Privacy Impact Assessment (PIA): HRSA - CART - QTR1 - 2022 - HRSA794772

Date Signed: 4/18/2022

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:	1439652		
PIA Name:	HRSA - CART - QTR1 - 2022 - HRSA794772	**Title:**	HRSA - BPHC Claims Analysis Review Tracking
OpDIV:	HRSA		

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://cart.hrsa.gov/Security/Logon.aspx

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	2/23/2022
PTA - 5B:	If no, Planned Date of ATO	2/23/2022
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
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 Bureau of Primary Health Care (BPHC) Claims Analysis Review & Tracking System (CART) will streamline and effectively catalog expert medical reviews, risk management

		reports, and other information pertinent to litigations, and track claims. It will create a more efficient, and accurate system for reviewers, BPHC, Office of General Counsel (OGC), and other litigation partners to better access and store information associated with claims and the expert reviews.
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 system will collect and maintain PHI (Protected Health Information), medical records, medical scans, and medical claims cases under litigation in federal court system. The information is used to assess the accuracy and validity of medical claims filed against the federal entities. The information contains some Personal Identifiable Information (PII), and the submission of personal information is mandatory to process the claims.
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
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	A claims tracking system with basic reporting analysis, and advanced tools used by HRSA, the Office of the General Counsel and the Department of Justice. The system is used in tracking litigation through administrative hearings and the federal court system. The system will collect medical malpractice claims data to make determinations on a claim. The data includes sensitive information such as PII, Personal Health Information, and adverse medical actions taken against a practitioner.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
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 Mother's Maiden Name Phone numbers Medical records (PHI) Date of Birth Photographic Identifiers Mailing Address Medical Records Number Legal Documents
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Employees/ HHS Direct Contractors Patients 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?	The information is used to assess the accuracy and validity of medical (malpractice)claims filed against the federal entities and to also track medical (malpractice) claims.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	Authority includes: Federal Tort Claims Act (FTCA), 28 U.S.C. 261-2680, 1346(b); Military Personnel and Civilian Employees Claims Act, 31 U.S.C. 240-243; Federal Claims Collection Act, 31 U.S.C. 951-953; Federal Medical Care Recovery Act, 42 U.S.C. 2651-2653; Federally Supported Health Centers Assistance Act, 42 U.S.C. 233(a)-(n); 42 U.S.C. 233(o) and 5 U.S.C. 552a (including §§ 552a(d)(5), (k)(2), (k)(4)).
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.	SORN 09-90-0062 https://www.hhs.gov/foia/privacy/sorns/09900062/index.html
PIA - 9:	Identify the sources of PII in the system	Government Sources Other HHS OPDIV
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	The PII related data is received from another HHS OPDIV, i.e., HHS/OGC/GLD. It was confirmed that OMB clearance is not required of us or applicable in this case.
PIA - 9B:	Identify the OMB information collection expiration date.	4/5/2024
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
PIA - 10A (Justification):	Explain why (and the purpose) PII is shared with each entity or individual.	CART supports management of FTCA claims for the Health Center and Free Clinic FTCA Programs, including claims and risk management reporting and statistical analysis, actuarial and premium reporting so PII information is shared amongst the program various health programs.
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)).	There are no agreements in place that authorizes the information sharing or disclosure.
PIA - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	PII sharing and disclosing is an automated process with various programs connected to CART using secure protocols wither the data is at rest or in-transit. All data is monitored, tracked, and accounted for using Splunk and other approved tools.
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	Given the legal authority and mandate of the HRSA/BPHC, it has been determined that a "covered entity" may disclose certain individually identifiable health information to the

