US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

OPDIV:

FDA

Name:

FDA CDER FDA Adverse Event Reporting System

PIA Unique Identifier:

P-1403714-071868

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?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

Provide new PIA form content.

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

Changed the Point of Contact (POC) to Alex Schultz

Describe the purpose of the system.

The FDA Adverse Event Reporting System (FAERS) will be used by FDA's Center for Drug Evaluation and Research (CDER) and Center for Biologics Evaluation and Research (CBER) to store, retrieve, and analyze adverse event and product problem reports.

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

The system collects adverse event reports regarding FDA regulated products. FDA requires certain types of organizations to make these reports, although individuals who experience adverse events may make reports, as well, even though reports on the part of those individuals are not required.

Typical data elements collected from the reports include the date of the event being reported, a narrative (possibly containing medical history and other medical data such as medical records numbers), coded or un-coded data relating to the affected person's disease or health condition, and a limited amount of PII, including (if known or applicable) the subject's name, date of birth, and subject/submitter contact information such as name, address, phone and e-mail address.

Reports include what PII may be known to the reporting entity (e.g., the manufacturer) such as a patient's initials, date of birth, gender, description of medical history, and the name and contact information for the point of contact at the reporting importer/manufacturer. The system will receive PII and/or potential PII a submitter opts to include in narrative text fields or within documents attached to a submitted report. The system also contains administrative PII in the form of professional contact information for FDA personnel and for the point of contact submitting a report such as work e-mail, phone and mailing address. Members of the public submitting voluntary reports may do so using FDA online information technology systems (such as FDA's Electronic Submission Gateway (ESG) or CDRH Center Electronic Submissions system (CESub), both covered by other PIAs), or through reports that may be transmitted in some other method such as e-mail, at which time FDA FAERS Administrators can integrate the information received into FAERS.

While any member of the public can use FAERS to submit a report of an adverse event, for the purposes of this document, "users" of the FAERS system are all FDA employees who access the system in order to conduct activities in support of the FDA mission. These include FDA staff that use the information to evaluate the safety of drugs; users that assess the compliance of regulated entities with requirements to report adverse events, users who access the system to respond to Freedom of Information Act (FOIA) requests; users from the Division of Medication Error Prevention and Analysis (DMEPA) who assess whether adverse events resulted from medical errors; and data entry personnel.

System users (analysts with access to all reports in order to perform evaluations of the safety and effectiveness of drugs) access the system under a single sign-on model. However, once the system is accessed, users (including administrators) will have access to a module called Oracle Adverse Event Reporting System (OAERS), used to conduct system oversight, that will require login credentials (username and password). OAERS will govern a role-based access approach under which individuals with different roles will have different levels of access. For example, only individuals with administrative-level access will be able to create new accounts.

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

This FDA Adverse Event Reporting System (FAERS) is a computerized information database designed to support the FDA's post marketing safety surveillance program for approved drug and therapeutic biologic products and devices. The FDA uses FAERS to collect, analyze and respond to safety reports, also referred to as adverse event reports and product problem reports, regarding health and safety problems that may be associated with approved drugs and biologic products. The goal of FAERS is to improve the public health by providing the best available tools for storing and analyzing safety reports.

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

Yes

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Work contact information for FDA personnel (permanent and contract employees). Professional contact information (phone, email, mailing address) for point of contact submitting a required report. Submitters may choose to include PII in the patient identifier and/or narrative text fields of a reporting form, such as personal history, names of individuals, or descriptions of actions associated with an adverse event.
All users have a password and user ID that are used to administer role-based access.

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

Employees

Public Citizens

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

Patients

"Employees" includes HHS and FDA permanent employees and direct contractors. "Public citizens" include individual public users (voluntary submitters). "Patients" is a subset of public citizens. Business partners include federal, state, and local agencies.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The FDA uses the collected PII to effectively capture, track and respond to adverse events reported to FDA. Access credentials (user password and ID) are used for controlling and authenticating access to FDA FAERS.

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.

