# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

09/12/2016

### OPDIV:

FDA

### Name:

Administrative Applications: Ethics Applications

**PIA Unique Identifier:**

P-9982341-092311

**The subject of this PIA is which of the following?**

Minor Application (child)

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Operations and Maintenance

**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?**

No

**Identify the operator.**

Agency

**Is this a new or existing system?**

New

**Does the system have Security Authorization (SA)?**

Yes

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

**Describe the purpose of the system.**

This PIA addresses two applications, Ethics eForms (which provides relevant forms and collects information) and Ethics (which stores the information). These applications permit the submission of documents required of certain FDA employees. Employees download templates of these forms from eForms and then also submit the completed forms via eForms. Forms may be Word documents, Adobe interactive PDFs, or in other formats.

The purposes of these forms include:

Financial Disclosure: Financial disclosure reports are used to demonstrate whether employees have any investments, property, or other interests that could result in a perceived or actual conflict of interest.

Outside Activities: Employees submit outside activity request forms which are then reviewed by ethics staff for the purpose of assuring that employees do not violate the conflict of interest laws regarding outside employment and holding positions with outside entities.

Widely Attended Gatherings: Employees submit notices indicating an intention to attend functions and events, and Ethics staff confirms whether they may do so under existing ethics laws and regulations.

Confidentiality: Employees verify that they are aware that some information made available to them must not be disclosed without specific authorization, especially if such information involves national security or if it is private, personal, or business information which has been furnished to the government in confidence.

These requirements are reported using standard forms.

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

These applications are used to collect and store information saved on forms. In some cases, additional documents may be supplied to explain information entered onto forms (i.e., attachments to forms). Financial disclosures forms may contain contact information (home or work address, phone, e-mail and fax information); job title, pay grade, salary, and terms of employment; financial interests including name of investment, type of investment, and date acquired; assets and income outside of federal employment; dates and other information about significant purchases, sales, or exchanges; other information about financial holdings such as percentage of total investments made in regulated organizations; gifts, reimbursements, and travel expenses; liabilities include descriptions, amounts, interest rates, dates incurred, and identities of creditors; agreements and arrangements with former employers concerning benefits, payments, leaves of absence, and offers of future employment; positions held outside of the United States government including uncompensated positions; compensations over $5,000 provided by one source; and recommendations of ethics staff; dates and other details of divestiture if ordered by ethics staff; and signatures of employees attesting to the truth and completeness of information provided on such forms. Some of these data elements (including information about investments, assets, and income) may be provided or the employee as well as spouses, children, or other close relatives or associates.

Event or activity forms may contain similar information and, in addition, dates of events or activities; sponsors or beneficiaries of events or activities; numbers of individuals involved; subject matter of the activity; text of any disclaimer provided; location of the activity; and compensation or other benefits offered to the employee. Additional space is provided where the individual is asked to explain the nature of the employee's FDA official duties; the relationship of the employee's official duties to outside activities; the effect of the individual's official duties on the outside employer; and any assignment provided by the outside employer.

Most or all forms used in ethics filings include open fields permitting employees, supervisors, and ethics reviewers to provide additional comments at their discretion. Most forms also include designated spaces for supervisors and ethics officers to indicate their review of the document and their findings (such as approval or denials of requests). The applications would also permit individuals to submit attachments or similar documents. Open fields may contain any information a submitter chooses to include, including any and all items of PII.

Neither application requires FDA users to have system-specific logon credentials. Both are part of a single-sign on protocol that relies on users' network credentials for multi-factor authentication. No credentials are required for employees, supervisors, nor ethics reviewers.

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

Ethics eForms is the application employees use to submit necessary documents to Agency and component ethics offices. It transmits PII but does not collect or store it, and it is not subject to the Privacy Act.

The documents then reside in the Ethics application repository, where they are available to ethics analysts. Based on the outcome of those analyses, ethics offices may advise employees to divest themselves of interests, forgo attending certain events, decline to take certain actions, or supply further information. In the case of some ethics violations, ethics officers may advise more extensive actions, including sanctions up to and including termination or referral to appropriate law enforcement entities.

