US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/05/2016

OPDIV:

FDA

Name:

Drug Quality and Compliance Portal

PIA Unique Identifier:

P-4880315-492389

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The Center for Drug Evaluation and Research (CDER) Drug Quality and Compliance Portal (DQCP) system serves as a central data holding place for information collected in relation to requirements of the Drug Supply Chain Security Act (DSCSA) and makes the data accessible to authorized CDER staff. The system contains several modules, including Electronic Drug Registration and Listing (EDRLS), which contains listings of drugs and no PII; CDER Generic Drug User Fee Facility Data Management (UFFDM); Compounder Reporting; Wholesale Drug Distributors Third-Party Logistics Providers (WDDs/3PLs), Submission, CDER Direct Admin, and Compliance. The system assists with documentation of compliance requirements using the CDER Labeler Code Management. It also integrates with the CDER Direct Admin component, “Structured Product Labeling” (SPL), the required format for sending information about how a manufacturer or seller of pharmaceuticals intends to provide information on the labels of packaging of the pharmaceutical products it produces. There are in addition a transmission component, and the DQCP Portal Administrative component.

Previously, the EDRLS system had its own PIA and authority to operate. Now, EDRLS is one component of DQCP.

DQCP enables FDA analysts to search and retrieve submitted information for use in the course of conducting approvals, inspections, approvals of imports, recalls, adverse event report and compliance actions, and drug supply chain tracking. FDA staff uses SPL data to conduct analyses intended to discover illegitimate products (which may include drugs that are adulterated, mislabeled, stolen, counterfeit, or damaged/degraded).

FDA also uses the system to: (1) facilitate SPL submission compliance verification and corrective action tracking; (2) host CDER Direct application administrative components (used to control CDER Direct user access and for auditing and monitoring of the use and access of CDER Direct); and (3) generate data sets of drug establishment registrations and drug listings, which may be made available to the public and which may include PII for points of contact (POCs) of regulated entities.

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

DQCP contains information submitted electronically by drug manufacturers and resellers, including information in the SPL format. This information is submitted electronically through many resources including FDA's Electronic Submission Gateway (ESG) and CDER Direct, which are covered under their own separate PIAs. In the near future some types of submissions will be made via the FDA Universal Registration and Listing System (FURLS) as well. These submissions pass through the CDER Electronic Listing (ELIST) system, which validates the information against a data repository for accuracy, and then into a DQCP database. Once in DQCP, SPL data is parsed into corresponding tables, and the data is then available for authorized FDA staff to perform data searches and retrievals, mainly to permit staff to conduct drug quality and compliance control.

Data collected in DQCP relates to drug labelers and submissions from particular drug sponsors requesting assignment of unique identifiers of drug sponsors called "drug labeler codes." Other data is related to required annual registrations of drug establishments (including generic drug facilities, compounders, WDDs, and 3PLs); drug labeling and listing; generic drug facility annual registration; generic drug facility fee payment status; compounder drug semi-annual reporting; compounder fee payment status; wholesale drug distributors (WDDs) annual reporting; and third party logistics provider (3PLs) facilities, licensing and annual reporting.

The information collected includes manufacturers' Data Universal Numbering System (DUNS) and Facilities Establishment Identifier (FEI) numbers (neither of which ever identify an individual, only institutions such as manufacturers), contact person's names, business e-mail addresses, and business phone numbers; registration information (i.e., DUNS number, organization name, contact person's name, work e-mail and work phone number); drugs listing information (e.g., ingredients, packaging of the drugs, and approved usages of specific drugs); and license information (i.e., license numbers, expiration date, significant disciplinary action conducted against license holders).

The security questions users answer as part of the registration process may contain PII, but the answers are stored in the database encrypted. The only person can view the answer is the person who answered questions via his/her CDER Direct application user profile editing page. The question and answer data is not viewable from any DQCP application web page.

FDA staff access the system using a single sign on (SSO) approach and there is no need for authorized users to enter authentication information. DQCP contains reference PII to automatically authenticate FDA users. DQCP also contains a user table to govern role-based access that includes user e-mail addresses.

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

FDA uses DQCP for functions related to requirements of the DSCSA. The following information is collect, maintained, and shared with authorized FDA staff:

Information on labeler code assignments, including which labeler code is assigned to which drug sponsor; labeler contact information key dates related to the assignments; and, names of FDA staff members that made each assignment.

Manufacturer facility information including each manufacturer's or facility's point of contact information.

Information concerning individual compliance cases. If drug manufacturers submit SPL requests that are not compliant with FDA policy or that include inaccurate information, FDA will open a case and record all communications and actions taken (including corrective action taken by the manufacturer or other sponsor), including dates.

DQCP Authorized FDA user registration information and event logs. The user registration information include user's organization and e-mail.

CDER Direct industry user registration information includes the user's organization, e-mail, phone, security challenge questions and answers (this may include biographical information linkable to the individual), and user access privileges. CDER Direct event logs contains detailed information about system use, such as which user took specific actions and the time of each. CDER Direct configuration updates acceptable SPL terminologies to support user data entry verification; this is used, for example, to ensure that only acceptable terminologies will be allowed.

