PTA / PIA: HRSA - 340B OPAIS - QTR2 - 2025 - HRSA1438755

Created Date: 8/7/2025 8:21 AM Last Updated: 11/20/2025 3:26 PM

General Information

PTA / PIA Name:	HRSA - 340B OPAIS - QTR2 - 2025 - HRSA1438755	**PTA / PIA ID:**	3613647
Component Name:	HRSA - 340B OPAIS	**ATO Boundary Name:**	340B OPA Information System
Overall Status:	Complete	**# of Days - Open:**	150
Submitter:		**Submit Date:**	8/20/2025
Next Assessment Date:	11/19/2028	**Expiration Date:**	11/19/2028
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	No	**PIA Required:**	Yes

General 01:	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
General 02:	Is this a FISMA-Reportable system?	Yes
General 03:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	Yes
General 04:	ATO Date or Planned ATO Date.	4/10/2024
General 05:	Is the system or electronic information collection, agency or contractor operated?	Contractor
History Log:	View History Log	

Privacy Threshold Analysis

Privacy Threshold Analysis

PTA 01:	Point of Contact (POC) Name	Yi Yu
PTA 01A:	POC Title and Organization	ISSO Office of Pharmacy Affairs
PTA 01B:	POC Email Address	yyu@hrsa.gov
PTA 01C:	POC Phone Number	301-443-4384
PTA 02:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA 02A:	Describe in further detail any changes to the system that have occurred since the last PIA.	The system will be migrated to the Azure Cloud

PTA 03:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA 04:	Please give a brief overview of the purpose of the system by describing what the functions of the system are and how the system carries out those functions in support of HHS.	The Office of Pharmacy Affair (OPA) is responsible for the administration of the 340B Program. The OPA has established the 340B OPAIS to respond to the needs created by the 340B Drug Program; the 340B OPAIS is a three-part system containing a registration module that manages the participation of entities, manufacturers and pharmacies in the 340B program, a confidential pricing module that contains proprietary information used to calculate and publish discounted drug prices, and an internal workflow for compliance activity tracking. The purpose of the system is three-fold; first, the system tracks Covered Entities (Covered Entities are healthcare providers such as certain types of Hospitals, Ryan White AIDS clinics, Community Health Centers, etc.) who participate in the 340B drug program. It is the official federal repository for information on the health care organizations, contracted pharmacies and pharmaceutical manufacturers that are participating in the 340B Drug program. The system has a registration module, where Covered Entities can register (apply) to participate in the 340B program, make changes to their data, and perform annual recertification of their data. The registration module makes the Covered Entities' membership status available to the public. Drug manufacturers use this data to determines who is eligible to receive 340B Drug program discounts. Drug manufacturers also enter similar data (contacts, addresses) into the registration module. The registration module creates user accounts based upon the Covered Entity and the Manufacturer data. The Registration Module has additional functionality in support of a mandated administrative dispute resolution (ADR) process for covered entities and manufacturers that have been unable to resolve disputes over drug pricing and purchase eligibility. Second, the pricing module is the sole official federal source for "340B ceiling prices", which are the highest prices that manufacturers and wholesalers can legally charge an eligible health care entity that has been accepted into the program (also called a "covered entity"). The pricing module is an external application that calculates "ceiling prices" based on information supplied by pharmaceutical manufacturers, the CMS, and a commercial data broker. This data is only available to 340B Covered Entities and drug manufacturers. The pricing module includes functions to reconcile pricing data from CMS and data from drug manufacturers to calculate correct 340B ceiling prices, that are made available to authorized system users. Third, the Compliance module 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 OPA decisions, and considerably reduce the time necessary to resolve customer issues. All of this leads to process automation of the following workflows: 1. CE Audit 2. Manufacturer Audit 3. Manufacturer CE Audit 4. Self-Disclosure/Allegation Audit 5. Correspondence Response Protected Health Information (PHI)/Personal Identifiable Information (PII) is not requested while performing 340B audits of covered entities and manufacturers. Some patient PHI, a form of PII, is inadvertently collected or contained in drug audit information. When such files are detected, they are removed and purged from the system.
PTA 05:	List and/or describe all the types of information that are collected, maintained, and/or shared by the system regardless of whether that information is PII and how long that information is stored.	The 340B OPAIS system will collect email addresses, work telephone numbers, and authorizing official and primary contact person's names in the registration module as well as information about the Hospitals, Clinics, and other Covered Entities, such as shipping addresses and Hospital financial data. The system also collects the equivalent data - email addresses, work telephone numbers, and physical addresses, from Manufacturers. The system uses PII information to create user accounts for those that will be accessing the registration module to enter changes to Covered Entity data, such as shipping addresses, Contract Pharmacies, etc., and to grant both Manufacturers and Covered Entities access to the pricing module. No SSN/Taxpayer ID is intentionally collected. At times a SSN may be inadvertently submitted during an audit of a covered entity or drug manufacturer due to information not being redacted prior to uploading documents into the compliance module of the 340B OPAIS. If, during an audit, the CE or Manufacturer sends the PII, OPA rejects the submission and asks for redacted materials without PII and deletes the submission. The registration module collects the Covered entity and Manufacturer data listed in the paragraph above. OPA uses the data in the registration module to determine whether a Covered Entity is eligible to participate in the 340B program. The registration module uses HHS' Access Management System user data to Identify Authenticate and Authorize (via Personal Identity Verification - PIV - card at IAL 3 and AAL 3) access to the specific functions in the system for Office of Pharmacy Affairs (OPA) (i.e., non-public) users. The system does not collect any OPA user PII that is not required for PIV card use. The Pricing module will also collect the following data from the drug manufacturer- National Drug Code, Package size, Average Manufacturer Price, Unit Rebate Amount, Unit Type, FDA product