Standard forms used for these purposes are publicly available and include:
FDA 2096, “Regulation Certification for New Employees” (created 03/04)
FDA 2097, “Certification for Separating Employees” (created 01/03)
United States Office of Government Ethics (OGE) 450, "Confidential Financial Disclosure Report" (expires 01/31/17)
OGE 450A, "Confidential Certification of No New Interests" (created 08/05)
OGE 278, "Public Financial Disclosure Report" (expires 03/31/17)
OGE 278T "Public Financial Disclosure Report: Periodic Transaction Report" (created 01/13)
HHS 717-2, "Report of Prohibited Financial Interests" (created 05/10)
HHS 520, “Request for Approval of Outside Activity” (created 01/06)
HHS 521, “Annual Report of Outside Activity” (created 01/06)
FDA 3539, “Request/Approval for Free Attendance at Widely Attended Gatherings (WAG)” (created 05/09))

Note that some of these forms are created and owned by agencies other than FDA, and FDA is not able to resubmit these for updated approvals to OMB, merely to request that the agency that owns the form does so.

Users and administrators most often retrieve forms by individuals' (applicants and applicants who become Special Government Employees (SGE)) names.

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Certificates

Education Records

Military Status

Employment Status

Foreign Activities

Any other information relevant to inquiries concerning individuals' potential legal, financial, or other

Information indicated is for employees completing ethics forms; some data elements (name, relationship to employee, financial information) may be required for spouses, children, or close relatives or associates.

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

Employees

Public Citizens

Applicants are public citizens. Accepted applicants are special government employees (SGEs).

**How many individuals' PII is in the system?**

10,000-49,999

**For what primary purpose is the PII used?**

The information provided is used to confirm the absence of ethical violations; ensure employee acceptance and acknowledgment of ethical responsibilities; or identify ethical conflicts of interest or possible unethical activity. Subsequently, ethics officials will address any findings of unethical activity by advising employees and supervisors of actions that must be taken, and/or reporting violations to the appropriate authorities to take actions up to and including dismissal from service or criminal or civil prosecution.

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

None.

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

All information use and disclosure is required by the Ethics in Government Act of 1978, as amended, Title 5 of the U.S. Code, Appendix. Regulations implementing these requirements include 5 C.F.R. Part 2634 (for most financial disclosures); 5 CFR 5501.104 (HHS Supplemental Ethics Regulations); 5 CFR 5502.106 (HHS Supplemental Financial Disclosure Regulations); and 5 CFR 2635.803, 5 CFR 5501.106(d) (HHS Supplemental Ethics Regulations).

**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.**

SORN 09-90-0018, Personnel Records in Operating Offices

SORN 09-90-0008, Conflict of Interest Records

**Identify the sources of PII in the system.**

Online

**Government Sources**

Other Federal Entities

**Identify the OMB information collection approval number and expiration date**

OGE 278, OMB No. 3209 - 0001
OGE 278-T, Pending
OGE 450, OMB No. 3209-0006
OGE 450A, Pending
FDA 2096, Pending
FDA 2097, Pending
FDA 3539, Pending
HHS 717-2, Pending
HHS 520, Pending
HHS 521, Pending

**Is the PII shared with other organizations?**

Yes

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

**Within HHS**

Sent to HHS Office of General Counsel or Ethics Offices to report items that need to be investigated as possible ethics breaches. FDA may also supply aggregated (non-PII) information to the HHS Ethics office for planning and evaluation purposes.

**Other Federal Agencies**

Other agencies such as the Department of Justice may be informed of the need to investigate or report suspected ethical violations. However, the initial disclosure would be made to an HHS office (as above), which would then in turn contact outside agencies as necessary.

**State or Local Agencies**

Investigate or report suspected ethical violations. The initial disclosure would be to an HHS office, which would in turn contact the outside agency as necessary.

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

No disclosures are made directly from these applications. If disclosures to the HHS Office of General Counsel are necessary to report or investigate ethics violations, these are made consistently with federal law, regulations, and internal procedures; further disclosures are governed by an extensive body of statutory and common law.

**Describe the procedures for accounting for disclosures.**

Disclosures from these applications are unlikely to be made. If Privacy Act records are disclosed, the disclosing office will maintain an accounting.

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

Individuals submit all information themselves at the time of collection via a web-enabled tool.

**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.**

Submission of information is "voluntary" as that term is used by the Privacy Act, but required for all employees by ethics laws and regulations. Some forms are only required from some employees. For example, OGE 450 is only required for employees serving in “Confidential Filing” positions (as that term is defined at 5 CFR 2634.904).

