The Privacy Act and the NIH Intramural Research Community

Office of Human Subjects Research Protections (OHSRP) Education Series – March 6, 2025

Training Goals

- Familiarize the NIH intramural research community—not just the privacy professionals—with the basic requirements of the Privacy Act.
- Ensure the NIH intramural research community knows how to identify a potential Privacy Act issue and where to go for assistance.
- Provide links to relevant information privacy resources, and the list of NIH Privacy Act Contacts to consult for assistance.

Agenda

- Section 1: Overview and Scope of the Privacy Act
- Section 2: Obligations of Federal Agencies
- Section 3: Rights of Individuals
- Section 4: Special Topics
- Section 5: Privacy Act Contacts & Resources

Policy Objectives of the Privacy Act

Restrict disclosure of information about individuals maintained by agencies

Grant individuals increased right of access and right of amendment of records

Based on a “code of fair information practices” which regulates the collection, maintenance, use and disclosure of identifiable personal data

Grant private rights of action against agencies for violations (i.e., the ability to sue and get redress)

Structure of the Privacy Act of 1974

Imposes **obligations** on federal agencies & pertinent contractors

Grants **rights** to individuals about whom records are maintained

Is not a source of specific security requirements

Is based on the Code of Fair Information Practice

Code of Fair Information Practice (1973)

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for a person to find out what information about the person is in a record and how it is used.
- There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
- There must be a way for a person to correct or amend a record of identifiable information about the person.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Proposed by HEW Advisory Committee on Automated Data Systems in 1973 (full report)

Fair Information Practice Principles (FIPPs)

Principle	Agencies should:
Access and Amendment	Enable individuals to access, correct, or amend their PII as appropriate.
Accountability	Monitor, audit, and document compliance with privacy principles and requirements. Train employees and contractors on their responsibilities.
Authority	Only collect, use, maintain, or disclose PII for which there is legal authority.
Minimization	Only collect, use, maintain, and disclose PII that is relevant and necessary to accomplish a legally authorized purpose. Only maintain PII for as long as is necessary to accomplish the purpose.
Quality and Integrity	Ensure accurate, relevant, timely and complete PII to ensure fairness to individuals.
Individual Participation	Seek consent for the collection, use, and disclosure of PII. Address privacy complaints and inquiries.
Purpose Specification and Use Limitation	Identify in advance the specific purpose for which PII is collected. Tell individuals from whom information is collected what that purpose is (see also Transparency) Only collect, use, disclose PII for that purpose, compatible purposes, or other legally authorized.
Security	Protect PII commensurate with the potential risk of harm.
Transparency	Be transparent about information policies and practices with respect to PII. Provide clear and accessible notice regarding collection, use, maintenance, and disclosure of PII.

Scope & Important Definitions

Individual	• "natural" person (not an organization or corporation) • living person (deceased people do not get Privacy Act rights) • US citizen or permanent resident alien
Record	• Information about an *Individual* • Connected to a personal identifier (e.g., name, account number, fingerprint) • Maintained by a federal agency
System of Records	• Collection of *records* • Retrieved by the personal identifier

Obligations of Federal Agencies

- Collect only relevant and necessary records
  - Must be authorized by a federal statute or Executive Order
- Collect information “to the greatest extent practicable” from the subject individual
- Give both general and individual notice
- Maintain records that are accurate, relevant, timely, and complete
  - Enough to ensure fairness to individuals in making determinations about them
  - Check the records to ensure before making a disclosure
- Establish rules and training for employees and contractors handling records
- Establish appropriate security

System of Records Notice (SORN)

SORN = “constructive” notice (no secret recordkeeping systems)

Describes existence and character of the records

- Who is covered?
- What records or data elements are being kept?
- What is the purpose of maintaining this collection of records?
- What disclosures can be made without consent, in addition to statutory disclosures? (“routine uses”)
- How can one find out about access to or amendment of the records?
- Are the records exempt from certain Privacy Act requirements?

System of Records Notice (SORN)

- May cover one or more functionally similar sets of Privacy Act records, IF all of the following are the same:
  - purpose
  - covered individuals
  - disclosures that apply
  - exemptions that apply, if any

- Uses standard format and headings prescribed by the Office of the Federal Register & Office of Management and Budget (OMB)

- After advance review by OMB & Congress, is published in *Federal Register* and posted on Internet, by the agency maintaining records.

