US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/14/2016

OPDIV:

FDA

Name:

User Fees System

PIA Unique Identifier:

P-7925017-042526

The subject of this PIA is which of the following?

Major Application

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

No privacy related changes.

Describe the purpose of the system.

FDA's User Fee System (UFS) automates, centralizes and standardizes billing and collection of industry paid user fees, which make up roughly half of the Agency's budget. UFS collects data related to user fee transactions, including customers, receivables and payments for more than twelve different user fee programs. The system services more than 60,000 customers across 120 countries.

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

UFS collects data related to transactions for which external industry users must pay fees, e.g., applications for FDA approval of a product. Such transactions involve user fees associated with:

Prescription Drug User Fee Act
Medical Device User Fee Act
Animal Drug User Fee Act
Animal Generic Drug and User Fee Act
Generic Drug User Fee Amendments
Biosimilar User Fee Act
Mammography Quality Standards Act
Export Certificates
Color Certification
Family Smoking Prevention and Tobacco Control Act
Freedom of Information Act
Food Safety Modernization Act

Individuals who are internal users are either permanent federal employees or direct contractors. UFS collects identifiable information about the name and email address for these individuals. This information is necessary to support and control access because these employees are responsible for accessing Oracle Applications as approved by the account approval process.

For individuals associated with external industry, UFS collects business identifiable information: name, address, telephone number, email address, DUNS (data universal numbering system no., issued by Dun & Bradstreet), waiver information, application specific data (e.g., new drug application number), Taxpayer Identification Number (TIN) and Federal Employer Identification Number (EIN; a small business may choose to use the owner's Social Security number as the EIN/TIN).

In each instance, the information collected is necessary to enable billing and collections actions required by the user fee legislation. The data collected is the minimum necessary to accurately and effectively complete the cover sheet, billing and refund processes.

Only FDA employees have access to the system. Access support is provided by help desk staff. All requests by users for password resets go through the help desk staff. Users cannot independently change their username or password (user credentials).

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

For internal federal users, UFS collects specifically identifiable information work context information such as name and email address. The records are of employees responsible for accessing Oracle Applications as approved by the account approval process. UFS also maintains user credentials for these individuals.

For external industry, UFS collects information necessary to accurately and timely account for payment activities, issue correct refunds to the relevant party, direct collections actions at the appropriate party, adjust invoices and credits and debits, and otherwise ensure data and actions are associated with the correct entities. FDA may share system information with other federal agencies as necessary in the context of subpoenas, litigation, debt collection, court proceedings, and records requirements.

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Taxpayer ID

Cover sheet ID

Data Universal Numbering System (DUNS)

New Drug Application/Biologics License Application Number

Federal Employer Identification Number (FEIN)

User Credentials

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

Employees

Public Citizens

Public citizens refers to Industry customers

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Information is collected to facilitate billing and collections required by user fee legislation. The data collected is the minimum necessary to complete the cover sheet, billing, collection and refund processes.

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

None.

Describe the function of the SSN.

Domestic firms must provide an Federal Employer Identification Number/Taxpayer Identification Number (FEIN/TIN). If a small business opts to utilize the owner's Social Security number (SSN) rather than a separate EIN/TIN, the company would enter the SSN in the EIN/TIN field. Otherwise, SSN's are not required.

Cite the legal authority to use the SSN.

Executive Order 9397, as amended; 5 U.S.C. 301; 44 U.S.C. 3101; 21 U.S.C. 393(d)(2).

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

42 U.S.C. 263b(r)(1); 5 U.S.C. 301, 552, 552a; 44 U.S.C. 2904, 2906, and 3101; 21 U.S.C. 371, 379, 379e, 379f, 379h, 379h–1, 379j, 379j–12, 379j–21, 379j–31, and 387s; Debt Collection Improvement Act of 1996 (31 U.S.C. 3701 note).

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.

09–10–0021, FDA User Fee System, HHS/FDA

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0910-0805, expires 11/30/2018
0910-0539, expires 08/31/2017
0910-0718, expires 08/31/2018
0910-0727, expires 02/28/2019
0910-0511, expires 08/31/2019
0910-0297, expires 03/31/2019
0910-0632, expires 07/31/2017
0910-0625, expires 06/30/2019

Is the PII shared with other organizations?

Yes

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

Within HHS

IT security purposes; Freedom of Information Act (FOIA) requirements; debt collection support.

Other Federal Agencies

Subpoena, litigation, court proceedings, records requirements.

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

There is no information sharing agreement or memorandum of understanding employed regarding the sharing of UFS data within HHS; this sharing is conducted in accordance with FDA and HHS policies such as the HHS Service and Supply Fund policies and procedures. Other sharing is governed by legal processes, such as the terms of a subpoena or court order.

Describe the procedures for accounting for disclosures.

Records of disclosures are maintained within the system and by related FDA offices as a standard practice inherent to the fee billing, collection and administrative processes.

