Privacy Impact Assessment (PIA): HRSA - CIBMTR - QTR2 - 2020 - HRSA593190

Date Signed: 4/23/2020

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:	1078721		
PIA Name:	HRSA - CIBMTR - QTR2 - 2020 - HRSA5931	**Title:**	HRSA - Stem Cell Therapeutic Outcomes Database
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?	No
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?	
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	4/29/2019
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?	One purpose of this system is to maintain the Stem Cell Therapeutic Outcomes Database (SCTOD), a component of the C.W. Bill Young Cell Transplantation Program (Program). The SCTOD is a subset of the Center for International Blood and Marrow Transplant Research (CIBMTR) Research Database (the System) that includes, in a standardized electronic format, information related to patients who have received stem cell therapeutic products. This information is defined as the information necessary to conduct an ongoing evaluation of the scientific and clinical status of transplantation involving recipients of a stem cell therapeutic product from a donor.
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.	Data on all allogeneic (related and unrelated) hematopoietic cell transplant. These data include demographic, disease, treatment, and outcomes. Examples of demographic data include--date of birth, gender, race, and ethnicity. Examples of disease data include primary diagnosis and disease status. Examples of treatment data include preparatory regimen administered, transplant data and date of treatment. Outcomes data include but are not limited to--relapse, secondary malignancies and survival. The system does not collect information about HHS system users or contractors. Access to the system is tightly controlled and limited to internal CIBMTR Medical College of Wisconsin (MCW) users using an MCW identity management 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.	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	The CIBMTR-MCW (Center for International Blood & Marrow Transplant Research - Medical College of Wisconsin) collects, maintains and shares information and data on allogeneic and autologous stem cell transplants and cellular therapies. As the Government contractor, the CIBMTR-MCW (Center for International Blood & Marrow Transplant Research - Medical College of Wisconsin) will also provide aggregated public information to increase availability, safety, and effectiveness of stem cell therapies. Using a subset of these data, the CIBMTR-MCW will report to the Government regarding activity of the C.W. Bill Young Cell Transplantation Program and transplant outcomes. The submission is voluntary, and contains data elements that include DOB, date of death, and treatment prescribed, but are not linkable to any particular individuals (the information gathered is de-identified, assigned a randomly generated number and used for statistical purposes). The CIBMTR-MCW also collects contact information from requestors via its public website for distribution of information or data. The contact information (name, phone and email address) collected, on the public website, from those who request data is not stored in or used by the CIBMTR data system. The contact information collected is solely used for the purpose of the transaction of responding to requests for information.
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.	See details within: 09–15–0068; C.W. Bill Young Cell Transplantation Program
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 Phone numbers Medical records (PHI) Date of Birth Employment Status User Credentials Others - Dates of Service for Treatment; Date of Death; Gender, Race, Ethnicity
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Patients
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained	Above 2000

	in the system	
PIA - 4:	For what primary purpose is the PII used?	The primary purpose for which the limited PII is used is to compute outcomes variables for research, including--patient age at time intervals, time intervals since transplant, time since last clinical follow-up, and for analysis of other specific outcomes. The contact information collected is solely used for the purpose of the transaction of responding to requests for information.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 USC 301, Departmental Regulations Public Law 109-129 establishes the C.W. Bill Young Cell Transplantation Program, authorizing the Department to establish by contract a system for identifying, matching, and facilitating bone marrow and cord blood transplants, including recruitment, patient advocacy and maintenance of a stem cell therapeutic outcomes database.
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.	09–15–0068; C.W. Bill Young Cell Transplantation Program
PIA - 9:	Identify the sources of PII in the system	Non-Government Sources Members of the Public Private Sector
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	OMB No: 0915-0310
PIA - 9B:	Identify the OMB information collection expiration date.	10/31/2022
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	Private Sector Within HHS
PIA - 10A	Explain why (and	Private Sector: Transplant Centers who provided the data to CIBMTR and

