Attachment 7
U.S. Nuclear Medicine Technologists Study
Privacy Impact Assessment

Save

Privacy Impact Assessment Form

v 1.43

5/19/2016

Status | Form Number: Read Only | Form Date: Read Only

	Question	Answer
1	OPDIV:	Read Only - OPDIV
2	PIA Unique Identifier:	Read Only- PIA Unique ID
2a	Name:	Read Only-Name
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ○ Minor Application (stand-alone) ○ Minor Application (child) ○ Electronic Information Collection ◉ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes X No
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No
5	Identify the operator.	○ Agency X Contractor
6	Point of Contact (POC):	POC Title: Staff Scientist/Contracting Officer Representative POC Name: Michele M. Doody POC Organization: NCI/Division of Cancer Epidemiology and Genetics POC Email: doodym@mail.nih.gov POC Phone: 301-518-6001
7	Is this a new or existing system?	X New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes X No
8a	Date of Security Authorization	

Save

11	Describe the purpose of the system.	The purpose of the system is to collect and store all data related to the U.S. Nuclear Medicine Technologists Study, including the cohort master file, questionnaire files, dosimetry files, medical outcome files, follow-up tracking and result files.
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The system will collect and maintain information on personal identifiers, demographic characteristics, nuclear medicine technology certification and work histories, medical outcomes, disease risk factors, radiation doses, follow-up, vital status, and causes of death. De-identified data will be shared with NCI and other investigators to evaluate disease risks associated with radiation or other factors.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The system collects and maintains information on a cohort of U.S. nuclear medicine technologists certified by the Nuclear Medicine Technology Certification Board or the American Registry of Radiologic Technologists during 1981-2016. The primary study objectives are to assess cancer and other disease risks associated with chronic fractionated occupational exposures to high-energy radioisotopes. Information obtained from the certification organizations may include names, addresses, dates of birth, gender, race, types and dates of certification, email addresses, and social security numbers if available. Study participants will be asked to provide on a baseline computer-assisted web interview calendar-specific nuclear medicine work histories (procedures performed, other work practices, radiation protection measures), cancer and other disease outcomes, disease risk factors (such as cigarette smoking, reproductive factors, personal medical radiation procedures). The study cohort will be followed for incident cancers via linkage with state cancer registries and for cancer and other causes of death through linkage with the National Death Index. Badge dose records will be obtained through linkage with a commercial dosimetry provider and used to estimate occupational doses for individual technologists for each year worked. The data will be stored for as long as cohort follow-up and active data analysis continues. De-identified data will be shared with NCI and other investigators to evaluate disease risks associated with radiation or other factors. An initial feasibility study will be conducted on a sample of 1,500 out of an estimated 25,000 eligible nuclear medicine technologists.
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

15	Indicate the type of PII that the system will collect or maintain.	☒ Social Security Number ☒ Name ☐ Driver's License Number ☐ Mother's Maiden Name ☒ E-Mail Address ☐ Phone Numbers ☐ Medical Notes ☒ Certificates ☐ Education Records ☐ Military Status ☐ Foreign Activities ☐ Taxpayer ID Medical outcomes and diagnosis dates Causes and dates of death ☒ Date of Birth ☐ Photographic Identifiers ☐ Biometric Identifiers ☐ Vehicle Identifiers ☒ Mailing Address ☐ Medical Records Number ☐ Financial Account Info ☐ Legal Documents ☐ Device Identifiers ☒ Employment Status ☐ Passport Number Other... Other... Other...
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☐ Employees ☐ Public Citizens ☐ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☐ Patients Other: U.S. nuclear medicine technologists
17	How many individuals' PII is in the system?	10,000-49,999
18	For what primary purpose is the PII used?	The PII is needed for cohort follow-up. Questionnaires will be administered to collect information on occupational and personal medical radiation exposures, cancer and other disease risk factors, and cancer and other medical outcomes. The cohort will also be linked with cancer registries to identify unreported cancers and obtain detailed histology data on reported cancers, the Social Security Administration (SSA) to determine vital status, the National Center for Health Statistics (NCHS), National Death Index (NDI) to obtain causes of death for decedents, and a commercial dosimetry provider (Landauer, Inc.) to obtain radiation badge dose readings.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None
20	Describe the function of the SSN.	The SSN is the primary identifier used to link with cancer registries, SSA, NCHS/NDI, and the commercial dosimetry provider.