Sections 201, 502, 505, and 701 of the Federal Food, Drug, and Cosmetic Act (the act) (21 U.S.C. 321, 352, 355, and 371) require that marketed drugs be safe and effective. In order to identify unsafe and/or ineffective drugs in use, FDA must be promptly informed of adverse experiences occasioned by the use of marketed drugs. Accordingly, FDA issued regulations at §§ 310.305 and 314.80 (21 CFR 310.305 and 314.80) to impose reporting and record keeping requirements on the drug industry. Collecting the reported information enables FDA to take the action necessary to protect the public from adverse drug experiences.

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Other

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Foreign

Non-Governmental Sources

Public

Media/Internet

Private Sector

Other

Identify the OMB information collection approval number and expiration date

0910-0291 expires September 30, 2018; 0910-0308 expires February 28, 2018.

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.

HHS and FDA personnel are notified, and as a condition of employment, consent to the use of their information by FDA and HHS at the time they are hired. A disclaimer on the FAERS home page on FDA.gov notifies users that FAERS is a U.S. Government system and that use of the system does not entail a right to privacy. FDA's privacy policies are also permanently available across all fda.gov web pages and describe FDA policies and practices for information collection and sharing.

Reporters do not have a choice regarding the submission of information including PII. Note that when required by their local law, regulation or other authority, foreign manufacturers may redact PII from reports they submit.

Individuals submitting a voluntary report using FDA form 3500 are provided an opportunity (section on the reporting form) to indicate that FDA should not disclose their identity to the relevant manufacturer and they may limit privacy risks by choosing not to include unnecessary PII when submitting a voluntary report.

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.

HHS and FDA personnel are notified, and as a condition of employment, consent to the use of their information by FDA and HHS at the time they are hired.

Reporters are not required to report PII of the affected individuals, and have full control over the submission of PII, if any. Reporters (e.g., manufacturers) do not have a choice regarding the submission of information including PII about themselves. This information is essential in order for FDA to effectively analyze and respond to event reports, and thereby protect against unsafe drug and biologic products in the marketplace.

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

HHS/FDA personnel consent at the time of hire, and system changes would not likely alter the use of their PII (used for authentication purposes only). If necessary, they would be notified of changes via an amended disclaimer statement they encounter when using the system and/or internal e-mail.

Institutional reporters (such as manufacturers) do not have a choice regarding the submission of information, including PII about themselves. Note that when required by their local law, regulation or other authority, foreign manufacturers may redact PII from reports they submit.

Reporters would be notified of any changes via updated statements on the submission form and on FDA.gov.

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 may also raise concerns with FDA officials via mail, phone and e-mail as provided on FDA.gov. Personnel may submit concerns using FDA's 24-hour technical assistance help line.

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

FDA validates PII for points of contact at institutional reporters, similarly to processes in existence for other similar FDA adverse event systems. User account information is subject to periodic reviews at least twice a year for accuracy and to ensure accounts are still active.

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

Users:

For the purpose of this PIA, "users" are analysts with access to all reports in order to perform evaluations of the safety and effectiveness of drugs. They require access to full reports.

Administrators:

Quality Control

Developers:

Unit and system test and development

Contractors:

Data entry, quality control

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

System managers review access requests on an individual basis.

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.

All users including administrators, developers and direct contractors are granted the minimal privileges that they need to do their job. The system supports different user "roles" and a process is in place to remove users who don't sign onto the system within a set period of time. Users who interface with the system at the database or application level can only get these privileges through a formal written request (3530 form). All users FDA network users must have a current Personal Identity Verification (PIV) compliant badge.

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 must complete security and privacy awareness training at a minimum of once a year.

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

System users receive system-specific training, review the HHS Rules of behavior and have access to specialized privacy training.

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 in accordance with NARA citation N1-088-07-2 and the specific provisions for FDA adverse event report records which provide for destruction of records 10 years after the end of the calendar year of creation or when obsolete.

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

There is administrative control in place through existing formal processes (security plan, contingency plans, etc.). Technical controls are employed through use of password and user identification, protective firewall, virtual private network, intrusion detection, encryption, and smart cards. The system will be maintained at a secure facility.