		name, Wholesale Acquisition Cost, manufacturer-determined ceiling price, and Labeler name. The Pricing module also holds the following data provided by CMS's Medicaid Drug Rebate Program: Drug category, Drug Type, product termination date, Units per package size, FDA approval date, Market date, Therapeutic Equivalence code, Clotting factor indicator, pediatric indicator, package size intro date, purchased produce date, Covered outpatient drug status, FDA application number/OTC monograph number, reactivation date, line extension drug indicator, and missing data indicator flag. The Compliance module will collect the following data: 1. Covered Entity (CE) or Manufacturer ID - Name, address contact person information, which includes name, business email address and business phone number 2. Work-flow status and documents associated with the workflow. Workflow includes audit document receipt, response to the document, and final audit letter from the OPA Director to the audited entity. 3. At present OPA grants access to the Compliance system to Federal employees of OPA only, uses HHS' Access Management System user data to Identify Authenticate and Authorize (via Personal Identity Verification - PIV - card at IAL 3 and AAL 3) 4. The System administrator, a Federal employee of OPA, grants roles to each user account to control access to the various functions of the system. 5. CE program information including: policies and procedures, Medicare cost report, lists of 340B drug dispenses, individual health records, proof of CE staff employment, lists of CE's wholesalers and 340B drug purchase orders including price paid, lists of contract pharmacies and the current contracts, lists of all accounts used to purchase drugs, lists of Medicaid billing numbers and NPI numbers, contracts with a State or local government to provide health care services to low income individuals, Notice of Grant Award (NGA) or sub-grantee documentation. No PHI data is contained in an audit report. Medical record numbers are collected in order to identify a drug dispensed to a patient on a given date in the covered entity's Electronic Health Records (EHR).
PTA 05A:	Are user credentials used to access the system?	Yes
PTA 05B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Username Password Email Address
PTA 06:	Describe why each type of information is collected, maintained, and/or shared by the system. Specify what information is collected about each category of individual.	Below are the classes of users for the system and the explanation for collecting the data from them. i. Covered entities – will have access to calculated and verified 340B ceiling prices. To ensure that we

are granting access to the appropriate person due to the sensitivity of the data, we collect their name, work title, work phone number, and the associated Covered Entity (Hospital, health center, etc.) information, and Rules of Behavior form.

ii. Manufacturers – we collect the same information mentioned above for the Covered entities. Additionally, the manufacturers have to submit the following drug pricing data points which are used to compare the manufacturer's ceiling price against OPA's calculation. The data points are- Average Manufacturer Price, Unit Rebate Amount, package size, National Drug Code, and manufacturer-determined ceiling prices.

iii. OPA staff – will have a mechanism to accept ceiling prices submitted by manufacturers and compare them to prices calculated by OPA using Centers for Medicare &Medicaid Services (CMS) pricing data. When discrepancies exist, the 340B OPAIS will enable reporting functions that assist OPA with monitoring and compliance enforcement. OPA staff will also have a mechanism to approve or reject Covered Entity registrations to the 340B program.

