PTA / PIA: HRSA - HDHP - QTR2 - 2025 - HRSA1445981

Created Date: 10/15/2025 8:23 AM Last Updated: 11/20/2025 3:26 PM

General Information

PTA / PIA Name:	HRSA - HDHP - QTR2 - 2025 - HRSA1445981	**PTA / PIA ID:**	3913431
Component Name:	HRSA - Hansen's Disease Health Portal	**ATO Boundary Name:**	Hansen's Disease Health Portal
Overall Status:	Complete	**# of Days - Open:**	143
Submitter:		**Submit Date:**	6/30/2025
Next Assessment Date:	11/19/2028	**Expiration Date:**	11/19/2028
Office:		**OpDiv:**	HRSA
Security Categorization:	Moderate		
Make PIA available to Public?:	Yes	**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.	6/3/2024
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	Reginald Ralph
PTA 01A:	POC Title and Organization	ISSO (HRSA)
PTA 01B:	POC Email Address	rralph@hrsa.gov
PTA 01C:	POC Phone Number	N/A
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 Hansen's Disease Health Portal (HDHP) has moved from initiation to operation and maintenance. A new FedRAMP component has been added to the system boundary. This new component has no impact on the PHI/PII collected, utilized, and stored by the HDHP. The proposed patient portal (https://hrsa.cyfluentphr.com/) is now accessible. Important to note, patients can only access their own data.
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 HDHP is an application used to collect, store, retrieve demographic and medical record data on patients treated for Hansen's Disease by the National Hansen's Disease Program. This will include Telehealth interactions with patients. Additional details are yet to be determined as project is in the design phase.
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.	Patient PHI for treatment of Hansen's disease as issuance of medication. The system is used to collect, store and share information related to patient demographics and medical records for in-house staff to provide service to the patient population served by NHDP. Demographic data consists of the following elements and is used to identify patients for accuracy of treatment: Name, DOB, SSN (last four), (Optional), Mother's Maiden Name (Optional), Mailing Address, Phone number and Email Address (Optional). Medical record data consists of the following elements and is used to document medical history, diagnosis and treatment to better monitor patient care and outcomes: Photographic Identifiers, Medical Records Number, Foreign Activities, Employment Status (Optional), medical notes, medical summaries and correspondence; EX: (Family to doctor, doctor to doctor, doctor to clinic).
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.	Patient PHI for treatment of Hansen's disease as issuance of medication. The system is used to collect, store and share information related to patient demographics and medical records for in-house staff to provide service to the patient population served by NHDP. Demographic data consists of the following elements and is used to identify patients for accuracy of treatment: Name, DOB, SSN (Last four), (Optional), Mother's Maiden Name (Optional), Mailing Address, Phone number and Email Address (Optional). Medical record data consists of the following elements and is used to document medical history, diagnosis and treatment to better monitor patient care and outcomes: Photographic Identifiers, Medical Records Number, Foreign Activities, Employment Status (Optional), medical notes, medical summaries and correspondence; EX: (Family to doctor, doctor to doctor, doctor to clinic).
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://hrsa.cyfluentchart.com/ (HDHP Link used by HRSA users and admins). https://hrsa.cyfluentphr.com/ (Patient portal link). https://hrsa.cyfluentphr.com/epp/Identity/Account/Login (External Provider Portal)
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.	https://hrsa.cyfluentphr.com/epp/Identity/Account/Login
PTA 10:	Does the website have a posted privacy notice?	Yes
PTA 11:	Does the website contain links to non-federal government websites external to 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 Truncated SSN Biographical Information Date of Birth Mother Maiden Name Employment Status/History Foreign Activities Contact Information Email Address (Personal) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Photographic Identifiers Medical Information Medical Records Medical Records Number
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Patients
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	10,000 – 49,999
PIA 25:	For what primary purpose is the PII used?	Assisting internal staff in the performance of duties by providing patient treatment for individuals with Hansen's Disease.
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	To provide data for use in facility management, continuing education, department initiatives, quality assurance activities, and research at the National Hansen's Disease Program in Baton Rouge, Louisiana.
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.	To provide data for use in facility management, continuing education, department initiatives, quality assurance activities, and research at the National Hansen's Disease Program in Baton Rouge, Louisiana.
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.	Section 320 of the Public Health Service Act, as amended (42 U.S.C. 247e), the National Hansen's Disease Program, section 326 of the Public Health Service Act, and E.O. 9397, as amended.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	Section 320 of the Public Health Service Act, as amended (42 U.S.C. 247e), the National Hansen's Disease Program, section 326 of the Public Health Service Act, E.O. 9397, as amended, and 09-15-0007, Patients Medical Record System Public Health Service Hospitals.
PIA 29:	Are records in the system retrieved by one or more PII data elements?	Yes

