Privacy Impact Assessment (PIA): HRSA - RWCA - QTR1 - 2020 - HRSA576423

Date Signed: 5/6/2020

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:	1078763		
PIA Name:	HRSA - RWCA - QTR1 - 2020 - HRSA576423	**Title:**	HRSA - HAB Chart Abstraction
OpDiv:	HRSA - HAB Chart Abstraction		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes

URL Details

Type of URL	List Of URL
Publicly accessible website with log in	https://rwca.abtsites.com

PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
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)?	Yes
PTA - 5A:	If yes, Date of Authorization	6/25/2019
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
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?	The HIV/AIDS Bureau Chart Abstraction system provides a medical chart abstraction (including a close read of the provider notes) as a way to

		obtain the primary data necessary for complete and accurate assessment of whether and to what degree Ryan White HIV/AIDS Program (RWHAP) providers are meeting the HHS and US Preventive Services Task Force (USPSTF) guidelines. The goal is to create statistics that are representative of clients and facilities. A representative probability based sample is the best approach for meeting HRSA, HIV/AIDS Bureau (HAB's) needs. The Abt Associates team will work collaboratively with HAB expert staff to identify the outcomes of interest that will determine the core data required for assessing quality of care. These data will reflect Department of Health and Human Services (DHHS) and USPSTF Guidelines. In addition to these core data, we will also work with HRSA, HAB to identify the most salient data regarding Sexually Transmitted Infection (STI) screening and treatment, opioid dependence screening and treatment, as well as hepatitis screening, vaccination, and treatment. Abt Associates will develop a secure web based chart abstraction tool that can be readily adapted for this project and meet all of HRSA, HAB's data collection and transmission security requirements. During the 18-month base period Abt Associates will work closely with HRSA, HAB experts to create a comprehensive study design, pilot the approach at nine RWHAP sites, assess the results and integrate the lessons-learned prior into our design for national implementation across 50 sites each year.
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.	The purpose of Chart Abstraction is for chart abstraction teams to collect relevant core and supplemental patient health variables from Ryan White HIV/AIDS Program (RWHAP) recipients. Information collected includes dates of service, routine health variables as well as variables related to HIV status, substance abuse, and sexually transmitted illness (STI). Patient data will be identified using an Encrypted Unique Client Identifier (eUCI). A client's demographic data are used to generate the eUCI but never stored in the system. The eUCI generation is based upon the following data elements: First and third characters of first name First and third characters of last name Full date of birth (MMDDYY) Gender Code 1 = Male, 2 = Female, 3 = Transgender, 9 = Unknown First names, last names and email addresses will be used to create user accounts and profiles for the users of Chart Abstraction system.
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 Email Address HHS Password HHS Username

		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	Abt Associates will employ a secure web-based system built in Amazon Web Services (AWS) cloud platform for client-level medical/administrative records abstraction that allows for direct upload to Abt Associates servers. Users log in using a user-name and password. Our Abt Associates/JSI site chart abstraction staff will only use secure full-disc encrypted laptops (FIPS 140-2-compliant algorithms) and then use a secure transfer protocol (HTTPS) to transmit the collected records to Abt's FedRAMP certified server. During transmission, the Abt team ensures that all data are encrypted both at rest and in transit. For in-depth analyses the collected records will be securely moved at regular intervals via the use of custom Application Program Interfaces (APIs) to Abt's FISMA moderate analytical environment, ACE3. Huddle, a FISMA-compliant data transfer tool, will be used to ensure the data security chain. Participant information collected includes dates of service, routine health variables as well as variables related to HIV status, substance abuse, and sexually transmitted illness (STI). This is collected to assess the quality of the provision primary care and screening treatment for hepatitis, sexually transmitted infections (STIs) and opioid use disorder. This information will be stored in Abt's FISMA Moderate analytical environment, ACE3. First names, last names and email addresses will be used to create user accounts and profiles for the users of Chart Abstraction system. Participants demographic data are used to generate the eUCI but never stored in the system.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	Yes
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	Name E-Mail Address Medical records (PHI) Date of Birth User Credentials
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Public Citizens
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	201 - 500
PIA - 4:	For what primary purpose is the PII used?	First names, last names, and email addresses will