Save

20a	Cite the **legal authority** to use the SSN.	The Social Security Administration program Service to Epidemiological Researchers to Provide Vital Status Data on Subjects of Health Research, OMB No. 0960-0701 is authorized under Section 205(r) of the Social Security Act. This authorization allows the investigators to provide the subjects name, date of birth, sex, and SSN. Linkage with the SSA records to determine who is alive and deceased is a cost effective method of verifying vital status. Vital status is necessary to assess eligibility for continued contact and follow-up, linkage with state cancer registries, and linkage with National Center for Health Statistics to evaluate cause specific mortality. This study is authorized under Section 411 of the Public Health Service Act [42 USC 285a]
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act [42 USC 242m, Section 308(d)] Privacy Act of 1974 Minnesota Government Data Practices Act (MGDPA), Chapter 13
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: NIH Systems of Record 09-25-0200 [Clinical, Published: Published: ☐ In Progress
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☐ In-Person ☐ Hard Copy: Mail/Fax ☐ Email ☒ Online ☐ Other Government Sources ☐ Within the OPDIV ☒ Other HHS OPDIV ☒ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☒ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☒ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	OMB No. 0905-0656 (expired 4/30/2015; reinstatement with revision is pending)

Save

24	Is the PII shared with other organizations?	(•) Yes ( ) No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS PII will be shared with the NCHS/NDI to obtain causes of death for decedents. ☒ Other Federal Agency/Agencies PII will be shared with SSA to obtain information on vital status. ☒ State or Local Agency/Agencies PII will be shared with state cancer registries to identify unreported incident cancers and to obtain detailed histology data for registry-identified and self-reported cancers. ☒ Private Sector PII will be shared with a commercial dosimetry provider (Landauer, Inc.) to obtain badge dose readings.
24b	Describe 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)).	Development of data security/transfer agreements between UMN and the certification boards (ARRT and NMTCB) is in process. Before any data linkages for individual studies, the SSA requires that a Memorandum of Understanding be established between the NCI and SSA, and the NCHS requires submission and approval of an NDI application. A long-standing agreement is in place with Landauer, Inc. to provide dosimetry records for medical radiation workers.
24c	Describe the procedures for accounting for disclosures	Procedures are in place to ensure the safety and integrity of all data and programs within the UMN control. These procedures include virus prevention, hardware and software configuration, management, disaster recovery, and incident response. In the event of a computer break-in, network intrusion, or data theft, the UMN policy for Network/Computer Incident Response establishes procedures to follow. Decisions will be made regarding the level of response required and the appropriate actions necessary to preserve evidence of the intrusion while restoring service to the affected entities.
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	Eligible nuclear medicine technologists will be sent a recruitment email inviting them to participate in the study. The email will include a brief description of the study, an individual-specific link and password to access the computer-assisted web interview, and a consent information sheet. The consent information sheet provides introductory and background information about the study, the procedures involved, the potential risks and benefits, the authority for collecting the data, data privacy, the voluntary nature of the study, and contacts to obtain additional information.
26	Is the submission of PII by individuals voluntary or mandatory?	(•) Voluntary ( ) Mandatory