PIA 29A:	Please specify which PII data elements are used to retrieve records.	Records can be retrieved using the truncated SSN & name
PIA 29B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-15-0007, Patients Medical Record System Public Health Service Hospitals. https://www.federalregister.gov/documents/2009/08/03/E9-18439/privacy-act-of-1974-report-of-altered-systems-of-records
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Online Government Sources Within the OPDIV
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA 31B:	Explain why an OMB information collection approval number is not required.	Not applicable authorized under: Section 320 of the Public Health Service Act, as amended (42 U.S.C. 247e), the National Hansen's Disease Program; and section 326 of the Public Health Service Act.
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.	Authorized disclosure detailed within the SORN.
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)).	There are no information exchange agreements required or in place.
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.	Data from the HDHP is not disclosed to outside entities on a regular basis. However, when it is (i.e. Research) the data is de-identified prior to use. In the event of other disclosures (i.e. audit log disclosure) a detailed accounting of whom the information is disclosed to will be kept.
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.	Patients are provided the option to opt-out of the collection or use of their PII by refusing service offered by the program.
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.	Written notification must be sent to the National Hansen's Disease Program, which reasonably identifies the record, specifies the information to be contested, and states the corrective action sought with supporting justification.

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.	Written notification must be sent to the National Hansen's Disease Program, which reasonably identifies the record, specifies the information to be contested, and states the corrective action sought with supporting justification.
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.	Review of PII data elements contained in the system are conducted during each encounter starting from the first day of service provided and continuing with each subsequent event. During this process clinical staff trained in HIPAA and Privacy rules review and document demographic and medical record information as validated by the patient and staff at the time of service; all entries into the system are audited and captured as part of the permanent record. Upon confirmation of errors in the data, a request is submitted with supporting events attached to flag the entry as erroneous; the request is reviewed by a secondary staff member and the necessary action is taken upon verification.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Contractors
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 39:	Provide the reason why each of the groups identified in 38 needs access to PII.	Users - The users of the HDHP require access to PII to perform their job functions. Administrators - Require access to PII to successfully administer the HDHP. Contractors - Access to PII is required to ensure the successful operation of the HDHP.
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Supervisor initials and approves request for account creation to support job duties, and accounts are created with assigned internal role based controls that are based on identified job duties an audit logs.
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.	Role based controls are established within the system and assigned during account creation.
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.	Annual role based training and review at time of account creation and system access.

PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	HDHP Training is role-based. This will allow users to be trained based on assigned capabilities. The following are the roles that will be granted to NHDP personnel. Medical Assistants/Nurses: The Nurses or Medical Assistants treat patients at NHDP. They are trained in the use of the HDHP. The nurses use the HDHP to view patient medical history, document diagnosis, update patient record, order lab tests, attach lab test results and refer the patient to an NHDP specialist. Physicians: The Physicians at NHDP treat patients at NHDP. They are trained in the use of the HDHP. The physicians will use the HDHP to view patient medical history, document diagnosis, update patient record, order lab tests, attach lab test results and refer the patient to an NHDP specialist. Laboratory Personnel: The Laboratory personnel at NHDP are primary users of the HDHP. They are trained in the use of the HDHP. The Laboratory personnel are not experienced in using the HDHP EHR. The Laboratory personnel use the HDHP to order lab tests, attach lab test results. Pharmacists: The Pharmacists at NHDP are primary users of the HDHP. They are trained in the use of the HDHP. Most of the Pharmacists are not experienced in using a web based EHR. The Pharmacists will use the HDHP to order prescriptions, refill prescriptions and fill prescription orders. Administrators: The Pharmacists at NHDP are super users of the HDHP. They are trained in the administration of the HDHP. The Administrators will use the HDHP to maintain users, maintain data tables and run reports. Additionally, all users will receive annual Privacy and security training as provided and required by HHS.
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).	Retention and disposal: Job Number N1-512-92-2 Former Public health Service Hospitals/Clinics: Destroyed 50 years after date of last treatment, inactive medical records for active duty uniformed service personnel and non-uniformed service personnel. National Hansen's Disease Program: Retained at facility-not transferred to a Federal Records Center. Destroyed, as appropriate, after 50 years, or when no longer needed for research purposes, as determined by the project leader or principal investigator.

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.	The HDHP will only be accessed by authorized personnel after appropriate credentials have been issued to the individuals. Such credentials are based on the least privilege principle and are controlled through Role Based Access measures. All access and changes to the system and environment are logged and securely stored in the EHR and server systems. All system traffic flows through TLS 1.2 or later encrypted channels and all data will be encrypted at rest on the server environment. In addition to the Azure disk encryption, the SQL databases are also encrypted by Microsoft SQL Server Transparent Data Encryption (TDE). All backups are performed by the Azure backup system and are also stored encrypted. The servers are hosted on a Microsoft FedRAMP certified data center with multiple physical controls in place to meet the FedRAMP certification requirements.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	9/25/2025
Privacy Analyst Review Comments:		**# of Days - PA Review:**	87

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	10/15/2025
SOP Review Comments:		**# of Days - SOP Review:**	20

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 This PIA is ready for SAOP review and approval.	**# of Days - APA Review:**	30

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 11:10 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
No Records Found				