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

Notice statements are provided on submission forms. FDA has published a system of records notice (SORN) in the Federal Register (Nov. 14, 2012). Individuals may also view FDA's privacy policy on FDA.gov.

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.

There are no opt-out processes. In order to attach payments to a specific company and otherwise manage the fee process, information must be collected.

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

Procedures include: Publication of an amended SORN in the Federal Register; updates of notice statements on user fee forms; potentially direct or agency-wide communication to internal individuals for major changes related to their PII.

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.

There are no agency procedures required for the correction of information; submitted information is entered by the individual and they may make changes if the information is inaccurate. Individuals with other concerns may contact FDA offices using phone, mail or email contact information provided on FDA.gov. Internal personnel may use the Employee Resource information Center (ERIC) to obtain assistance regarding PII issues.

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

There are no dedicated processes in place. Individuals may self-supplement or self-correct their information. Internal system problems impacting data integrity or availability are addressed at the time of discovery, through standard IT support programs.

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

Users:

Federal employees match payments to invoices and cover sheets.

Contractors:

Direct contractors support the operations and maintenance of the system, support the help desk, and support the resolution of system issues.

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

Access must be approved by system management and is granted to users (federal staff and direct contractors) based on their work requirements.

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.

Responsibilities are assigned to specific users and the scope of access permitted to each is limited to their specific work requirements.

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.

General security and privacy awareness training are provided to all staff and contractors at a minimum of annually.

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

Users are trained on the system, review the HHS Rules of Behavior and may complete specialized role-based privacy training as appropriate in accordance with their information handling duties.

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.

UFS records are maintained in accordance with FDA's Records Control Schedule, and with the applicable General Records Schedule (GRS) and disposition schedule approved by National Archives and Records Administration (NARA).

UFS records fall under GRS 20, Items 2a(4) Hard copy documents other than those covered by Items 2(a) (1) - (3). Destroy after the information has been converted to an electronic medium and verified, when no longer needed for legal or audit purposes or to support the reconstruction of or serve as a backup to the electronic records, or (applicable to permanent records only) 60 days after NARA has been provided the notification required by 36 CFR 1225.24(a)(1), whichever is later. (N1-GRS-07-4 item 2a4)

GRS 20, Item 12 Derived data and data files that are copied, extracted, merged, and/or calculated from other data generated within the agency, when the original data is retained. Delete from the receiving system or device when no longer needed for processing. (N1-GRS-95-2 item 12c)

GRS 20, Item16 Printouts derived from electronic records created on an ad hoc basis for reference purposes or to meet day-to-day business needs. Destroy when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes, provided the printouts do not contain substantive information, such as substantive annotations, that is not included in the electronic records. (Printouts that contain substantive information should be disposed of in accordance with the NARA-approved schedule that covers the series in which they are filed.) (N1-GRS-07-4 item 3.2. Slight edit in series description informally approved by NWML October 2009.)

NARA approved citation N1-088-09-011, Items 1.1 (files maintained in the Office of Financial Management), Disposition: Temporary. Cutoff at the end of the fiscal year after the completion of the 5-year User Fee Program cycle. Delete/destroy 75 years after cutoff, or when no longer need for administrative legal, or reference purposes, whichever is the latest.

1.2 (Data maintained by FDA Centers). Disposition: Temporary. Cutoff at the end of the fiscal year after the completion of the 5-year User Fee Program cycle. Delete/destroy 70 years after cutoff, or when no longer need for administrative legal, or reference purposes, whichever is the latest.

1.3.2 (database record after cutoff) Disposition: Temporary. Cutoff at the end of the fiscal year in which received. Delete/destroy 75 years after cutoff, or when no longer need for administrative legal, or reference purposes, whichever is the latest.

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

The information contained within UFS is protected by several layers of administrative, physical, and technical controls including use of user identification, passwords, firewall, virtual private network, encryption, intrusion detection, smart cards, guarded facilities, closed circuit tv, cipher locks and key cards.

Identify the publicly-available URL:

iStore URLs:

ADUFA

https://userfees.fda.gov/OA_HTML/fdaCAcdLogin.jsp

AGDUFA

https://userfees.fda.gov/OA_HTML/AGDUFACAcdLogin.jsp

BsUFA

https://userfees.fda.gov/OA_HTML/bsufaCAcdLogin.jsp

GDUFA

https://userfees.fda.gov/OA_HTML/gdufaCAcdLogin.jsp

MDUFA

https://userfees.fda.gov/OA_HTML/mdufmaCAcdLogin.jsp

PDUFA

https://userfees.fda.gov/OA_HTML/pdufaCAcdLogin.jsp

FURLS

https://userfees.fda.gov/OA_HTML/furls.jsp

iReceivables URL:

https://userfees.fda.gov/OA_HTML/irecLogin.jsp

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 do not collect PII.

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

No

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

Yes

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

Yes