Privacy Impact Assessment (PIA): HRSA - OPTN - QTR1 - 2021 - HRSA712428

Date Signed: 5/11/2021

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:	1325168		
PIA Name:	HRSA - OPTN - QTR1 - 2021 - HRSA712428	**Title:**	HRSA - National Organ Procurement and Transplantation Network
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

URL Details

Type of URL	List Of URL
Other	www.npdb.hrsa.gov

PTA - 3:	Is the system or electronic collection, agency or contractor operated?	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	2/20/2020
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	There have been significant changes within the UNet System during the timeframe of 2018 to present. For all changes that have occurred in the UNet System, the OPTN Contractor distributes System Notices and provides copies of all notices to HRSA. Infrastructure changes are maintained in the OPTN Contractor's Change Control System.
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 Organ Procurement and Transplantation Network (OPTN) was authorized by the National Organ Transplant Act of 1984, as amended

		(NOTA). The OPTN shall carry out specified functions as a private nonprofit entity established under 42 USC §274 to maintain the national computerized system and using established medical criteria to match deceased donor organs with a national list of individuals who need organs. The OPTN is operated by United Network for Organ Sharing (UNOS), s non-profit corporation from Virginia, pursuant to a contract with the US Department of Health and Human Services (HHSH250201900001C). UNOS utilizes proprietary software systems known as UNet to fulfill the requirements of the OPTN contract and meet the statutory obligations of the OPTN. The primary function of UNet is matching donated human organs to potential recipients. It is the only system in the country that serves this function for heart, lung, liver, pancreas, intestine, and kidney transplants. As part of this function, UNet maintains an active list of patients waiting for transplants. Due to the nature of organ transplantation, UNet must be efficient, readily available 24 hours a day, and secure. UNet is a contractor- owned system that is maintained and operated at its headquarters located in Richmond, VA. HHS/HRSA staff do not directly access the systems used to operate the OPTN.
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 OPTN collects pre- and post-transplant clinical information of patients on the patient waiting lists and living organ donors, histocompatibility information on donated organs, and records of matches run between organ donors and waiting list candidates. These records contain PII including Social Security Numbers, names, and state of residence for patients and included additional address and contact information for living donors. Information is collected and submitted by OPTN member transplant centers, histocompatibility labs and organ procurement organizations (OPOs). This information assists OPTN members throughout the United States with matching, transporting and sharing organs. The information entered into UNet is used to match transplant candidates to organ donors; electronically notify transplant programs of available compatible organs; and collect data on transplant candidates, deceased and living donors, eligible donors, and transplant recipients. The submission of personal information is mandatory for the OPTN member institutions. UNet also collects credentials from system users for the purpose of authentication to the system. Unique user login names are created for each user by system administrators, and users create a password associated with their assigned login.
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 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	UNOS utilizes UNet to operate the OPTN. UNet is the contractor-owned software that UNOS uses to accomplish the OPTN functions specified in the National Organ Transplant Act (NOTA), including

the “matching function.” The OPTN is a private not for profit entity established by NOTA, and which is operated by UNOS.

The primary function of UNet is matching donated human organs to potential recipients. It is the only system in the country that serves this function solid organs. UNet maintains an active list of patients waiting for transplants. Due to the nature of organ transplantation, UNet must be efficient, readily available 24 hours a day, and secure. UNet's main components are database and application servers using a storage area network, front ended with Web servers. Through UNet, the OPTN collects pre- and post-transplant clinical information of patients on the national patient waiting lists and living organ donors, histocompatibility information on donated organs, and records of matches run between donated organs and waiting list patients. These data items include: Name, Social Security number, identifiers assigned by OPTN and SRTR contractors, hospital and hospital provider number, State and zip code of residence, citizenship, race/ethnicity, gender, date and time of organ recovery and transplantation, name of transplant center, histocompatibility status, donor medical information and, if donor is deceased, cause of death, patient medical information before and after transplantation, cause of death (if recipient is deceased), health care coverage, employment and education level, and included additional address and contact information for living donors. Information is collected by OPTN member transplant centers, histocompatibility labs and organ procurement organizations (OPO) and is then submitted to the OPTN system for matching. The system also collect credentials from system users for the purpose of authentication to the system.

