US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/14/2017

OPDIV:

FDA

Name:

Electronic Submissions Gateway

PIA Unique Identifier:

P-9523858-382822

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.

Upgraded software; migrated database from 10g to 11g ; implemented WebTrader Hosted Solution.

Describe the purpose of the system.

The FDA Electronic Submissions Gateway (FDA ESG) provides a centralized, secure, Agency-wide solution for receiving electronic regulatory submissions. The FDA ESG serves as a component of a communications system, for regulatory submissions from multiple sources, such as pharmaceutical companies and medical device manufacturers. It enables the FDA to receive guidance-compliant submissions electronically which the ESG directs to the appropriate subject matter Center within the Agency.

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

The FDA ESG collects and stores two sets of data. The first set of data is collected from external entities to create user accounts within the FDA ESG to support the transmission of regulatory documents.

The accounts are owned by corporate entities submitting materials to FDA. The corporate entity supplies the name, phone number, and e-mail address for a primary and secondary contact person. This information is used by the FDA ESG when necessary to resolve technical issues. The second set of data is metadata about each regulatory submission and includes time of submission, user account, transmission protocol, a message identification number, and a file name. This information is used by the Agency to track the submission and if necessary aid in file recovery.

Some electronic submissions transmitted through ESG may contain patient or consumer information. ESG does not process these submissions but instead passes them through to the appropriate destination system.

There are two ways to submit submissions to FDA ESG, one is gateway to gateway or using the user interface, Webtrader. Both are methods to submit within ESG with Webtrader just providing a user interface for easier computer access.

Webtrader is a user interface within ESG to assist with regulatory submissions for external submitters who may need technical assistance with their submissions. Submissions are not stored within Webtrader; they move through it in route to be processed by the internal components of ESG. Technical support staff (FDA personnel providing support to ESG/Webtrader as a single/joint application) do not have access to materials submitted using Webtrader. Once at the ESG, the system forwards all submissions downstream to the appropriate FDA Center as a function of ESG.

ESG system administrators and users (agency employees, direct contractors, and external submitters/users) employ usernames and passwords to access ESG (Webtrader/ESG administration are the same for administration purposes there are no separate credentials). For all users, the ESG system administrator provides a username and a password that these users must change upon the first login.

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

The FDA ESG facilitates the receipt of electronic submissions with the assistance of Webtrader. The Webtrader application does not store any of the pass-through submissions; it facilitates the technical needs that external submitters may have in regards to regulatory submissions to ESG, e.g., technical format options and standards appropriate for ESG. The FDA ESG serves as a component of a communications system, collecting information (regulatory submissions) from multiple sources, such as pharmaceutical companies and device manufacturers, then forwarding that information to a file server where the appropriate FDA system can retrieve the information. Pending this retrieval, submissions are temporarily stored within the FDA ESG on a limited basis (up to 10 days) in support of integrity and availability procedures at FDA. FDA maintains submissions in separate systems dedicated to the various product types, e.g., medical devices.

Submissions contain files with information about FDA-regulated products such as drug approval applications or formulations, device applications and reports of the adverse event associated with a product. ESG also stores data related to where the submission originated, the destination, the receipt and delivery date and time stamps. The FDA ESG does not "own" or maintain the data that passes through its components. The data is “owned” by the destination application used by the relevant receiving FDA center. In sum, the FDA ESG is providing a supporting service to these applications which are the subject of their own Privacy Impact Assessments.

Metadata about each regulatory submission and includes time of submission, user account, transmission protocol, a message identification number, and a file name are also captured in the ESG database. This information is used by the Agency to track the submission and if necessary aid in file recovery.

FDA does not use Personally Identifiable Information (PII) to retrieve records transmitted through or temporarily stored within ESG.

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

Phone Numbers

Logon credentials (username, password and company name).

For industry submissions, the name of a point of contact may be included. FDA does not retrieve data from the system using this professional contact information PII.

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

Patients

Logon credentials are maintained for all of the above categories of individuals. "Public Citizens" in this case refers to industry-side individuals.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

PII is used to manage accounts in the system and communicate with users regarding their account status and submission status.