(Justification):	the purpose) PII is shared with each entity or individual.	very rarely, private sector research partners on a specific research protocol with whom an Agreement has been executed. Within HHS: HRSA
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)).	CIBMTR/MCW uses different agreements to govern information sharing and disclosure: Master Healthcare Data and Sample Submission Agreement (MHA) - an agreement between the CIBMTR and centers that formalizes lawful terms and transfer of data for mandated reporting under the C.W. Bill Young Cell Transplantation Program, as well as data and samples with informed consent submitted under CIBMTR protocols. Letter of Commitment for the Use of CIBMTR Datasets --often simply referred to as the Data Use Agreement (DUA) -- delineates for a principal investigator, the purposes for permissible use of CIBMTR data and the obligates the data recipient (and their institution) to protect privacy, prevent unauthorized data sharing or attempts to re-identify centers or patients(unless previously authorized to do so), data retention periods or destruction of datasets at the completion of the proposed work (where relevant). Research Services Agreement (RSA)- outlines CIBMTR services and data set ownership and incorporates data use language when contracting with commercial, private sector organizations.
PIA - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	In accord with the CIBMTR Data Use and Processing Policy, CIBMTR will only use personal data/PII to fulfill its obligations under agreements with third parties. In any case where personal data is shared, such as to facilitate computerized matching of CIBMTR data with other data sources under a specific research protocol, CIBMTR maintains complete and accurate records of any disclosure of Personal Data. This disclosure must include identification of data elements, documented approval from a senior CIBMTR leadership as well as review and documented approval by the CIBMTR centralized IRB. Approval documentation is maintained in accordance with CIBMTR General Records Schedule.
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	Institutions submitting data to the CIBMTR are expected to comply with their country's laws and regulations governing human subjects and privacy protection, and to obtain explicit individual consent for data submission to CIBMTR. In the U.S., the CIBMTR operates as a Public Health Authority (PHA) under the Stem Cell Therapeutic Outcomes Database (SCTOD) contract set forth by the Stem Cell Act of 2005, which mandates collection of data from centers on the allogeneic (related or unrelated) transplants they perform to further public health matters defined in the SCTOD. Beyond this mandate, data that is used for research or any other purpose, must be accompanied by center attestation that individual consent was obtained.
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 may not opt out of collection of PII for the purposes of the public health requirements of the SCTOD. Patients who have given consent for research uses of their PII may subsequently opt out of those uses by contacting their treatment center and requesting a change in their consent status. CIBMTR will also notify treatment centers of any communication from a patient, if the patient provides this information. Centers are instructed to update their reporting to CIBMTR and the patient's record will not be used for any other non-SCTOD matters from that date forward.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when	Major changes to the system are communicated to the public in the following ways: Updates to the CIBMTR System of Records Notice (SORN) publication in the Federal Register in accord with the US Privacy Act. Updates to the CIBMTR Privacy Impact Assessment (PIA) that is filed with HRSA and HHS.

	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	Publication of updates to the CIBMTR Data Use and Processing Policy (DUPP) on the CIBMTR public website and notification is provided to treatment centers that provide data to CIBMTR in accord with our standard procedure.
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	CIBMTR's personal data protection statement--published on its public website--summarizes the rights of those individuals for whom data has been collected and provides instructions on how to contact CIBMTR to exercise any of these rights. This link can be found at the following URL: https://www.cibmtr.org/About/dataprotection/_layouts/15/WopiFrame.aspx?sourcedoc=/About/dataprotection/Documents/QAC_O0005_PersDataProtxnStmt_v6_15JUN2018.pdf&action=default.
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	PII and other data collected by CIBMTR undergoes ongoing review to ensure its integrity, availability, accuracy and relevancy. Data capture forms with questions that require PII data responses undergo regular updating and revision by CIBMTR data operations staff and scientific directors and receive input from the wider transplant community to collectively maintain ongoing relevance. PII collected by CIBMTR undergoes ongoing validation and verification for integrity, accuracy, consistency, and completeness both at the point of capture and throughout the data lifecycle. Monthly processes are in place to assess data quality and as discovered, correct inaccurate PII data at the source. Additionally, CIBMTR conducts random audits of key data fields that include PII for specific centers. PII and other data that is extracted from the system for use undergoes additional validation for integrity and availability prior to analysis, sharing these data back with treatment centers or prior to fulfilling reporting obligations with third parties, including HRSA.

PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Users Administrators Developers Contractors
	Provide the reason of access for each of the groups identified in PIA -17 Users - Defined list of qualified CIBMTR clinical research coordinators, statisticians, and scientific directors. Administrators - Database Administrators and data quality personnel within CIBMTR for the purpose of maintaining systems and validating quality and integrity of the data. Developers - Defined list of qualified CIBMTR Information Technology developers for the purpose of maintaining and enhancing systems that maintain the data. Contractors - Only contractors engaged directly by CIBMTR MCW or NMDP BeTheMatch, and who have executed a Business Associate Addendum, and have received training for the purpose of maintaining and supporting CIBMTR personnel in maintaining and enhancing systems that maintain the data.	
PIA - 17A:		
PIA - 17B:	Select the type of contractor	Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	CIBMTR Data Use and Processing Policy: Access to Personal Data/PII is limited to only those personnel who have a legitimate business purpose to access the Personal Data/PII and that all personnel who have access to and/or use Personal Data/PII are obliged to keep these Data confidential. Administrative procedures used to determine legitimate business purpose require the supervisor to define the role and responsibilities of personnel for assignment to specific security groups that permit access to systems and data required of these job function.
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	CIBMTR staff follow a standard procedure for creation of anonymized, pseudonymized or de-identified datasets that specifies the removal of all patients, donor, and center identifiers, which could lead to the identification of a patient or transplant center from data files. There are numerous system controls that limit access to the type, amount or categories of PII, including--roles-based security groups; account management procedures that require supervisor or business unit manager authorization to access systems and see data; system access enforcement; and procedures for analyzing and sharing data (as noted above).
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	Staff receive general information and data privacy training at the point of hire and annually thereafter. Staff also receive periodic specialized training that includes data privacy topics and may receive additional functional training related to their position.

PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	All users receive Human Subjects Research training through the Collaborative Institutional Training Initiative (CITI) upon hire and at least every 3 years thereafter.
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)	According to the SCTOD Performance Work Statement established with the HRSA, CIBMTR will retain records permanently throughout the duration of the SCTOD contract or a HRSA Records Schedule has been approved by National Archives & Records Administration (NARA) to obtain the appropriate retention value of these records.
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	Administrative Access to PII is limited to only those staff members who have a legitimate business purpose to access the PII. CIBMTR has identified a limited set of users who have access to the RDB environment and even smaller number of users with privileged accounts. All personnel who have access to and/or use PII receive training and are obliged to keep the PII confidential. CIBMTR regularly tests key processes and perform annual risk assessments against reasonably foreseeable information security risks. Physical Physical access to the CIBMTR office space requires users present an authorized physical security badge Physical access to the Data Center that hosts the System is permitted only to specific, authorized personnel using a physical security badge and biometric controls. All other personnel, maintenance contractors or visitors must be logged and escorted by authorized personnel. The RDB environment (The system) is segmented by a dual redundant firewall within a subnetwork of the MCW parent enterprise network domain and identity management and access is maintained locally within this subnetwork. Technical If on-premise and wireless, users must authenticate to the parent organization network with a certificate-based authentication before being given a valid DHCP IP address that is non-routable across the MCW/CIBMTR network. A user must then successfully authenticate to their company issued workstation using single factor username/password If off-premise, user must successfully authenticate using multifactor authentication and then authenticate to their company issued workstation using single factor username/password. If on premise, users authenticate to an X-WIN session using single factor username/password Authorization credentials and role based permissions to the database application within the protected MCW/CIBMTR subnetwork are maintained separate from enterprise Active Directory System Incident and Event Monitoring is conducted on an ongoing basis.

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	Questions 25-29 to be reviewed/updated during next review.
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