Generic drug manufacturer facility information and point of contact information. Also WDD/3PL licensing information. Drug label and listing information including ingredients and associated manufacturers (both of which may be confidential, and this information is only accessible to privileged FDA users).
Compounded drug information including ingredients, the time when the compound was produced, and the quantity produced.

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

Industry points of contact submit PII including name, address, phone, and e-mail.

Dun & Bradstreet (Data Universal Numbering System (DUNS) number). Usually a DUNS is for a business, but can refer to an individual in their entrepreneurial capacity.
A "Facilities Establishment Identifier" (FEI) could be used to identify the work address of an individual contact, but this information is normally also provided directly.
Access and authentication information for FDA users, including work e-mail,work phone, and user-supplied information, but not a username or password.

Security questions may include PII, such as biographical information about the individual that they would know well.

Security Answers are encrypted within DQCP.

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

Employees

Public Citizens

Public Citizens are the manufacturers' or drug sponsors' points of contact. Employee information is authentication information as described above.

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Information collected is used for the purpose of maintaining FDA mandated manufacturer annual registration and to communicate with manufacturers concerning reminders about annual registration and statements of noncompliance.

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.

Federal Food, Drug and Cosmetics Act; 21 U.S.C. Sections 360(b)-(f), (i), (p); and the Drug Supply Chain Safety Act (DSCSA), (21 U.S.C. 581 et seq.).

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

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

OMB No. 0910-0045, expiration date is December 31, 2018.

Is the PII shared with other organizations?

Yes

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

Private Sector

WDD and 3PL data is made available to the public via the FDA public web site. The only PII included is professional contact data (name, e-mail and telephone number).

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

None.

Describe the procedures for accounting for disclosures.

Because this information is not retrieved by any individual's name or other unique identifier

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

The Federal Food, Drug, and Cosmetic Act, FDA regulations, and guidance published on the FDA website all inform the public that manufacturers are required to provide a point of contact and include that individual's business address, e-mail, and telephone. These materials also detail the requirement that FDA make copies of registration submissions available for public viewing and are available on www.fda.gov (for example, see 21 U.S.C. 360(f) and 21 CFR 207.37).

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 the POC's information is "voluntary" as contemplated by the Privacy Act of 1974, but entities are required to register. Entities are required to submit contact information for communication and compliance tracking purposes. Failure to register may result in penalties for an entity, although not for any individual POC.

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

If FDA’s privacy practices change or FDA changes its collection, use, or sharing of PII data in the system, the individuals whose PII is in the system will be notified by the most efficient and effective means available and appropriate to the specific change(s). This may include a formal process involving written and/or electronic notice, or informal processes such as 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.

Submitters may contact FDA by e-mail to resolve any issues regarding their PII information, and may resubmit information or corrections to their PII.

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

CDER users routinely review the information. Any data problem caused by the system will be reported and the system maintenance team will fix the problem following FDA standard IT system maintenance practices. If the data is entered incorrectly by an industry submitter, CDER will contact the submitter to request a correction and re-submission.

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

Users:

Access is needed for drug review, drug imports, drug safety, and drug compliance.

Administrators:

Administrators need to have complete access for system operation monitoring, troubleshooting, and auditing the integrity of the data.

Contractors:

Only authorized system maintenance direct contractors have access to PII data to troubleshoot possible data issues.

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

PII in DQCP is available to all FDA employees through the intranet. The PII within this data consists of the manufacturer's representative's contact information (which includes business/work contract information only).

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.

Personnel in offices across the agency require access to the limited business contact PII that is collected in the system. Because no other PII is collected or maintained in the system, these users are effectively limited to accessing the minimum amount of PII necessary to perform their 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 FDA system users complete annual FDA information security and privacy awareness training. This training is similar in scope and content to HHS's Annual Privacy and Security service trainings.

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

Users review the Rules of Behavior and warning notices when logging onto the FDA network. No additional specific security/privacy oriented training is provided. Users may obtain additional privacy guidance upon request via FDA's privacy office.

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 system information retention guidelines include FDA File Codes 7220 (Registration and Listing Systems, NARA N1-88-07-2), FDA File Codes 7221 (for Input Records, GRS 20-2a, 2b), and FDA File Codes 7222 (for Database Records, N1-88-07-2). Records are retained for ten years after a firm goes out of business or the product is no longer marketed "or when no longer needed for legal, research, historical or reference purposes, whichever is later."

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

DQCP staff have implemented the baseline controls listed in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3 controls. Any deficiencies are documented and addressed via the agency’s management process. Further specific details about security controls have been established through the system accreditation process.

Submission files are stored in a restricted access environment protected by physical controls including that all system servers are located at FDA facilities protected by guards, locked facility doors, badge requirements and climate controls. Technical controls include firewall and system user access controls using PIV card based Citrix environment access.