No SSN/Taxpayer ID is intentionally collected. At times a SSN may be inadvertently submitted during an audit of a covered entity or drug manufacturer due to information not being redacted prior to uploading documents into the compliance module of the 340B OPAIS. If, during an audit, the CE or Manufacturer sends the PII, OPA rejects the submission and asks for redacted materials without PII and deletes the submission.

The compliance module is mainly designed to integrate and automate the following work-flow processes carried out by OPA. 1. CE Audit 2. Manufacturer Audit 3. Manufacturer CE Audit 4. Self-disclosure and Allegation Audit 5. Correspondence Request Processing The system maintains information: 1. Audit/Compliance information: a. Covered Entity (CE) or Manufacturer 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 in the 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: 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.
PTA 07:	Does the system collect, maintain, use, or share PII?	Yes
PTA 08:	Does the system include a website or online application?	Yes
PTA 08A:	Provide the URL(s).	https://340bopais.hrsa.gov https://340bregistration.hrsa.gov https://340bpricing.hrsa.gov https://340bpricingsubmissions.hrsa.gov https://internal-340b.hrsa.gov
PTA 08B:	Are any of the website or online applications accessible by the public (including publicly accessible log in pages)?	Yes

PTA 09:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	The 340B OPAIS public site allows manufacturers and wholesalers to verify that an organization requesting 340B pricing is an active participant in the 340B program. The public 340B site has anonymous access, so that anyone who can access the internet can access the site. There is no login required. The URL is https://340bopais.hrsa.gov/ The 340B Participant site allows representatives of health care organizations and drug companies who want to participate in the 340B program to create an account in OPAIS and submit registrations during published intervals for review and approval by OPA staff. After registration approval, the representatives access the registration site periodically to update, terminate and maintain their 340b participation. The URL is https://340Bregistration.hrsa.gov/ The 340B Pricing CE site allows representatives from the covered entities participating in the 340B program to access the approved and published ceiling prices of products in the 340b program. The URL is https://340bpricing.hrsa.gov/ The 340B Pricing Manufacturer site allows representatives from the drug manufacturers participating in the 340B program to submit prices for products in the 340b program and work with OPA to calculate the quarterly ceiling prices for their products. The calculated prices are considered non-public information due to the proprietary nature of some of the underlying data. Calculated ceiling prices can only be viewed by selected OPA staff and authorized staff of manufactures/covered entities currently participating in the 340B Program with secure access. The URL is https://340bpricingsubmissions.hrsa.gov/ The OPAIS Internal site is accessible only by internal OPA staff with defined security roles to administer and manage the 340B program. The internal users access the Registration module to review and manage the registrations of the 340B participants. The 340B OPAIS Pricing module is an official federal source for 340B ceiling prices. The internal OPA users collaborate with drug manufacturers to calculate ceiling prices based on information supplied by manufacturers, the Centers for Medicare and Medicaid Services (CMS), and a commercial data broker. Calculated ceiling prices can only be viewed by selected OPA staff and authorized staff of manufactures/covered entities currently participating in the 340B Program with secure access. The URL for the Internal OPAIS site is not accessible from Internet and is only available on the HRSA Intranet. The URL is https://internal-340b.hrsa.gov/
PTA 10:	Does the website have a posted privacy notice?	No
PTA 11:	Does the website contain links to non-federal government websites external to HHS?	Yes

PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	No
PTA 12:	Does the website use web measurement and customization technology?	Yes
PTA 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	Session Cookies- Does Not Collect PII
PTA 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA 14:	Does the system have a mobile application?	No
PTA 20:	Are any third-party websites or applications (TPWA) associated with the system?	No
PTA 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