Unique user login names are created for each user by system administrators and users create a password associated with their assigned login. Information is obtained from medical personnel at organ transplantation institutions. Submission of this information to the OPTN is mandatory for OPTN member transplant centers, histocompatibility labs and OPOs. The information collected in UNet is for the continued operation and improvement of the National Organ Procurement and Transplantation Network (OPTN). This information assists transplant centers, organ procurement organizations and histocompatibility laboratories throughout the United States with matching, transporting and sharing organs. The information entered into UNet is used to match transplant candidates to organ donors; electronically notify transplant programs of available compatible organs; and collect data on transplant candidates, deceased and living donors, eligible donors, and transplant recipients. The submission of personal information is mandatory for the OPTN member institutions.

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	Social Security Number Name Medical records (PHI) Biometric Identifiers Mailing Address Medical Records Number Legal Documents Patient ID Number Others - Identifiers assigned by OPTN and SRTR contractors.
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Business Partners/Contacts (Federal, state, local agencies) Patients Vendors/Suppliers/Third-Party Contractors (Contractors other than HHS Direct Contractors) 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?	PII is primarily used to identify and match transplant candidates with donors.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	PII collection, use & disclosure authority as described in the SORN, Final Rule, OPTN Contract, OPTN Policies, and as the OPTN's designation as a "public health authority" to include for purposes of bonafide research.
PIA - 6:	Describe the function of the SSN/Taxpayer ID.	The Social Security Number (SSN) is used to identify an individual candidate, recipient or living donor. SSN are used for patient linkage with United States Renal Data System (USRDS) end-state renal disease (ESRD) database for ESRD initiation and dialysis start dates, and the Social Security Administration Death Master File (SSADMF) for death ascertainment. SSN is also used to check for duplicate patient data in the system.
PIA - 6A:	Cite the legal authority to use the SSN	There's no authority specific to the collection and use of SSN; however, 42 CFR 121 provides the OPTN the authority to collect data on donors, recipients, and transplant candidates as directed by the Secretary.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	42 CFR 121 and 42 USC 274
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	09-15-0055, OPTN/SRTR

	indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system	Non-Government Sources Members of the Public Private Sector Other
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	There are two OPTN data system information collection packages. The Data System for Organ Procurement and Transplantation Network (TIEDI) (OMB number, 0915-0157, expiration date: 08/31/2023) and the Organ Procurement and Transplantation Network Application Form (Membership) (OMB number 0915-0184, expiration date: 08/31/2023).
PIA - 9B:	Identify the OMB information collection expiration date.	8/31/2023
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 Private Sector State or Local Agency/Agencies Within HHS
PIA - 10A (Justification):	Explain why (and the purpose) PII is shared with each entity or individual.	PII collection, use & disclosure authority as described in the SORN, OPTN Final Rule, OPTN Contract, OPTN Policies, and as the OPTN's designation as a "public health authority". Within HHS (HRSA) – as requested and as a OPTN Monthly Data File transmission SRTR – OPTN Monthly data file transmission as directed by the OPTN Contract Patient/Personal Representative – an individual or their authorized representative can request their complete patient record we hold (excludes Donor Information which is not disclosed as part of the patient record) Patient Identified Data Requests for bona fide research purposes only – HRSA approval, HRSA Data Use Agreement, Research Plan, Security Plan and IRB approval required Court ordered subpoenas, Civil or Criminal Law Enforcement UNOS Internal disclosures for roles that support the OPTN Contract requirements and operation (e.g. Research, Organ Center, Review Board, etc.)
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)).	The OPTN contract requires data sharing with Health and Resource Service Administration (HRSA) and with Scientific Registry of Transplant Recipients (SRTR) contractor, and with