		HRSA/BPHC without written consent or authorization of the individual, when the disclosure furthers the HRSA/BPHC's statutory purposes and functions (including those indicated in 42 U.S.C. 233). The personal information collected is not disclosed in any way to anyone outside of the program. It is used for claims tracking and risk management related purposes and to support ongoing litigation only.
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	HRSA, BPHC, and HRSA contractors qualify as "public health authorities" for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation, "Standards for Privacy of Individual Identifiable Health Information" (Privacy Rule), 45 CFR Parts 160 and 164. Under 45 CFR 164.512, a "covered entity" may disclose an individual's protected health information without the individual's written consent or authorization when such a disclosure is made to a "public health authority" that is authorized by law to collect information for the purpose of preventing or controlling disease, injury, or disability. Given the legal authority and mandate of the HRSA/BPHC, it has been determined that a "covered entity" may disclose certain individually identifiable health information to the HRSA/BPHC without written consent or authorization of the individual, when the disclosure furthers the HRSA/BPHC's statutory purposes and functions (including those indicated in 42 U.S.C. 233). The personal information collected is not disclosed in any way to anyone outside of the program. It is used for claims tracking and risk management related purposes and to support ongoing litigation only.
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	The personal information given to the program will be used only in connection with the administration and execution of the FTCA mission of protecting the public and providing quality health care. All web sites will have both a machine readable and HTML Privacy statement that can be viewed by the users at all times. Within this privacy statement, users are informed of how their information is protected and their rights as users in terms of the Federal system protecting their PII
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	The claimant or individual may request that the Department of Health and Human Services (HHS) Office of General Counsel respond regarding the procedural processing status of a relevant claim and related use of PII. The claimant or

		individual may send a request to the following address: Office of the General Counsel General Law Division Claims and Employment Law Branch U.S. Dept. of Health and Human Services 330 C Street, SW Attention: CLAIMS Switzer Building, Suite 2600 Washington, D.C., 20201 HHS-FTCA-Claims@hhs.gov
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 accuracy of the PII entered into CART is validated during the data entry process. Additionally, cases are selected at random each month and the integrity, accuracy, availability, and relevancy of the PII is reviewed and verified during these monthly quality audits.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17 Users are provided access: Review data and prepare reports Administrators are provided access: System Operations and Maintenance Developers are provided access: System Operations and Maintenance Contractor are provided access: Direct contractors develop and maintain the system database, stored data, and system functions	
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	All application users are assigned a user role within the application. Each user's role is defined by their job duties. Roles are assigned on the principle of least privilege. Users will only have access to PHI if their job requires access. The application does not display or provide access to PII for users whose role does not allow access to PII. Additionally, the entire database is encrypted to prevent unauthorized administrative staff from accessing the database. Employees acting as administrators, developers, etc. are only granted access to the database if their job duties require them to have access.
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 access is provided within the CART application. A user's role defines whether that user can view PII. Roles are defined based on the principle of least privilege. The application provides access to only the information that the user requires to fulfill their job responsibilities.
PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors	CART users are provided with annual privacy and security training that provides details on rules of behavior regarding

	and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	the use and protection of PII and PHI. This training must be completed prior to accessing CART and is a condition of employment. Additionally, CART users must acknowledge a warning message upon login. The message warns the user that CART is a U.S Government-owned system and is meant only for Government-authorized use.
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)	Paper Records are retained and disposed of under the authority of the National Archive and Records Administration (NARA) Job Number NC1-90-81-5, HSA Appendix B-351 Item 14. Office Services, Letter O. Administrative Tort Claims: Destroy 35 years after a claim is closed. HRSA is working with NARA to determine the appropriate retention, and scheduling of the electronic records for the CART System.
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	PII will be secured in the following manner: System will reside at HRSA facilities and will inherit all physical controls associated with this site. Application security will be role based and will grant permission to end-users based upon least privilege. Application will record end-user transactions and maintain audit history. The web application will not be public facing and will only be accessible by users on local network or via HRSA approved remote access method. System servers and application will be scanned and vulnerabilities remediated on at least a quarterly basis. System servers will be protected by anti-virus. System Administrators / Database Administrator will be the only personnel given access to systems housing the application. The application database will be encrypted. The application will be subject to and must pass a formal Certification and Accreditation process prior to being allowed Production access. A formal Change Management process will be followed.
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	The purpose of the website allows claims to be reviewed, analyze, and tracked. The website is publicly accessible but requires Multifactor Authentication (MFA) in order to access. The users are internal and external to HRSA.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	No
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