US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/10/2016

OPDIV:

OS

Name:

FOIAXpress

PIA Unique Identifier:

P-4424762-293857

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Initiation

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The purpose of FOIAXpress is to enable ASPA's FOIA/Privacy Acts Division (the OS FOIA Office) to more efficiently receive, track, and respond to records requests and appeals made under the Freedom of Information Act (FOIA) and Privacy Act (PA), securely store, process (redact), and transmit responsive records, and generate associated correspondence and internal and public reports in a manner that complies with statutory and Department of Justice requirements and best practices.

This is an all-inclusive system; it replaces a prior system that provided limited tracking and reporting capability and that did not provide storage, form documents, online features, and processing tools.

Describe the type of information the system will collect, maintain (store), or share.

The system will collect:
- FOIA/PA requests and appeals received in the OS FOIA Office by mail, phone, or fax, or online through the system's Public Access Link (PAL), from individual and entity requesters or by referral

from another FOIA office (containing requester or appellant name and contact information (mailing address, email address and/or telephone number) and a description of the records requested and issues raised on appeal);
- Responses to requests and appeals (containing requester or appellant name and mailing address or email address, a summary of the request history, the number of pages of responsive records located, released, and pages or portions withheld, an explanation of the exemptions applied to the withheld portions, the agency's decision on any appeal issues, and a notice of appeal rights);
- Intra- and inter-agency communications about requests (containing contact information for agency personnel and the requester/appellant and any information conveyed, pertaining to issues such as which offices could have responsive records, search or processing status, types and quantities of records located, reasons for delays, and estimated time-frames);
- Clean, marked, and redacted copies of responsive records processed for release (which could be any agency record, on any topic, containing any type of PII, depending on the request);
- Case tracking information (containing requester/appellant name, case tracking number, and processing stages such as date request received, date response due, number of days overdue, whether the response deadline is tolled (stopped), date records received, date response letter submitted for signature, date response provided, FOIA Analyst assigned to request);
- Form letters and report templates (these do not contain PII);
- Fee-related records (containing fee estimates and discussions or decisions about fees and fee waiver/reduction requests);
- Statistical and narrative reports (these do not contain PII);
- Internal productivity reports (these might include requester names, descriptions of records requested, and status information that indicates something about a requester); and
- records used to administer users' access to the system (containing user name, office/role, password, email address, and for HHS employees and direct contractors, Personal Identity Verification (PIV) card number).

Information from the system will be shared as follows:
1) For the purpose of processing requests and appeals, relevant information will be shared with:
- Agency personnel who assist in routing requests, locating responsive agency records, communicating with requesters, reviewing and processing responsive records, and preparing, approving, and signing the response letters;
- Other federal agencies and business submitters that may have an interest in responsive records;
- Any direct contractors assisting the OS FOIA Office to process requests;
- Requesters/Appellants; and
- The Department of Justice if necessary to resolve a FOIA policy or legal issue.
2) In the event of litigation, information would be shared with:
- The Department of Justice, courts, and opposing parties.
3) In the event of a mediation or review of HHS' FOIA Program, information would be shared with the Office of Government Information Services (OGIS) within the National Archives and Records Administration (NARA).
4) For the purpose of collecting any fees charged to requesters, fee-related information would be shared with HHS' financial management system.
5) For FOIA program reporting purposes, statistical (non-PII) information would be shared in internal management reports and in public reports.
6) To trouble-shoot system issues, information would be shared with or would be available to the system contractor and/or HHS IT personnel or direct contractors.
7) To administer user access privileges, user information would be shared with system administrators.
8) In the event of a data security incident, relevant informatio

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

FOIAXpress is an all-inclusive system that provides a FOIA Office with all tracking, storage, processing, communication, management, and reporting tools required to administer its FOIA program in accordance with statutory and Department of Justice requirements and best practices.

The system includes a Public Access Link (PAL) which is an online portal that allows any member of the public to register to create an account that he/she can use to submit requests online, receive limited status information online, and receive responses and responsive records online. To create a PAL account, the user enters his or her name, an email address, selects a requester category (commercial, educational, public, news media, nonprofit), and enters a user name, a hint question and a hint answer. PAL will notify a requester via email when information is available within the PAL portion of the system for the requester to access by logging into his or her PAL account. A registered PAL user will have access to only the PAL portion of the system, and only to information he/she submits in PAL or that the system delivers to his/her PAL account.

The information collected in FOIAXpress will be received directly from registered PAL users (members of the public) who submit FOIA requests and communications to HHS online; or will be received from a requester, or from an HHS office, or from another agency via mail, email, fax, disk, or from an HHS user's workstation drive and will then be uploaded to FOIAXpress by an HHS user; or will be created or entered in FOIAXpress by an HHS user.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Photographic Identifiers

Driver's License Number

Biometric Identifiers

Mother's Maiden Name

Vehicle Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Financial Accounts Info

Certificates

Legal Documents

Education Records

Device Identifiers

Military Status

Employment Status

Foreign Activities

Passport Number

Taxpayer ID

any PII in records considered to be agency records under FOIA

HHS user credentials

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

Patients

members of the public who are not citizens;
entities that are not U.S. Dept of Health and Human Services (HHS) business partners or vendors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purposes for which PII is used are to document and analyze requests received from individual requesters or that seek records about individuals, locate responsive records about individuals, verify the identity of individual requesters, contact requesters, locate cases in the system (e.g., to manage cases or provide status information to requesters), process responsive records containing PII, maintain clean, marked and redacted versions of the processed records, and document responses to requests, including fee issues.