A Note about SORNs v. PIAs

System of Records Notice (SORN)

- Established by Privacy Act of 1974
- Covers all similar records, could be multiple paper collections, IT systems, both
- Subset of an IT system might be Privacy Act records
- Contractors could be running a SOR
- Reviewed by OMB, Congress and published in *Federal Register*
- **Updated only for significant changes**

Privacy Impact Assessment (PIA)

- Established by E-Government Act of 2002
- Assessment of privacy risks when IT systems and electronic information collections collect, disseminate, maintain, or dispose of PII about members of the public
- Conducted before developing/procuring IT systems or initiating projects
- Posted on Internet (e.g., HHS website)
- **Updated for major changes, and every 3 years even if no significant change**

Privacy Act Statement

- Notice to a particular individual when collecting information
- When information will end up in a Privacy Act system of records
- Must be given at point of collection to enable informed decisions
  - whether paper, electronic, or by telephone

Note that HHS policy *may* require privacy notices more broadly than just what is required by the Privacy Act. (e.g., when collecting info from an individual not in SOR.*)

*see *HHS Information Systems Security and Privacy Policy (IS2P) (Nov. 2021), implementing NIST SP 800-53 (Rev 5)*

Privacy Act Statement

The Privacy Act requires the following elements:

- Federal statute or EO that authorizes collection
- Whether responding is mandatory or voluntary
  - Could be required to receive a benefit
- Principal purpose(s)
- Routine use disclosures as published in applicable SORN(s)
- Effect on the individual of *not* providing all or part of the requested information.

Addt'l content required by OMB Circular A-108

- Citation to the relevant SORN(s)
- If practicable, a link to the relevant SORN(s).

Disclosure Prohibition and 12 Exceptions

5 USC § 552a(b): No disclosure w/out prior written consent, UNLESS:

(b)(1) To agency officers/employees with need to know.

(b)(2) When required by FOIA [not discretionary]

- weigh the privacy interest v. the public interest

(b)(3) Pursuant to a routine use

- Disclosure outside of HHS
- Purpose is compatible with the purpose of the collection
- published in the SORN (30 days notice required)

(b)(4) To the Bureau of the Census for activities under Title XIII

Disclosure Prohibition and 12 Exceptions

(b)(5) Statistical Research or reporting

- w/o identifiers
- recipient has given advance written assurance for solely statistical use

(b)(6) National Archives for permanently valuable records

(b)(7) *In response to* a law enforcement request

(b)(8) Compelling health or safety issue

- notice sent to last known address

(b)(9) House or Senate, or Cong. Committee when requested by chair

- not an individual Member of Congress

Disclosure Prohibition and 12 Exceptions

(b)(10) To the Comptroller General or GAO for their duties

(b)(11) To the Congressional Budget Office for its duties

(b)(12) Pursuant to the order of a court of competent jurisdiction

- court-issued, not clerk-issued
- federal court, not state or tribal court
- Not discretionary – unless you want to go to jail

(b)(13) To a consumer reporting agency

- for debt management/collection purpose
- if notice of such disclosure was published in the SORN.

<u>If no exception fits</u>, publish routine use or get written consent

Criminal Penalties

- Federal Employees
  - Willful and intentional disclosure of Privacy Act records where not permitted
  - Willfully maintaining a system of records without SORN (no secret recordkeeping!)

- Any person
    - Knowingly and willfully requesting or obtaining Privacy Act records under false pretenses

- Misdemeanor (up to one year in prison)
- Fine up to $5000

Rights of Individuals

- Examine and retain a copy of their own records
- Amendment
- Accounting of Disclosures
- Appeals
- Obtain notices
- Records that are fair (accurate, relevant, timely, complete)
- Redress wrongs (you can sue)

Privacy Act Requests

Right to examine and obtain a copy of your own records

- Notification: The right to ask whether a particular system of records contains a record about you
- Access: The right to request access to a Privacy Act record about you
- Amendment: The right to request correction of factual (not judgmental/qualitative) information in a Privacy Act record about you

Agency may be exempt via a rulemaking from having to respond

- Examples: law enforcement investigations
- agency may still consider a request, even if exempt

Accounting of Disclosures

- List of disclosures made by the agency of your record
  - Date, nature, and purpose of each disclosure
  - Name and address of the person to whom disclosure made

- Agency must use accounting to notify recipients to update
  - Amendments, notices of dispute

- Accounting must be kept 5 yrs or life of record, whichever is longer
  - Just be able to construct the accounting when requested

    - Accounting not required to be *maintained*:
      - disclosures to agency employees with valid need to know (b)(1)
      - disclosures required by FOIA (b)(2)

    - Accounting not required to be *released*:
      - disclosures responsive to law enforcement requests (b)(7)

Administrative Remedies

Denial of access request

appeal remedy is consistent with HHS FOIA regs

90 days to appeal (write a letter requesting reconsideration)

appeal is decided by HHS Appeal Official

Denial of amendment request

reviewed by NIH Appeal Authority

agency has 30 days to respond

if still denied, individual may file concise statement of disagreement to be included with the record

Denial of accounting request

no administrative remedy in current HHS Privacy Act regulations

Redress/Civil Remedies

When can an individual sue? When an agency:

- denies a request for access, amendment, accounting
- fails to maintain records that are accurate, timely, relevant, and complete enough to ensure fairness
- fails to comply with any other requirement that has an adverse effect

What can an individual get from the court?

