PTA / PIA: HRSA - NMDP - QTR2 - 2025 - HRSA1445976

Created Date: 10/30/2025 12:25 PM Last Updated: 12/22/2025 3:22 PM

General Information

PTA / PIA Name:	HRSA - NMDP - QTR2 - 2025 - HRSA1445976	**PTA / PIA ID:**	3953077
Component Name:	HRSA - C.W. Bill Young Cell Transplantation Program	**ATO Boundary Name:**	C.W.Bill Young Cell Transplantation Program
Overall Status:	Complete	**# of Days - Open:**	175
Submitter:		**Submit Date:**	12/10/2025
Next Assessment Date:	12/21/2028	**Expiration Date:**	12/21/2028
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.	9/6/2024
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	Ernest Boakye
PTA 01A:	POC Title and Organization	Information System Security Officer
PTA 01B:	POC Email Address	eboakye@hrsa.gov
PTA 01C:	POC Phone Number	301-443-0413
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.	In 2025 National Marrow Donor Program (NMDP) enforced Multifactor Authentication (MFA) for all Donors/Registry Members (vs. optional before). Several websites have been consolidated. The Be The Match name has been deprecated and replaced by NMDP
PTA 03:	Is the data contained in the system owned by the agency or contractor?	Contractor
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 purpose of the C.W. Bill Young Transplantation Program is to increase the number of blood stem cell transplants for patients without a suitably matched related donor. The system matches the human leukocyte antigens (HLA) tissue types of volunteer adult donor registrants with the HLA types of searching patients.
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.	The C. W. Bill Young Cell Transplantation Program (Program) will collect medical information of patients needing a blood stem cell transplant, and on people who volunteer to donate blood stem cells. The information collected is stored on the contractor system and used to match potential donors with those in need. The PII necessary information to operate the Program is maintained by HRSA's contractor, the National Marrow Donor Program/NMDP. PII is used to assist in locating a potential donor if they are found to be a match for a patient in need of a lifesaving blood stem cell transplant.
PTA 05A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system.
PTA 05C:	Please identify the system that maintains the user credentials or controls access to this system.	For NMDP employees and network partners, Active Directory is used as the credential store, with Okta as the SSO/MFA solution. For Donors/Members (i.e. public users), Okta is used as both the credential store and MFA solution.
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.	The Contractor (NMDP) maintains and processes these data within its enterprise set of interconnected applications. These Contractor Owned and Operated applications, and their associated middleware, are used in part to fulfill its contracted obligations to HRSA. The system maintains the minimum necessary genetic information (human leukocyte antigen) of stem cell donors, minimum necessary health history, and minimum necessary PII in order to provide donor matching services to blood cancer patients.
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).	NMDP.org network.nmdp.org - Network & Payer Site
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.	The nmdp.org website is used for registering potential donors to the donor matching registry. Each user must register using basic contact information (name, address, email, etc.). Members of NMDP and the individual who registered has access to the data entered, and donors may update their contact information at any time.
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?	Yes
PTA 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by 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.	Persistent Cookies- Does Not Collect PII Other technology - Does Not Collect PII
PTA 12B:	What other technology is used?	The type of browser used to access the site The date and time of your visit The pages visited The address of the website that referred the user if they clicked a link to get to this site
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 Financial Account Information (e.g., account numbers, credit card numbers) Biographical Information Name Date of Birth User Credentials Employment Status/History Contact Information Email Address (Personal) Mailing Address (Personal) Phone Numbers (Personal) Biometrics/Distinguishing Features Biometric Identifiers (e.g., fingerprints, retina scans, DNA samples) Medical Information Medical Records Medical Records Number
PIA 23:	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	Employees/HHS Direct Contractors Patients
PIA 24:	Indicate the approximate number of individuals whose PII is maintained in the system.	1,000,000 or more
PIA 25:	For what primary purpose is the PII used?	The C.W. Bill Young Cell Transplantation Program shares medical information in an attempt to find donor matches with recipients, however the C.W. Bill Young Stem Cell Transplantation Program does not share the associated information about the individual, and such information cannot be obtained through other sources. Information is shared within the Program exclusively for facilitating blood stem cell transplants. For example, information may be shared from the National Marrow Donor Program (NMDP) to its participating network centers (e.g., transplant centers, donor centers, apheresis centers, marrow collection centers).
PIA 26:	Describe any secondary uses for which the PII will be used (e.g., testing, training, or research).	None. Any testing or research data is scrubbed of all PII information.
PIA 28:	Identify legal authorities, governing information use and disclosure specific to the system and program.	None, The Stem Cell Therapeutic and Research Act of 2005, Public Law (P.L.) 109-129, as amended by P.L. 111-264, does not specifically address system uses and disclosures related to this exercise.
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.	User Credentials Email Address Date of Birth Mailing Address Patient ID Number Name Phone numbers Medical Records Number Employment Status Financial Account Info
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.	09-15-0068, C.W. Bill Young Cell Transplantation Program
PIA 30:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains In-person Hard Copy Mail/Fax Phone Email Online Non-Government Sources Members of the Public
PIA 31:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA 31A:	Provide the information collection approval number(s) and expiration date(s).	OMB Control Number: 0906-0004 Expiration date: 10/31/2026
PIA 32:	Is the PII in the system shared directly with other organizations outside the system's Operating Division?	No
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.	PII is given voluntarily from persons who register as potential donors of blood stem cells. The individual's information is correlated through blood samples of that individual. If a major change to the system should occur, we are able to contact the patients and/or volunteered donors in writing to notify them of the changes and/or gain additional consents (if necessary). At the time of recruitment, donors are informed through the completion of consent forms that their information will be used by the program to facilitate unrelated blood cell transplantation. PII can also be provided by our partner network for research purposes. The individual would, via the network partner, provide consent to medical research opportunities. This consent is managed and handled via the network partner, and through NMDP via a network partner agreement. If an individual were to opt-out, it would go through the network partner, and the network partner would work with NMDP to remove the PII from NMDP if necessary.

