US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/23/2016

OPDIV:

HRSA

Name:

OPA Compliance Tool

PIA Unique Identifier:

P-5265600-919402

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

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)?

No

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

Describe the purpose of the system.

The basic purpose of OPA Compliance Tool (OPACT) is to provide the latest known compliance information about a Covered Entity (CE), pharmaceutical manufacturer, or pharmacy in an integrated and organized fashion so that OPA staff can provide the best service to the customer, to the public, and to the government. The other objective of the system is to significantly increase customer satisfaction, increase the quality of HRSA decisions, and considerably reduce the time necessary to resolve customer issues.

All of this leads to process automation of the following work-flows:

1. HRSA CE Audit
2. HRSA Manufacturer Audit
3. Manufacturer CE Audit
4. Self-Disclosure/Allegation Audit
5. Correspondence Response

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

The types of information processed are:

1. Covered Entity (CE) or Manufacture ID - Name, address contact person info, which includes name, business email address and business phone number
2. Work-flow status and documents associated with the work flow. Work flow includes audit document receipt, response to the document, and final audit letter from the OPA Director to the audited entity.
3. Electronic Signature of OPA Director

(Note: Other OPA user information is used from Active Directory).

4. At present OPA grants access to the OPACT system to Federal employees of HRSA only.
5. The system uses HRSA's Active Directory to grant access to the system. Additionally, the system will enforce PIV card login by September, 2017. The System administrator, a Federal employee of OPA, grants roles to each user account to control access to the various functions of the system.

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

The system is mainly designed to integrate and automate the following work-flow processes carried out by OPA.

1. HRSA CE Audit
2. HRSA Manufacture Audit
3. Manufacturer CE Audit
4. Self-disclosure and Allegation Audit
5. Correspondence Request Processing

The system maintains information like:

1. Audit/Compliance information:

a. Covered Entity (CE) or Manufacture ID: we need to track what entity is being audited.
b. Type of Audit: we need to know the type of audit being conducted so that we can use the appropriate business process.
c. Status of the Audit: we need to know where we are int he audit process.
d. Documents associated with audits: we need the documentation to analyze the audit results.

2. Identification information for any given CE or Manufacturer or Pharmacy.

a. CE/Manufacturer name and address: we need to know how to contact the entity.
b. Authorizing Officer's contact information: we need to know who is responsible for attesting to the accuracy of data given to us by the entity. We also need to contact them if there are issues.
c. Contact Person's contact information: We need to know with whom to work at the entity as we do the audit.

3. Internal User Information

a. Name, Email address from Active Directory: the system sends emails to users when they are given a task in the system.
b. Electronic Signature of OPA Director: the system generates audit letters that must be signed by the OPA Director.
c. The system also stores the roles that each user (person) has in it. Roles determine what the user can do and see in the system. The system requires and tracks user credentials.

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

Signature

User Credentials

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose for PII is for identifying and contacting a given OPA staff or CE, Manufacturer or Pharmacy.

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

Not Applicable

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

Section 340B (a)(5) (C) requires covered entities to submit to audits, section 340B (d)(1)(B)(v) authorizes selective auditing of drug manufacturers and wholesalers, section 340B (d)(3) requires the establishment of a process of formal administrative dispute resolution.
OPA cannot perform any of these functions without collecting audit and contact data.

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

No

N/A

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

0915-0327, expires 09/30/2018

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.

There is no process in place to notify individuals that their personal information will be collected. The PII information used by the system is because of the person's role in the organization and is public information. All the PII collected by this system are voluntary and individual is well aware of where and when or why his/her information is used. The address and emails of contact persons of the CE and Manufacturer are public information. Also all the information like Name, Address, Email id for a OPA employee is received from active directory maintained by HHS. The only PII this system collects is the signature of the individual which is voluntary and not mandatory.

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.

The PII this system collects is the signature of the individual which is voluntary and not mandatory. The individual is the Director of the Office of Pharmacy Affairs. This signature is used in the communication which goes out of the OPA agency to any of the Covered Entities or Pharmacies or Manufacturers. The user can opt out of automatic signing of the document by the system and provide the ink signature as required. The Director of Pharmacy Affairs must click a button in order for the system to create a letter containing her digitized signature. She can, instead, print an "unsigned" letter and sign it manually before sending it out.

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

Any requirement for changes made to the system on data usage or disclosure will come from the user . So all the user need to provide consent and are well informed about these changes if any. Systems administrators access the system via the HRSA Active Directory permissions and by Personal Identity Verification (PIV) card. The system assigns administrative rights based upon the AD account. Any changes to the way systems administrator data is handled or disseminated is through the Configuration Control Board (CCB) for OPACT. The systems administrator is a member of the CCB, and therefore will have a direct say as to the disposition of his data.

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.

The OPA Information System Security Officer (ISSO) and Assistant ISSO will investigate and address any concerns about PII handling and respond to the individual. OPA does not anticipate a large number of issues, since the individuals enter their own PII into the system. The PII obtained is "Public" information - the work email address for an employee of a covered entity or manufacturer. The systems administrator's data is part of the HRSA Active Directory General Support System, we inherit their processes for dealing with 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.

The information of the users is cross verified with HHS active directory every-time the user logs into OPACT. All the information about Covered Entity, Manufacturer or Pharmacy is refreshed every day and is loaded into OPACT form 340B Registration system. The PII associated with HRSA Active Directory accounts is covered by the HRSA GSS.

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

Users:

Part of the job is to review the information. Users only review their own information. (System Administrator of this application is a special user.)

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

Data access is based upon roles in the system. Role assignments determine access to data. There is a user form and associated authorization process where OPA determines who gets what role.

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.

OPACT system has role based access control in place. The information accessible by each role is different and is limited to the information necessary to perform their jobs.

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 user is provided and need to accept the Government property or information usage terms and condition policy at login. Users who have access to PII are all HRSA employees, who must go through privacy and IT security training.

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

Users receive hands-on training specific to their assigned roles.

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.

DAA-0512-2014-0004-0134. Temporary. Cut off at end of calendar year. Destroy 10 year(s) after cut off.

We follow National Archives and Records Administration (NARA) guidance. In addition, the system does not accept PII contained within audit materials. If, in the course of an audit, the CE or Manufacturer sends PII, OPA rejects the submission and asks for redacted materials containing no PII. OPA immediately destroys (shreds) any submitted materials containing PII.

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

Technical:
Access to OPACT system and to its data is restricted to:
1) Internal user defined in the Active Directory and authenticated by Personal Identity Verification card.
2) User having a specific role defined in the OPACT system

Administrative
Also user is provided and need to accept the Government property or information usage terms and condition policy at the start of session using OPACT.

Physical
Servers containing the data are in the Sterling Data center, part of the HRSA GSS, and they inherit the GSS controls for physical protection of the data (guarded, ID badges, key cards, etc.)