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.

Authority for the collection of information by this system is given by provisions of the Federal Food, Drug and Cosmetic Act, 21 U.S.C. 301 et seq., many of which require reporting by regulated entities in fields such as the manufacture and distribution of foods, drugs, cosmetics, dietary supplements, and tobacco products.

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

No

Not applicable.

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not applicable.

Is the PII shared with other organizations?

No

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 is provided within information and guidance provided to users on the ESG website. Notice is also provided via the FDA Privacy Policy which is accessible via fda.gov (see "Website Policies" in the footer of the webpage) and all pages within that domain including the pages associated with the electronic submission process.

Individuals or entities that collect PII from third parties (such as patients) and submit that information via the ESG are responsible for satisfying applicable notice and consent requirements, if any.

Users such as a system administrators, developers, or direct contractors are notified of the collection of their information on the ESG Website. When setting up an account, the user is asked to provide their company name, first and last name, phone number, submission method, and type of account they are requesting. Setting up an account is a requirement for access to ESG. At the time of hire, FDA employees also receive notice of the necessary use of their information in the context of their service as government employees.

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 PII is voluntary as that term is used by the Privacy Act. FDA employees, direct contractors, and external users who access ESG can opt-out of collection or use of their PII. However, the submission of PII is necessary in order for systems users to obtain access and use the ESG system. Some electronic submissions transmitted through ESG may contain patient or consumer information, however, ESG does not process these submissions but instead passes them through to the appropriate destination system.

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

No such changes are anticipated. If the agency changes the collection, use, or sharing of PII data in this system, 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 the website or e-mail notice to the individuals.

If the agency ever changes its use of the PII of its system users that serve as access credentials, employees, direct contractors or external users could be notified many ways, including by phone, e-mail, and notices on the intranet.

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 suspect their PII has been inappropriately obtained, used or disclosed in any FDA system have a number of avenues available to request to rectify the situation.

Often, these individuals contact the office or division where they have determined that their information is held. Individuals may then make further requests for their information to be corrected or amended.

Employees or direct contractors with such concerns can additionally work with their supervisors, a 24-hour technical assistance line, FDA's Systems Management Center, and other channels. External users can contact the ESG System Administrator or Help Desk for assistance.

Contact information for the FDA Privacy Office is provided on FDA.gov and FDA's intranet.

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

The integrity, availability, accuracy and relevancy of the PII within submissions is the responsibility of the FDA organization which maintains the destination system where they maintain submissions.

FDA personnel are responsible for providing accurate information and may independently update and correct their information at any time.

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

Users:

ESG users will not have access to others' logon credentials.

Administrators:

Administrators may be application administrators who require access to create and manage user accounts, but will not have access to users' self-created passwords.

Developers:

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

Contractors:

Some developers may be direct contractors with access under the same circumstances as developers. Webtrader contractors (non-direct) do not have access to ESG.

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

The only PII in the system is user access credentials and professional contact information. Although administrators may have access to usernames in the course of creating and maintaining accounts, they will not have access to passwords. The name, email address, and phone number are used by the system administrators and help desk support staff for providing technical assistance. Administrators and support staff must have supervisory approval before they are granted access.

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 set 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.

The FDA requires all agency personnel and contractors to complete FDA's IT Security and Privacy Awareness training at least once every 12 months. A portion of this training is dedicated to guidance on recognizing and safeguarding PII.

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

Additional on-the-job or informal training may be received.

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.

General Records Schedule (GRS) 24-(6) 9961 User Identification, Profiles, Authorizations, and Password Files.

Disposition: TEMPORARY. Destroy/delete inactive file 6 years after user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

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

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical Safeguards include firewalls, network monitoring and intrusion detection, virtual private networks, and multi-factor authentication. Physical controls include that all system servers are located at FDA facilities protected by guards, locked facility doors, and climate controls. Other 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.

Identify the publicly-available URL:

http://www.fda.gov/ForIndustry/ElectronicSubmissionsGateway/default.htm

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?

No

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

N/A