Privacy Impact Assessment

Privacy Impact Assessment

PIA 22:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Identifying Numbers Social Security Number Taxpayer ID Number (TIN) Biographical Information Name Date of Birth Contact Information Email Address (Business) Phone Numbers (Business) Medical Information Medical Records
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Business Partners/Contacts (Federal state, local agencies) Employees/HHS Direct Contractors Grantees Patients Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors)
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	50,000 – 99,999
PIA 25:	For what primary purpose is the PII used?	Names, work email and work telephone numbers for covered entity (CE) and manufacturer contacts/authorizing officials for Registration and Pricing modules. These modules are used to create user accounts for those accessing both the pricing and registration systems for business purposes only. The primary purpose of PII for the Compliance module is to identify and or provide contact information for OPA staff. Additionally, contact information for CE's, Drug Manufactures, and contract pharmacies may be used to determine eligibility for the 340B Drug Program.

PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	No
PIA 27:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses include that in your response.	At times a SSN/Taxpayer ID may be inadvertently submitted during an audit of a covered entity or drug manufacturer due to information not being redacted prior to uploading documents into the compliance module of the 340B OPAIS. OPA does not programmatically use SSN for any purposes.
PIA 27A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID. If the Taxpayer IDs collected are only for businesses, you may respond N/A.	We do not use the SSNs/Taxpayer ID.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Section 340B(d)(1)(B)(iii) of the Public Health Service Act requires the "provision of access through the Internet website of the Department of Health and Human Services to the applicable ceiling prices for covered outpatient drugs as calculated and verified by the Secretary in accordance with this section, in a manner (such as through the use of password protection) that limits such access to covered entities and adequately assures security and protection of privileged pricing data from unauthorized re-disclosure". We established and continue to maintain the 340B database based on the following provisions: 340B(a)(9) Notice to Manufacturers: The Secretary shall notify manufacturers of covered outpatient drugs and single State agencies under section 1902(a)(5) of the Social Security Act of the identities of covered entities under this paragraph, and of entities that no longer meet the requirements of paragraph (5) or that are no longer certified pursuant to paragraph (7). The collection of personally identifiable information is limited only to collecting contact information only in their business capacity from participating covered entities and manufacturers. Section 340B of the Public Health Service Act has numerous requirements including the registration of covered entities, provision of information about the covered entities and signing of Pharmaceutical Pricing Agreements by Manufacturers that require the identification of an authorized official who has authority to register and change data in the database. OPA is required to verify the accuracy of the information and has ongoing verification of the information contained in our database. All forms used to collect information are included on forms approved by OMB. 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.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	No

PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Email Online Government Sources Within the OPDIV Other HHS OPDIV Other Federal Entities Non-Government Sources Members of the Public Private Sector
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Number: 0915-0327, Expiration: 01/31/2026
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	Yes
PIA 32A:	Identify with whom the PII is shared or disclosed.	Other Federal Agency/Agencies
PIA 32B:	For each disclosure, name the organizations/systems the system shares PII with and the purpose(s) of the disclosure.	OPA's Prime Vendor, which currently is Apexus supports OPA Help Desk in assisting external users.
PIA 32C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	We have 340B Prime Vendor Agreement between OPA and Apexus, LLC.
PIA 32D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	All PII Apexus accesses is public PII. Apexus does not disclose PII nor do they have access to the internal part of 340B OPAIS that may contain PII. Our agreement with Apexus outlines what can/cannot be done with information shared. So there is no process in place.
PIA 33:	Is the submission of PII by individuals voluntary or mandatory as defined in the Privacy Act?	Voluntary