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.	We utilize a recommitment process, in combination with address update requests to maintain contact with our registry of volunteer donors. If we have any issues with communication with a volunteer donor, such as disclosure or data use changes, we will use this avenue of outreach. This recommitment process is accomplished via physical mailings, phone contact, email and web site interactions. For data collected via our network partners, no notification is required to the individuals as they have consented to medical research through the network partner and not directly through NMDP. As described prior, the opt-out would be performed by the network partner, and information removed by the network partners request.
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.	There are multiple methods for the public to contact NMDP in regards to PII. The primary mechanism for complaints regarding use or disclosure of PII is through the NMDP Donor Advocacy Program. The Donor Advocacy Program website (https://www.nmdp.org/support-the-cause/donate-bone-marrow/donor-safety-and-support/donor-advocacy), which is accessed under the "Registry Members" tab of the NMDP.org website, specifically refers to the Donor Advocacy Program's charge to protect the rights of donors, including but not limited to the donor's right to confidentiality of PII. A direct toll-free number and specific e-mail address is provided for individuals seeking to engage the assistance of the Donor Advocacy Program. Additional methods include: email via the website privacy statement; contacting the Office of Patient Advocacy; contacting the local donor or transplant center; or calling the public 800 number, which provides a link to the Donor Advocacy Program. NMDP has a corrective action process in place which facilities the reporting and investigation of the improper usage or disclosure of PII.
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.	We routinely perform change of address verification in order to update our donor address information to increase the likelihood of donor eligibility. Additionally, as donors are removed from the Registry, either by request, age, or other criteria, their information is removed.
PIA 38:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors
PIA 38A:	Select the type of contractor.	Third-Party Contractor (Contractors other than HHS 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 - Appropriate users for search management process. Administrators - Administrators of appropriate systems for the management of the systems. Developers - Selected developers of appropriate applications for the support and enhancements of the applications and support of the users. Contractors - Selected contractors of appropriate applications for the support and enhancements of the applications and support of the users
PIA 40:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All user access to PII data is through an application layer, which uses authenticated user roles to determine what data any user can interact with.
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.	User roles for our applications are designed to permit users to access only as much data as they need to perform their jobs.
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.	Ongoing training is provided throughout the fiscal year as well as annual sign off on NMDP's policies with respect to the protection of PII collected from donors, and patients.
PIA 43:	Describe the training system users receive above and beyond general security and privacy awareness training.	All system users receive ongoing security and privacy training in compliance with NIST 800-53.
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).	The National Marrow Donor Program has the following existing retention policy: Electronic records must be retained as if they were paper records: unless otherwise stated herein, the retention requirement associated with any electronic record is determined by its content, not the method of delivery. Therefore, any electronic records that fall into one of the document types on the schedules must be maintained for at least the amount of time that is appropriate to that document type. HRSA is working with the Records Management Program to develop the appropriate retention and scheduling of the records, pending the National Archives approval.