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

If the agency changes the collection, use, or sharing of PII data in these applications, the affected individuals will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a notice on FDA web site, or e-mail notice to the individuals.

**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.**

Individuals who are the subject of records in these applications may exercise the rights available to them under the Privacy Act. The Privacy Act permits information subjects whose records are retained in systems of records to request notification of the existence of, access to, and amendment of records about themselves.

Individuals have many other avenues available to address these concerns. They may for example work through their supervisors, human resources officials, the FDA Privacy Office, information system security officers, the information system owner, the Computer Security Incident Response Team, or the employee help line to address any concerns about inaccuracies or incidents. Any changes to an individual's name or address would need to be updated using a Standard Form 50 or 52, just as would be the case with other FDA employees, and the data would be updated in HHS's human resources information system.

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

Annual Filers must resubmit form 450A each year (if there are no significant changes from the previously-submitted 450), and a complete and full form 450 every three years, and any inaccuracies or changes will be addressed by ethics program staff. Other forms are submitted annually or ad hoc to address changed conditions or status, such as form 278 (submitted annually), 278T (the Periodic Transaction Report), and form HHS 520 (the Annual Report of Outside Activity). Also, information is updated if information in the databases that populate Ethics are updated. Changes made in HHS's human resources system are sent to FDA's Enterprise Administrative Support Environment (EASE) which in turn updates Ethics.

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

**Users:**

Submitters have access to their own PII only. Ethics office employees are "users" for the purpose of this document and will have access to PII in order to conduct assessments of ethical compliance.

**Administrators:**

Administrators conduct management and oversight of the information system, including managing access for system users within ethics offices.

**Developers:**

Developers will not normally have access to PII, but may in the course of maintaining the systems or providing technical assistance.

**Contractors:**

Some developers may be direct contractors and will have access under the same circumstances as developers.

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

Submitters do not require access to others' PII and may submit information without accessing the applications. Users who require access to the application (e.g., ethics staff) need to have supervisor approval and sign off before access is granted. Administrators with the ability to provide user access are limited to senior ethics staff; points of contact in component agencies (Centers) can only provide access to records of individuals employed by those Centers.

The user's supervisor will use an account creation form to specify the minimum information system access that is required in order for the user to complete his/her job. The agency reviews the access list for the application on a quarterly basis to review and adjust users' access permissions, and to remove unnecessary accounts from the application.

**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.**

Management establishes roles for individual personnel, with role-based restrictions permitting access only to information that is required for each individual to perform his/her job.

**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 personnel/users are required to complete FDA's IT Security and Privacy Awareness training at least annually.

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

A user manual for the Ethics application is available that provides assistance to users. This is available from within the Ethics application only, and so access to this training is restricted through system access control.

All users are instructed on adhering to the HHS Rules of Behavior in the context of their work involving this system. For additional privacy guidance, personnel may contact the agency's privacy office. Privacy program materials are provided to personnel on a central intranet page. Personnel may take advantage of information security and privacy awareness events and workshops held within FDA.

**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.**

Records are maintained under the FDA 9400 series of records retention schedules. Retention periods vary by form. Retention times vary and can be as long as six years or even longer if they are needed for an ongoing investigation, in which case they will be retained until no longer needed in that investigation.

Retention times for individual forms is as follows. Forms are to be destroyed after the retention period unless they are in ongoing use, e.g., if they are needed in an ongoing investigation.
FDA 2096: Schedule 9461, six years
FDA 2097: Schedule 9412, six years
OGE 450: Schedule 9422a, one year (if not confirmed for a position); Schedule 9422b, six years (all others)
OGE 450A: Schedule 9422b, six years
OGE 278: Schedule 9421a, one year (if not confirmed for a position); Schedule 9421b, six years (all others)
OGE 278T: Schedule 9421b, six years
HHS 717-2, Schedule 9430, six years
HHS 520, Schedule 9470, six years
HHS 521: Schedule 9451, three years
FDA 3539, Schedule 9411, three years

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

Administrative Safeguards include training and awareness provided for all users; manuals that advise on the proper use of the applications; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include that PII entered via Ethics eForms is immediately pulled into Ethics, and is not accessible to other users of Ethics eForms or fda.gov.  Ethics resides behind the FDA firewalls.  Physical controls include that all servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. More broadly, appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.