PIA 34:	Describe the method in place to notify and obtain consent from individuals whose PII will be collected. If no prior notice is given or consent cannot be obtained, explain why.	The method for the covered entities (i.e. health centers, hospitals, etc.) to change/terminate from the program is done via a change or termination request. Consequently (per entity's request) their point of contact and or authorizing official's PII (e.g. name, email, phone number, etc.) will be updated and or removed from OPA's website. The email addresses are used to create user accounts for the participating stakeholders to assist them in performing the functions required by law. If they object to the submission of their email address, this will prevent them from fulfilling this requirement. The same process is applicable to drug manufacturers as well with the exception to the termination process which is specified in the pharmaceutical pricing agreement. For the Compliance module, there is no process in place to notify individuals that their personal information will be collected in any capacity nor stored in any government IT system. The PII information used by the system only identifies the person's role in the organization. All the PII collected by this system is voluntary and an individual is well aware of how and why their information is used. The names, addresses and emails of contact persons of the covered entity and Manufacturer used in Compliance module are public information and accessible from the 340B OPAIS external sites. Also all the information collected in the system that includes Name, Address, Email ID for an OPA employee is maintained by HHS. Some patient PHI, a form of PII, is inadvertently collected or contained in drug audit information. There is no mechanism to notify patients when PHI has been collected. The goal of OPA is to not collect any PII from patients in our system. If PII is found, OPA works directly with the auditor to request new data that does not include PII; however, not all PII collected as part of an audit is immediately identified. If the information is accidentally collected, it will not be shared with any other entities and removed as soon as possible. Any additional collection of PII/PHI is unintentional and incidental.

PIA 35:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). If they cannot be notified or have their consent obtained, explain why.	There is no process in place to notify and obtain consent from individuals when major changes occur to the system because the PII information that the application uses is publicly available and accessible to the general public. For the Compliance module, the collection of any patient PII/PHI incidentally is unintentional and therefore no mechanism has been set up to obtain consent or provide notification as this PHI is not used or shared.
PIA 36:	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. If no process exists, explain why not.	The authorizing official (AO) and Primary Contacts (PC) are the only persons for the 340B covered entities that submit their name, telephone number and email to register their organization. The AO and PC can submit an OMB approved change request form to correct inaccurate information in the 340B database. There is no formal process in place to address an individual's concerns when they believe that their PII has been inappropriately obtained, used, or disclosed. All PII is publicly available and individuals are notified that their PII is publicly available and thus can be accessed, used, or disclosed by any member of the public. The OPA Information System Security Officer (ISSO) will investigate and address any concerns about PII handling and respond to the individual inquiry as needed. 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 agency's Active Directory General Support System, we inherit their processes for dealing with PII issues.

PIA 37:	Describe the process in place for periodic reviews of the system to ensure the integrity, availability, accuracy, and relevancy of the PII in the system. Please address each element in your response. If no processes are in place, explain why not.	The PII information collected in this application consists of name, work telephone numbers and email which are provided by the applicants. This information is collected for administrative reasons only. Covered entities are encouraged to maintain accurate information on the database. OPA staff verify each application for accuracy to ensure that covered entity eligibility and program integrity is maintained. OPA staff also conduct annual recertification of all cover entities to ensure that each meets the program requirements. The recertification process also includes validation of participant's information. For internal applications, the information of the users is cross verified with HHS active directory every time the user logs into the system. The PII associated with agency's Active Directory accounts is covered by the agency's GSS. Any incidental PHI/PII is received from covered entities through Secure Email and File Transfer (SEFT). Once identified during the review process, the covered entity will be asked to re-submit with PHI/PII redacted.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors Others
PIA 38A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA 38B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA 38C:	Identify the additional person(s) who will have access to the PII in the system not mentioned in the list above.	None

PIA 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users - Access to limited PII (names/telephone numbers) for program operations in accordance with agency/program rules of behavior. Administrators - Access to limited PII (names/telephone numbers) for program operations in accordance with agency/program rules of behavior. Administrators also need access in order to manage, create or delete accounts. Developers - Access to limited PII (names/telephone numbers) for program operations in accordance with agency/program rules of behavior. Additionally, they might need access for testing purposes. Contractors - Access to limited PII (names/telephone numbers) for program operations in accordance with agency/program rules of behavior. Others - Names and telephone numbers are available to the public.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	OPA has Identification, Authorization, and Authentication standard operating procedures for 340B OPAIS system. All users that have access to PII are internal OPA users. OPA users must sign an HHS and OPA Rules of Behavior contract and must have a user account request form signed by the system owner, the business owner, and the Information System Security Officer (ISSO) before they can access the system (via PIV card authentication). The user form identifies which authorized roles each user has in the system. Each role has different access rights and permissions in the system. Per NIST (and HHS) guidelines, OPA ISSO conducts quarterly audits of its internal user accounts, rules of behavior, and user request forms to ensure that user access rights are current and appropriate. 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.