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.	Administrative Controls: NMDP enforces strict governance through documented security policies aligned with NIST SP 800-53 Rev. 5. All personnel complete annual security awareness training and adhere to role-based access responsibilities. PII handling is governed by the Information Security and Technology Control Policy, which prohibits use in non-production environments. Compliance is monitored through internal audits, risk assessments, and enforcement of the Code of Business Ethics. Technical Controls: PII is encrypted at rest and in transit using industry-standard cryptographic protocols. Access is restricted through multi-factor authentication, least privilege principles, and centralized identity management. Continuous monitoring, vulnerability scanning, and secure coding practices ensure system integrity. Logging and alerting mechanisms provide real-time detection of unauthorized activities. Physical Controls: Systems hosting PII reside in secure, collocated data centers with 24/7 surveillance, two-factor building access, and visitor escort requirements. Facilities employ alarm systems and environmental safeguards to prevent unauthorized entry and maintain operational resilience.

Review and Comments

OpDiv Privacy Analyst Review

Privacy Analyst Review Decision:	Approved	**Privacy Analyst Review Date:**	12/16/2025
Privacy Analyst Review Comments:	For PTA-2A, please spell out the acronym upon 1st use - National Marron Donor Program (NMDP) Multifactor Authentication (MFA)	**# of Days - PA Review:**	6

SOP Review

SOP Review Decision:	Approved	**SOP Review Date:**	12/16/2025
SOP Review Comments:	Please review PTA 02A, PIA 09, and PIA 36 and update based on comments.	**# of Days - SOP Review:**	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Decision:	Approved	**Agency Privacy Analyst Review Date:**	12/17/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 12/17/2025 Comments were addressed, this PIA is ready for SAOP review and approval. 12/10/2025 Please see comments and update accordingly: PTA-5: HRSA states " HRSA does not host information on its servers from the Program that contain PII" but you list several PII elements in PIA-22. Does the system collect, maintain, store, and share PII? If so then remove the above sentence or revise so that it is clear as to if this PII is store on an HHS system or a Contractor system. If this PIA is for the contractor system use to capture the PII then state that in your response and list the PII listed in PIA-22. PIA-45: Please explain what administrative, technical, and physical controls are in place.	**# of Days - APA Review:**	1

SAOP Review

SAOP Review Decision:	Approved	**SAOP Review Date:**	12/22/2025
SAOP Review Comments:		**# of Days - SAOP Review:**	5

SAOP Signature

Date	User	Type	Name	Original Value	New Value
12/22/2025 12:59 PM	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
PTA 02A	Data Feed Service, pta_pia_HSRSA_Release	10/27/2025	Update Marron to Marrow	
PTA 09	Data Feed Service, pta_pia_HSRSA_Release	10/27/2025	Be the Match is deprecated. Please update.	
PIA 36	Data Feed Service, pta_pia_HSRSA_Release	10/27/2025	bethematch is deprecated	
PTA 05	BLAND, CRYSTAL	12/10/2025	HRSA states " HRSA does not host information on its servers from the Program that contain PII" but you list several PII elements in PIA-22. Does the system collect, maintain, store, and share PII? If so then remove the above sentence or revise so that it is clear as to if this PII is store on an HHS system or a Contractor system. If this PIA is for the contractor system use to capture the PII then state that in your response and list the PII listed in PIA-22.	
PIA 45	BLAND, CRYSTAL	12/10/2025	Please explain what administrative, technical, and physical controls are in place.	