		researchers approved by HRSA. HRSA and Centers for Medicare & Medicaid Services (CMS) also has a Sharing Agreement for OPTN data.
PIA - 10C:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII	The OPTN contract requires data sharing with HRSA and a written agreement and schedule to share data with the SRTR contractor. In addition, HRSA, the OPTN, 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 OPTN, it has been determined that a "covered entity" may disclose certain individually identifiable health information to the OPTN without written consent or authorization of the individual, when the disclosure furthers the OPTN's statutory purposes and functions. Under 42 CFR 121.11, the OPTN shall maintain records of all transplant candidates, all organ donors, and all transplant recipients and shall operate, maintain, receive, publish, and transmit such records and information electronically. The records are collected by transplant centers and Organ Procurement Organizations (OPOs), and submitted to the OPTN Contractor. These records are used for matching transplant candidates in the national waiting list to donated deceased organs. The OPTN maintains a record of match runs and data requests. UNOS also maintains information relative to each disclosure for all areas as described in 10a.
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	The OPTN, has been designated as a "public health authority" 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 OPTN, it has been determined that a "covered entity" may disclose certain individually identifiable health information to the OPTN without written consent or authorization of the individual, when the disclosure furthers the OPTN's statutory purposes and functions. The information is taken from medical records. It is used to correlate those needing organs with donor organs as they become available based on strict guidelines. The UNet System is accessed by authorized employees of OPTN member institutions. Those member institutions are notified by UNOS when a major change occurs in the UNet System. UNOS does not collect and maintain contact information for individuals. Therefore, consent and notification of collection of data are performed by the OPTN member institutions who have direct contact with the individuals on whom the information is being collected.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Mandatory
PIA - 12A:	If mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties	42 CFR §121.5 states in part, "Transplant hospitals shall assure that individuals are placed on the national list as soon as they are

		determined to be candidates for transplantation. The OPTN shall advise transplant hospitals of the information needed for such listing." In order for any hospital to retrieve or transplant any deceased organs in the US, the hospital must be an active member of the OPTN and must comply with OPTN policies. Accordingly, a patient must be in the national list to be a candidate for transplantation. The Secretary has determined that data submitted to the OPTN by organ procurement organizations and transplant hospitals are considered mandatory under 42 CFR §121.11(b)(2). Failure of an OPO or transplant hospital to submit the data accurately and completely could be a violation of this section of the OPTN final rule. An OPO or transplant hospital participating in Medicare or Medicaid could be considered in violation of Section 1138 of the Social Security Act of the Secretary found that it did not provide information to the OPTN as required specifically by §121.11(b)(2). The OPTN is required by law to maintain records on all transplant candidates, all organ donors, and all transplant recipients. These records are transmitted to the OPTN by OPTN member institutions. The information is taken from medical records. It is used to correlate those needing organs with donor organs as they become available based on strict guidelines. The UNet System is accessed by authorized employees of the OPTN member institutions. Consent and notification of collection of data are performed by the member institutions who have direct contact with the individuals on whom PII is being collected.
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	42 CFR §121.5 states in part, "Transplant hospitals shall assure that individuals are placed on the national list as soon as they are

		determined to be candidates for transplantation. The OPTN shall advise transplant hospitals of the information needed for such listing." In order for any hospital to retrieve or transplant any deceased organs in the US, the hospital must be an active member of the OPTN and must comply with OPTN policies. Accordingly, a patient must be in the national list to be a candidate for transplantation. The OPTN is required by law to maintain records on all transplant candidates, all organ donors, and all transplant recipients. These records are transmitted to the OPTN by OPTN member institutions. The information is taken from medical records. It is used to correlate those needing organs with donor organs as they become available based on strict guidelines. The UNet System is accessed by authorized employees of the OPTN member institutions. Those member institutions are notified by the OPTN contractor when a major change occurs in the UNet System. . Consent and notification of collection of data are performed by the member institutions who have direct contact with the individuals on whom PII is being collected. The System of Records for the OPTN/SRTR is reviewed periodically by HRSA. Any alteration or proposed change to the routine use of OPTN data is published in the Federal Register. Per the OPTN contract, UNOS responds to requests from individuals for information about their records in UNet.
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	UNet is not accessed by individuals on whom PII is collected. The UNet System is accessed by authorized employees of the OPTN member institutions. The member institutions, not the OPTN contractor, obtain consent and notify the individuals how their PII is to be used. It is important to note that the UNet System is the system of record only for match result information. Source documentation for all other information does not reside with UNet but resides elsewhere. UNOS does not collect and maintain contact information on the individuals who PII is maintained in UNet.
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 UNet System is accessed by authorized employees of the OPTN member institutions. It is the responsibility of the OPTN member institutions to ensure the accuracy and appropriateness of the information entered in UNet. In the event of a disclosure of information residing in UNet, the OPTN contractor would notify the specific OPTN member institutions impacted, and those institutions would, in turn, notify the individuals impacted. The OPTN contractor, UNOS, does not collect and maintain contact information on individuals.
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 input of date of birth and SSN into the UNet system is validated on input as it requires dual entry (the information must be input twice). The facilities who are entering patient data are