PIA 41:	Describe the technical methods in place to allow those with access to PII to access only the minimum amount of information necessary to perform their job.	340B OPAIS has user roles associated with each type of user - public, Covered Entity, Manufacturer, Office of Pharmacy Affairs, Administrators, etc. Each user role has limited rights to see data and perform functions in the system, depending upon the requirements of their job. Covered Entities only have access to their own data as each covered entity account is associated with a particular covered entity. Similarly, Manufacturers only have access to their own data. Public users only have access to publicly available data. OPA users must sign a HHS and OPA Rules of Behavior and must have a user account request form signed by the system owner, the business owner, and the Information System Security Officer (ISSO) before they can access the system (via PIV card authentication). The user form identifies which roles each user is authorized to have in the system. Each role has different access rights and permission in the system. Per NIST (and HHS) guidelines, OPA conducts quarterly audits of its internal user accounts, rules of behavior, and user request forms to ensure that user access rights are current and appropriate. 340B OPAIS 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.
PIA 42:	Identify the general security and privacy awareness training provided to system users (system owners, managers, operators, contractors and/or program managers) to make them aware of their responsibilities for protecting the information being collected and maintained.	Everyone accessing the system is required to take the "HHS annual IT security and privacy awareness training".
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	None
PIA 44:	Describe the process and guidelines in place for the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	The PII is only retained as long as it is in use. Following the General Records Schedule 1.2, the records in the 340B OPAIS which are terminated for more than 10 years will be deleted permanently from the system. For Compliance, the system does not accept PII contained within audit materials. If, in the course of an audit, the CE or Manufacturer sends the PII, OPA rejects the submission and asks for redacted materials without PII. OPA immediately destroys (deletes) any submitted materials containing PII.

PIA 45:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.	Administrative control: 340B OPAIS uses Role Based Access Control (RBAC): Non-organizational users get their roles based on the currently reviewed and approved registration records. A user is considered an Authorizing Official (AO) if their account is the current authorizing official on an active and approved record. The same applies to Primary Contacts (PC). Organizational users who access to the system must be approved by the system owner, business owner and the Information System Security Officer (ISSO). Technical control: 340B OPAIS is multi-tier architecture where the presentation layer is separated from the business logic/rules and database. All traffic to the database is encrypted. In addition, the database is encrypted to protect data at rest. Physical control: Servers containing the data are part of the GSS, and they inherit the GSS controls for physical protection of the data (guarded, ID badges, key cards, etc.)

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/4/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	15

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	10/2/2025
SOP Review Comments:		**# of Days - SOP Review:**	28

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	11/14/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 11/14/2025 All comments have been addressed. This PIA is ready for for SAOP review and approval. Reviewer: Shanai Shobowale 8/20/2025 Please see comments and update accordingly. PIA-22: Per PTA-5, please include the following PII elements "taxpayer ID (can inadvertently be collected per PTA-5), medical record number, and financial account information (per PTA-5 financial data is collected)." PIA-27: Per PTA-5, Taxpayer ID is also mentioned are they collected similar to SSN? PIA-27A: Would this be the same for Taxpayer ID?	**# of Days - APA Review:**	43

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	11/20/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	6

SAOP Signature

Date	User	Type	Name	Original Value	New Value
11/20/2025 11:28 AM	BAUR, VANESSA	Signature	SAOP (Email PIN)		Content Signed

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA 27A	BLAND, CRYSTAL	8/20/2025	Updated to include Taxpayer ID	
PIA 27A	BLAND, CRYSTAL	8/20/2025	Updated to include Taxpayer ID	
PIA 27A	BLAND, CRYSTAL	8/20/2025	Updated to include Taxpayer ID	
PIA 27A	VILLAFUERTE, NESTOR	8/20/2025	Updated to include Taxpayer ID	