

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/12/2015

OPDIV:

HRSA

Name:

C.W. Bill Young Cell Transplantation Program

PIA Unique Identifier:

P-4719879-017793

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

NMDP Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

New Interagency Uses

Describe in further detail any changes to the system that have occurred since the last PIA.

None

Describe the purpose of the system.

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.

Describe the type of information the system will collect, maintain (store), or share.

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 used to match potential donors with those in need. HRSA does not host information on its servers from the Program that contain PII. The PII information necessary to operate the Program is maintained by HRSA's contractor, the National Marrow Donor Program/Be The Match. The PII collected includes names, addresses, and phone numbers. It is optional whether donors opt to provide their social security numbers and/or email addresses. 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 life saving blood stem cell transplant.

Provide an overview of the system and describe the information it will collect, maintain (store), or share,

The systems that stores this data are custom developed Java and .Net based software assets. All PII information is collected and maintained in a single datastore. Donor information is stored in a Microsoft SQL database, and patient information is stored in an Oracle database. Each database is accessed through securely authenticated means, and any interactions with this data is logged and audited.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number

Date of Birth

Name

Driver's License Number

Biometric Identifiers

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Military Status

Employment Status

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Patients

How many individuals' PII is in the system?

1,000,000 or more

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 NMDP to its participating network centers (e.g., transplant centers, donor centers, apheresis centers, marrow collection centers).

Describe the secondary uses for which the PII will be used.

None. Any testing or research data is scrubbed of all PII information.

Describe the function of the SSN.

SSN information is collected voluntarily, and is used when trying to contact registry members who have been out of touch for a long period of time. It is only used when primary contact methods have failed.

Cite the legal authority to use the SSN.

None

Social security numbers are requested on a voluntary basis.

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.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-15-0068, C.W. Bill Young Cell Transplantation Program

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Online

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

The OMB numbers associated with collecting data for the C.W. Bill Young Cell Transplantation Program include: OMB #0915-0310

Expiration date: 12/30/2017

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Registry members are informed through the completion of hard copy consent forms.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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.

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 hard copy consent forms that their information will be used by the program to facilitate unrelated blood cell transplantation.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

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 would use this avenue of outreach.

This recommitment process is accomplished via physical mailings, phone contact, email and web site interactions.

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.

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 (http://www.marrow.org/DONOR/Donor_Advocacy_Program/index.html), which is accessed under the "Registry Members" tab of the BeTheMatch.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 facilitates the reporting and investigation of the improper usage or disclosure of PII.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

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.

Identify who will have access to the PII in the system and the reason why they require access.

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

Describe the 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.

Describe the methods in place to allow those with access to PII to only access 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.

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.

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.

Describe training system users receive (above and beyond general security and privacy awareness training).

Information Security and Privacy policies are available on an internal website. Weekly updates on information security/privacy are provided in addition to a monthly newsletter and advanced training for systems personal and developers.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

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. NARA/OMB M-12-18, Managing Government Records Directive Item 2.5 directs agencies to identify all unscheduled records by DEC 31, 2013. HRSA is working with the Records Management Program to develop the appropriate retention and scheduling of the records, pending the National Archives approval.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

PII is protected in transmission and at rest by using secure protocols. Individuals with access to the system have a user ID, password and are provided with two-factor authentication for remote access when deemed necessary.

Identify the publicly-available URL:

www.marrow.org

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No