		responsible for the integrity of the data. Data is routinely audited for data integrity and compliance with OPTN polices, and relevance by the OPTN Contractors Member Quality Department as required of the OPTN contract. SSN is also used to check for duplicate patient data in the system.
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	
	(1) Users -End-user use of data. Internal QA data audits. IT System Administration Programming and development. Statistical analysis); (2) Administrators - End-user use of data. Internal QA data audits. IT System Administration Programming and development. Statistical analysis. (3) Developers- End-user use of data. Internal QA data audits. IT System Administration Programming and development. Statistical analysis; (4) Contractors - End-user use of data. Internal QA data audits. IT System Administration Programming and development. Statistical analysis	
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	Each Site (OPO, Transplant Center, or Histocompatibility Lab) can only view donor, candidate or recipient data they have been granted access to (role-based). Each site has a site security administrator who reviews system rights. In addition, UNOS conducts a Site Security Administrator and End User Audit each year that serves as another review/checkpoint. In addition, UNOS limits physical and logical access to the production environments.
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	Each Site (OPO, Transplant Center, or Histocompatibility Lab) can only view donor, candidate or recipient data they have been granted access to (role-based). Each site has a site security administrator who reviews system rights. In addition, UNOS conducts a Site Security Administrator and End User Audit each year that acts as another review/checkpoint. In addition, UNOS limits physical and logical access to the production environments.
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	The security administrators training, System Terms of Use, UNOS employees/contractors receive annual security awareness training and review of corporate security policy, UNOS employees/contractors receive annual Privacy Training and review of privacy policies.
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	None
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)	The language below is directly from the SORN and is applicable to the Government's copy of the OPTN data: HRSA is working with the Records Management Program to develop the appropriate

		retention and scheduling of the records, pending the National Archives approval.
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	To protect PII, UNOS uses a three-tiered system (1) the top layer is a web browser (examples include Microsoft's Internet Explorer or Google's Chrome) using TLS technology encryption to protect the data in transit. (2) layer two, or the middle layers, are the web servers. The OPTN Contractor uses multiple web servers and multiple, geographically dispersed operating environments. (3) The third and final layer is the data layer which includes application servers and SQL database servers where The OPTN Contractor uses Microsoft's Clustering software for the SQL servers. All official OPTN data is encrypted at rest at both the database level, using industry standard strong encryption algorithms, as well as in the Nutanix hyper-converged environment where the storage is encrypted. These operating environments are located within a highly secured, industry leading, co-location facilities. The OPTN contractor (developers of the system) has access agreements in place defining system security policies and rules of behavior for both internal staff as well as site administrators and users of the system. Internal staff who have access to the system and the data are required to pass pre-employment verification, background investigations, including criminal history, and other prerequisites prior to being provided access to the facility as well as systems. Site Security Administrators are required to review access for their users on an annual basis. The OPTN Contractor uses a Defense-in-Depth and Zero Trust hybrid model to secure the environment. This includes, but is not limited to, vulnerability management, anti-malware protection, access management, code scanning, penetration testing, intrusion detection and prevention, etc. The OPTN contractor also employs an electronic security system and 24 X 7 security guards that monitor door access and people movement. Physical access points to sensitive facilities, or restricted areas housing information systems that process or display information are controlled during working hours and guarded or locked during non-working hours. Each employee, contractor, temporary employee, consultant, or contractor is issued a security badge. Each person must scan his or her badge to the electronic reader before entering a controlled door on the OPTN contractor's premises.

Access to systems at the co-location facilities requires individuals to be on an approved access list, have a badge as well as specific access to the cage where the systems are housed.