Describe the secondary uses for which the PII will be used.

Secondary uses of the PII are to identify requests from the same requester or that seek records about the same individual(s), to prepare internal productivity and status reports, and to use as examples for training purposes.

Describe the function of the SSN.

SSN may be contained in some of the requests (even though we will discourage its inclusion) and in some of the pre-existing agency records processed for release under FOIA using the system.
SSN is very seldom needed because other information almost always exists that can serve the same functions. The functions would be: to verify the requester's identity, locate responsive records, or distinguish between records about individuals with the same name and associate records that are under different names but are about the same individual--but only when no other information will suffice as an alternative to using SSN.

Cite the legal authority to use the SSN.

5 U.S.C. 552 (FOIA) and 5 U.S.C. 552a (Privacy Act), which impliedly permit or require use of enumerators or other identifying information as necessary to provide individual requesters with access to their records while avoiding inadvertently releasing records to an individual requester that are about a different individual; see also Executive Order (E.O.) 9397 as amended by E.O.13478.

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. 552 (FOIA) and 5 U.S.C. 552a (the Privacy Act).
These are the correct legal authorities, because all requests for agency records are processed under FOIA, except to the extent they are first-party requests for records from a Privacy Act system that are fully granted under the Privacy Act alone. First-party requests for Privacy Act records that are not fully granted under the Privacy Act are processed under both the Privacy Act and FOIA.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Other Federal Entities

Other

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Other

Identify the OMB information collection approval number and expiration date

N/A. The online request mechanism will not constitute an information collection under the Paperwork Reduction Act.
It will state that a requester may submit a request using that online method or in any manner that conforms to HHS' FOIA regulations, and will enable the requester to provide only his/her name, contact information, and a description of the records he/she is requesting.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

To route and process requests, records and report data containing PII, verify identity of requesters, and locate records pertaining to particular individuals.

Other Federal Agencies

To effect consultations and referrals involving individual requesters and/or requested records containing PII.

State or Local Agencies

To ascertain facts (such as the existence of a consultant relationship with a state or local agency) or potential harms (such as to federal deliberative processes) affecting whether a FOIA exemption applies to information involving the state or local agency.

Private Sector

To comply with the submitter notice process with respect to financial or commercial records containing PII - this process shares with the submitter the records that the submitter originally provided to HHS, but may also share the identity of the requester

Describe any agreements in place that authorizes the information sharing or disclosure.

No agreements authorize information sharing. Dept of Justice (DOJ) guidance governs consultations and referrals with other agencies. The White House requires FOIA offices to consult with it on records implicating White House equities. Executive Order 12,600 governs the submitter notice process.

Describe the procedures for accounting for disclosures.

N/A (responses to FOIA and PA requests are exempt from this requirement per 5 USC 552a (c)(1).)

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Requesters using the Public Access Link (PAL) to submit a request will see a Privacy Act Statement at the point of collection.

Anyone visiting the main HHS FOIA website (home page) will see a Privacy Act Statement and a link to System of Records Notice (SORN) 09-90-0058 Tracking Records and Case Files for FOIA and Privacy Act Requests and Appeals, notifying individuals that, if they submit a FOIA/PA request to HHS or if existing agency records about them are processed by HHS in responding to a FOIA request, personally identifiable information about them will be included in FOIA/PA tracking records and case files, which may be maintained electronically and/or in hard copy, and that they should refer to SORN 09-90-0058 for descriptions of the purposes for which the records may be used by HHS and the "routine use" purposes for which the records may be disclosed to parties outside HHS. This notice will apply to requests at the point of collection and to pre-existing records after-the fact (post-collection).

HHS offices whose records are processed by the OS FOIA Office may also provided notice to individuals--at the time of collection--of the possible inclusion of their information in a FOIA/PA system. For example, the OS FOIA Office processes FOIA/PA requests seeking Office for Civil Rights (OCR) complaint investigation records from OCR's Program Information Management System (PIMS) 09-90-0052, and the OCR complaint form notifies complainants that the complaint and all investigation records are agency records subject to FOIA.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

An individual requester can choose which contact information to provide to the FOIA office and which method to use to submit a request (e.g., need not use the online method). A third-party requester can make a request anonymously through a nominee. A first-party requester can limit the type, number, date range, subject matter, etc., of records requested about himself/herself, and need not provide SSN or other identification information if other information is sufficient to locate the requested records and verify the requester's identity.

An individual whose PII is in records responsive to a FOIA request has no option to object to the inclusion of the records in the system.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Major changes to the system would be published in a revised System of Records Notice (SORN) for Privacy Act system 09-90-0058 Tracking Records and Case File for FOIA and Privacy Act Rquests and Appeals.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

An individual's concern that his/her PII was inappropriately released to a FOIA requester would be reported within HHS as a privacy incident and would be analyzed to determine if an improper disclosure occurred; the concern would be responded to in writing; and remedial measures would be taken if an improper disclosure occurred.