- court order to force compliance
- actual/monetary damages if the violation was intentional or willful
- reasonable attorney's fees & court costs, if individual substantially prevails

Lawsuit must be filed within 2 years after

- cause of action arises (e.g., exhaustion of administrative remedies), or
- discovery of violation

Special Topics: Best Practices

Privacy Act is silent about further uses and redisclosures by recipients.

- Consider whether you could do more to protect records in litigation:
  - Consult with OGC
  - Seek a protective order in response to a court order;
  - Limit use of the records to the particular lawsuit; and
  - Ensure the records are kept under seal by the court.

- Consider a Data Use Agreement with recipient or a transmittal document:
  - Limit use of the records to your specific purpose;
  - Prohibit redisclosure for other purposes unless authorized in writing by HHS;
  - Spell out especially harmful uses; and
  - Cease disclosure if recipient uses or rediscloses for an unauthorized purpose.

Special Topics: Contractors

- PA requirements apply if the contract is for operation of a system of records to accomplish an agency function

- For purposes of criminal penalties, subsection (m) contractors are considered employees of the agency

- Contract must include clauses binding contractor to provisions of the Act
  - These can be found in the FAR, HHSAR, and agency guidance

- *Talk with your Privacy Act Contact and your procurement people*

Special Topics: First Amendment Rights

The Privacy Act prohibits an agency from collecting information about how individuals exercise their First Amendment rights

- Applies to all information, even if not contained in a SOR
- Prevents compiling of gov't files on people who express views, practice religion, assemble, seek redress that could be used to harass them
  - Disfavored minority groups, protesters, political opponents, misinformation spreaders
  - E.g., Hoover's misuse of FBI resources to investigate MLK, John Lennon, etc.

- Exceptions
  - expressly authorized by statute
  - expressly authorized by the individual about whom the record is maintained
  - pertinent to and within the scope of an "authorized law enforcement activity"
    - *Some courts hold this means "ongoing" (that records can't be maintained after investigation closes)*

Privacy Act Resources

The Privacy Act of 1974, as amended to present: 5 U.S.C. § 552a

OMB Circular A-108 (Dec. 2016) – PDF (basic Privacy Act guidance)

DOJ Privacy Act Overview (explains provisions and discusses specific cases in legal context)

Federal Privacy Council (FPC) resources: https://fpc.gov

HHS Systems of Records Notices HHS SORNs

HHS Privacy Impact Assessments HHS PIAs

HHS Privacy Act regulations:

- Most of HHS: 45 CFR Part 5b (outdated; to be revised and moved to 45 CFR Part 6)
- FDA: 21 CFR Part 21 (to be replaced by the revised HHS Privacy Act regs)

Key HHS Offices and Roles

Office of the Assist Secretary for Public Affairs (ASPA):

- Has HHS-wide **Privacy Act** implementation responsibility.
- HHS Privacy Act Officer is in ASPA.

Office of the Assistant Secretary for Administration (ASA):

- Has HHS-wide **privacy compliance** responsibility.
- Senior Agency Official for Privacy (SAOP) is in ASA/OCIO.

Office of the Assistant Secretary for Planning and Evaluation (ASPE):

- Has HHS-wide **privacy policy** responsibility.
- Senior Advisor, Privacy Policy is in ASPE.

OpDivs (NIH, FDA, CDC, etc.):

- Each OpDiv has a Privacy Act Contact and Senior Official for Privacy (SOP).

Key NIH Offices and Roles

NIH OD Privacy Office:

- Advises NIH-wide on **privacy policy** & **privacy compliance** requirements.
- NIH Privacy Act Officer (i.e., Privacy Act Contact) is in the Privacy Policy Branch, Division of Compliance Management, OMA/OM/OD.
- NIH Senior Official for Privacy is in the Privacy Policy Branch, Division of Compliance Management, OMA/OM/OD.

NIH Institutes, Centers, & Offices (ICOs):

- Has ICO-wide **privacy policy** and **privacy compliance** implementation responsibility.
- ICO Privacy Coordinator is designated at the ICO level.

Other Privacy Points of Contact

To reach the Department-level Privacy Program, please contact the Office of Privacy and Information Management (PIM) at PrivacyProgramMailbox@hhs.gov.

To reach the NIH Privacy Program and NIH Senior Official for Privacy (SOP), please see: https://www.hhs.gov/web/policies-and-standards/hhs-web-policies/privacy/index.html#HHS-Privacy-Officials.

Important Privacy Act Takeaways!

Consult your ICO Privacy Coordinator to:

- Determine if the Act applies to information you're handling.
- Find out which SORN applies
- Determine Privacy Act applicability prior to procuring products or services to collect/process PII on behalf of the government
- Determine if an information sharing agreement/contractual arrangement is needed to govern downstream uses of data