Privacy Impact Assessment (PIA): HRSA - HDHP - QTR4 - 2020 - HRSA658015

Date Signed: 3/8/2021

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

PIA ID:	1290763		
PIA Name:	HRSA - HDHP - QTR4 - 2020 - HRSA658015	**Title:**	HRSA - Hansen's Disease Health Portal
OpDIV:	HRSA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Initiation
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Contractor
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	3/24/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	New system no previous PTA
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	Cyfluent 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 - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in 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 -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	HHS User Credentials HHS/OpDiv PIV Card Non-HHS User Credentials Email address Password Username
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should 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 - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
PTA - 10B:	Please specify which PII data elements are used.	Last name, first name Medical Records number Last four of SSN Date of birth Phone number

PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Truncated SSN Name E-Mail Address Phone numbers Medical records (PHI) Date of Birth Photographic Identifiers Biometric Identifiers Medical Records Number
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Other
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	Above 2000
PIA - 4:	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 - 5:	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 - 6:	Describe the function of the SSN/Taxpayer ID.	Secondary unique identifier for record indexing.
PIA - 6A:	Cite the legal authority to use the SSN	Records indexed by SSN are retrieved in accordance with section 7(a)(2)(B) of the Privacy Act.
PIA - 7:	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; and section 326 of the Public Health Service Act.
PIA - 8:	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.	09-15-0003, Contract Physicians and Consultants 09-15-0007, Patients Medical Record System Public Health Service Hospitals 09-15-0028, PHS Clinical Affiliation Trainee Records
PIA - 9:	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 - 9A:	Identify the OMB information collection approval number or explain	Authorized under:

	why it is not applicable.	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 - 10:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 10A:	Identify with whom the PII is shared or disclosed and for what purpose	Other Federal Agency/Agencies State or Local Agency/Agencies Within HHS
PIA - 10A (Justification):	Explain why (and the purpose) PII is shared with each entity or individual.	HHS - Any employee in their official capacity with a need to know to provide the appropriate patient care for Hansen's Disease. Other Federal Agencies - For the purpose of assisting the department's efforts to provide appropriate patient care for Hansen's Disease. State or Local Agencies - For the purpose of assisting the department's efforts to provide appropriate patient care for Hansen's Disease.
PIA - 10B:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	All information sharing is done on a need-to-know basis and requires a signed Consent or Release of Information (ROI) form from each patient at time of request or service.
PIA - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	Copies of written notification (Consent Forms) and Release of Information (ROI) requested are collected at time of service and maintained in the Patient Chart.
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Patients are provided written notification at the time of service pertaining to the data collected, potential use, and disclosure.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	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	Patients are provided the option to opt-out of the collection or use of their PII by refusing service offered by the program.
PIA - 14:	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). Alternatively, describe why they cannot be notified or have their consent obtained	Notification of major changes are posted to the Federal Register following the SORN process, with patients provided written notification of updates at the time of service as to the data collected, potential use and disclosure. Alternatively, deceased patients or patients lost to follow up cannot be notified or have their consent obtained.
PIA - 15:	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 - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. 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 - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 Users - Daily data collection as it relates to the mission and patient care Administrators - Daily operations as it relates to system performance and availability to end users Contractors - Access required for data extraction and migration activities involved in the transition between the legacy system and HDHP as required by the contract.	
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	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 and audit logs.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	Role based controls are established within the system and assigned during account creation.
PIA - 20:	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	Annual role-based training and review at time of account creation and system access.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Cyfluent Training will be 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 will be trained in product usage. Most of the nurses are not experienced in using an Electronic Health Record (EHR). The nurses will use Cyfluent 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 will be trained in product usage. Most of the physicians are not experienced in using an EHR. The physicians will use Cyfluent 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 Cyfluent. They will be trained in product usage. The Laboratory personnel are not experienced in using the Cyfluent EHR. The Laboratory personnel will use Cyfluent to order lab tests, attach lab test results. Pharmacists: The Pharmacists at NHDP are primary users of Cyfluent. They will be trained in product usage. Most of the Pharmacists are not experienced in using a web based EHR. The Pharmacists will use Cyfluent to order prescriptions, refill prescriptions and fill prescription orders. Administrators: The Pharmacists at NHDP are super users of Cyfluent. They will be trained in product usage. The Administrators will use Cyfluent 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 - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific 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 - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	The system 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.
PIA - 25:	Describe the purpose of the web site, 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	Cyfluent 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. Those that will have access include end users and staff at the Hansen's facility in Baton Rouge LA for daily data collection as it relates to the mission of the facility and patient care; Administrators as it pertains to daily operations related to system performance and availability end users; Contractor (Team MicroHealth) for data extraction and migration activities involved in the transition between the legacy system and Cyfluent as required by the contract. Cyfluent is currently accessible via a web browser with a login; however, in the future we'll be enabling PIV login capabilities.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	Yes
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	Session Cookies - Does Not Collect PII
PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	No