Although this system is excepted from the Privacy Act "accounting of disclosures" requirement, an individual can make a FOIA request for the FOIA request log to identify any individuals and entities requesting records about him/her, a description of the records requested, and the dates of the requests.

An individual requester who believes that his/her contact information or other information about his/her request is inaccurate in the system can contact the OS FOIA Office or System Manager identified in SORN 09-90-0058 to request access to the records and contest and seek correction of any inaccurate information. Requesters submitting requests online can update or correct their profile information, including their contact information, at any time.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

HHS system users will be instructed to enter or upload into the system any updated contact or other PII information they receive from requesters.

Paper case files will be periodically compared to printouts of cases in the system to ensure that the tracking numbers match the names, that all requests and paper files are accounted for, and that concluded cases are closed in the system.

Closing cases in the system and indicating if a case involves litigation (and if so, entering the date litigation was concluded) will enable the system to calculate disposition eligibility dates so that PII records can be destroyed when no longer needed.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

FOIA Office staff and FOIA Coordinators will have access to PII pertaining to requests they handle, for purposes of handling the requests.

Members of the public who use the Public Access Link (PAL) will have access to their own PII in order to update their PAL account information, submit requests and related communications to FOIA staff, and receive responses to same.

Administrators:

Administrator-level access will be granted only to certain users in the OS FOIA Office and at the system contractor (and possibly also in the agency's Office of the Chief Information Officer (OCIO)). Administrators will have access to PII for purposes of maintaining and updating the system, administering user access, and troubleshooting system problems.

Contractors:

The system contractor will have access to PII for purposes of maintaining and updating the system, administering user access, and troubleshooting system problems.

Any direct contractor retained to assist the OS FOIA Office with processing requests and appeals would have access to PII for purposes of providing that assistance.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

All users necessarily must have access to PII, because many of the requests and appeals involve individual requesters and/or agency records containing PII.

Each user's access will be determined based on the user's role; for example:
-Each OS FOIA Office Staff member will have access to all or most records pertaining to that FOIA office;
-Each OS FOIA Coordinator will have access to only his/her program office's communications and records;
-Each representative of another HHS FOIA office will have access to only his/her FOIA office's requests and referral and report data;
-A requester using PAL will have access to only records pertaining to requests submitted through his/her PAL account;
-System administrators will have system-wide access but will access PII only if necessary to perform a system administrative task.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

User access will be controlled by role-based access privileges, and each user will log-in with a unique user ID and password.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All users are information disclosure specialists who will use the system (or, in the case of the system contractor, designed the system) to process records for disclosure in accordance with FOIA and Privacy Act requirements. All users receive initial and annual HHS IT system security and privacy awareness training. They also receive basic refresher training and advanced training on a regular basis at FOIA/Privacy Act conferences and workshops hosted by HHS, Department of Justice (DOJ) and outside vendors, regarding safeguarding personal privacy information and avoiding improper disclosures of PII.

Describe training system users receive (above and beyond general security and privacy awareness training).

Because the users are information disclosure specialists, they receive specialized training on a regular basis at FOIA/PA conferences and workshops hosted by HHS, Dept of Justice, and outside vendors providing advanced instructions and guidance regarding safeguarding personal privacy information and avoiding improper disclosures of PII in particular contexts and with respect to specific types of records.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

The applicable records schedule is GRS 4.2, Information Access and Protection Records (formerly GRS 14); it prescribes retention periods ranging from approximately 2 years to 6 years after the date a case is closed.

The system will be updated when a case is closed, will calculate when case records are eligible for destruction, and will generate a report of eligible cases each year, for use in deleting eligible electronic records and shredding eligible paper files.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative: User access will be limited based on role, and will be controlled by assigning each user a unique user ID and password.

Technical: Records stored in the system (which includes the Public Access Link--PAL) will be protected by encryption. Responsive records and communications containing PII can be directly uploaded to the system from HHS users' encrypted workstation drives. HHS users must first log

onto the HHS network with their personal identify verification (PIV) card, using an HHS-issued laptop or personal computer. HHS users who telework must access the system through HHS' virtual private network (VPN) using HHS-issued laptops and their PIV card. Separate web and database servers will provide the online features used by requesters; each requester's access will be limited to his or her PAL account. OS FOIA Office records will be stored separately from records of other HHS FOIA Offices and records of other federal agencies that use FOIAXpress. Auditing features will record when a user accesses the system and the actions taken.

Physical: The buildings and offices where the system contractor's servers are located, and where HHS workstation laptops and PCs used to access the system are located, are secured by locks and security guards during off-duty hours, and by I.D. badges and security guards during office hours. Teleworkers' homes are secured by locks, and teleworkers use encrypted HHS laptops. Users do not leave computer screens unattended or visible to unauthorized persons.

Identify the publicly-available URL:

https://requests.publiclink.hhs.gov/palMain.aspx,
accessible from http://www.hhs.gov/foia
Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null