		be used to create user profiles. This information is used to set user level permissions and to distinguish between the different chart abstraction users.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	Not Applicable - There are no secondary uses for which the PII will be used.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 USC 301, Departmental regulations
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.	Not Applicable - Records on the system are not retrieved by one or more PII Data Elements.
PIA - 9:	Identify the sources of PII in the system	Non-Government Sources Members of the Public
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
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	There is no formal notice given to Chart Abstraction participants about the use of their information. This information is readily available and has been shared with Abt Associates, as part of the HIV-AIDS Bureau Chart Abstraction contract, and Abt Associates has been given permission from HRSA to provide the participants with user accounts using their information. HRSA provided the names and email addresses of the users from participating organizations. All login information that will be used to log into the chart abstraction web tool de-identified once the record is created following the login.
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	RWHAP sites will be invited to participate in the Chart Abstraction study by HRSA . Abt will establish agreements with each of the sample sites,. There is no formal patient opt-out process provided by Abt Associates.
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	Due to existing agreements in place with HRSA and Chart Abstraction participants, formal consent process and notification is not required, nor in place with Abt Associates and the participants. There will be no changes to the use of PII; any major changes to the system will not impact the use of participant's PII. Users will not have access to other users' credentials (PII). However, if there is a change that impacts the user's information, Abt Associates will work with HRSA to notify affected Chart Abstraction participants.
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	Individuals will notify the Information System Owner (i.e., system administrator) to resolve any concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.
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	The system will be reviewed annually and users who no longer need access to the system will be removed, thus removing their accounts and email

		addresses.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	Administrators - Abt Associates Administrators require access to the platform in order to create and manage user accounts, monitor Chart Abstraction team progress and to overall analyze the effectiveness of the platform. Developers - Developers need access to the platform for routine maintenance, to remove defects and complete AD HOC updates, if any. Contractors - Abt Associates, direct contractor to HRSA, but not using agency's credentials, requires access to the PII, as Abt Associates serves as the contractor for building and managing the platform, and also administering users to the system.
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	Users are assigned roles in the system, and access to the system is controlled via roles. Only administrators that need access to the system user PII are able to see it. Access to chart abstraction participant's email addresses are restricted only to administrators. Regular users do not have the ability to view each other's name and information. Administrators and users must be approved by project team before being granted access to the system. Access to the system is restricted via permission levels as follows: -Level 1 Administrator Privileges: Ability to read, write and edit all chart abstraction record information. - Level 2 : Ability to only create their own records. Once the record is created and submitted, it cannot be edited.
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	Access to the system is controlled via roles and permission levels. During the design of the system, each role was evaluated by the project team to determine what data, at a minimum, is necessary to perform the user's job. PII of users will not be displayed to users outside of the administrator team.
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	All users of the system and project team will receive security awareness training offered by HRSA, in addition to training of the overall system use and how to properly use the system and walk through the different functionalities, to understand their roles and responsibilities.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	A full day in person training for the chart abstraction team staff will be provided. The

		overall objectives of the training will be to: Review all data elements including definitions, values and where each element will be found in the medical record Instructions will be provided for entering each data element into the online data collection system Assess inter-rater reliability of the chart abstractors Review the pre-site and on-site questionnaires
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)	Abt Associates has established a Data Use Agreement with HRSA that defines in detail the process and guidelines in place with regard to retention and destruction of PII for Chart Abstraction. After the completion of all tasks, Abt Associates will destroy the data provided by HAB using methods recommended by the National Institute of Standards and Technology in Guidelines for Media Sanitization (NIST SP 800-88). Abt Associates will also destroy any data stored on long term storage within 13 months after the noted destruction date.
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 is categorized as FIPS 199 “Moderate,” and is required to be FISMA compliant. As required by FISMA, numerous policies and procedures will be in place to govern and protect the information stored and processed in the system. Access to the system is restricted by user-name and password. The system cannot be accessed without valid log-on credentials. The system is hosted in AWS environment, and standard denial of service, antivirus, and patching/remediation are in place to prevent unauthorized access. Should unauthorized access occur, the incident response process will be activated to resolve the incident. AWS is FedRAMP certified, and has implemented numerous physical, technical and administrative controls to comply with FISMA security controls.
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	New question for Archer workflow - will provide response upon PIA review.
PIA - 26:	Does the website have a posted privacy notice?	No
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 - 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