIPP should accompany the icon.
- Do not change or create new color combinations.
- Do not place icons on top of photographs without proper color contrast.
- Do not place color icons on vibrant backgrounds.

Download the Privacy Icons Toolkit

In 2022, the Federal Privacy Council developed icons to represent each of the 9 FIPPs. Agencies may download these icons below and may use them in accordance with the guidance contained in the [FIPPs Icons Toolkit](#).

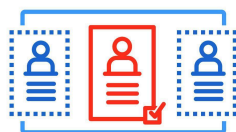
- [Color Icons](#)
- [Black & White Icons](#)
- [Reverse Color Icons](#)

 Please note that these icons are available for download via Connect. You must have permissions to view the [Federal Privacy Council page](#) in order to access these icons. If you are unable to access the Icons Toolkit on Connect, please contact privacy.council@gsa.gov.

Overview of Icons

They are as follows:

ACCESS AND AMENDMENT Access and Amendment. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.	ACCOUNTABILITY Accountability. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.	AUTHORITY Authority. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.
MINIMIZATION Minimization. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.	QUALITY AND INTEGRITY Quality and Integrity. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.	INDIVIDUAL PARTICIPATION Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.



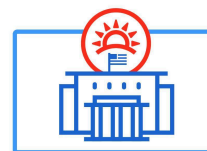
PURPOSE SPECIFICATION AND USE LIMITATION

Purpose Specification and Use Limitation. Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.



SECURITY

Security. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.



TRANSPARENCY

Transparency. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.