Save

27	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.	Individuals can opt-out of the study by contacting the study office, by not logging in to the computer-assisted web interview, or by indicating on the consent form that they do not consent to complete the questionnaire. Any individual who agrees to participate can withdraw from the study at any time. Upon request, data already collected can be withdrawn from the database but cannot be withdrawn from analyses that are completed or are underway. This information is provided in the consent form.
28	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.	All study activities are reviewed and approved annually by the institution review boards (IRB) at NCI and UMN. Before any major changes are made to the system, the study team will seek NCI and UMN IRB approvals for the changes. IRB recommendations regarding subject notification and/or re-consent based on the specific nature of changes in disclosure or data use will be implemented. If either IRB require a change in the consent, participants will be re-contacted by email in the same manner that they were recruited to participate in the study.
29	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 is a section in the study consent information sheet included with the study recruitment email and in the consent form included at the beginning of the computer-assisted web interview that reads: "Contacts and Questions: This study is being conducted by Bruce H. Alexander, PhD, in the School of Public Health at the University of Minnesota, in collaboration with the National Cancer Institute, the American Registry of Radiologic Technologists (ARRT), and the Nuclear Medicine Technologists Certification Board (NMTCB). If you have any questions about this study or about your rights as a study participant, please contact the research staff at the University of Minnesota. You may call (800) 447-6466 or email usnmt@umn.edu. If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher(s), you are encouraged to contact the Research Subjects' Advocate Line, D528 Mayo, 420 Delaware St SE, Minneapolis, MN 55455; (612) 625-1650." The UMN will review all reported concerns on a case-by-case basis. The UMN follows these IRB guidelines: Federal regulations [45CFR46.103(b)(5) and 21CFR56.108(b)(1)] require the IRB to ensure that investigators promptly report "any unanticipated problems involving risk to subjects or others" (UPIRTSO). The IRB defines UPIRTSO as any problem or event which in the opinion of the local investigator was unanticipated, reflects new or increased risk to the subjects and was possibly related to the research procedures. The IRB makes the determination of whether the unanticipated problem meets the criteria as a UPIRTSO. The Principal Investigator will provide his or her opinion of whether an event meets UPIRTSO criteria when reporting to the IRB. The IRB will determine whether the event reported fits the criteria for UPIRTSO and if any further changes to the approved study should be made as a result of the report. All problems/events that do not meet the IRB's requirements for prompt reporting will be reported to the IRB in summary form at the time of continuing annual review. The IRB has created a Non UPIRTSO Adverse Event Log template for researchers to use to track these events.

Save

30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	All of the Windows workstations log user access via Active Directory. Access logs are reviewed daily for anomalies. An automated reporting tool is used to analyze the server logs to look for abnormal activity. Access is only available through Local Area Network (LAN). A firewall is in place that logs all incoming and outgoing connections to the LAN. This log is maintained and checked for evidence of attempted unauthorized access to the LAN. UMN computer center staff performs weekly security checks of the computer center resources using the Qualys vulnerability scanner.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	The University of Minnesota (UMN) is the coordinating center for this study. Only UMN staff working directly on this study will have access to the database where the PII will be stored. Individual staff members will only have to access to the specific PII needed to perform their specific tasks.
		☒ Administrators	To perform backups and disaster recovery functions.
		☐ Developers	
		☐ Contractors	
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The University of Minnesota deploys Active Directory (AD) technology with Shibboleth to authorize and authenticate user access to network resources. Depending on the study, access may also include IP address authentication. All computers require a University account to log in.	
33	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.	The UMN study management team determines the type and scope of data access per individual staff member. Each staff member has access only to the specific PII needed to perform their specific tasks. User account privileges are configured accordingly by system administrators. PII will be shared with the SSA to obtain information on vital status and with the National Center for Health Statistics (NCHS) to obtain causes of death for decedents from NDI. These privileges are removed from accounts when staff leave the study. Also, accounts are automatically locked after three failed login attempts and can only be unlocked by a system administrator. The UIS department notifies the Division of any questionable security behavior for immediate resolution.	
34	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.	UMN study staff must complete a series of online courses on data security and privacy practices and policy, mandated by the University and tracked by Human Resources. Study management also maintains records certifying the completion of all necessary training.	

Save

35	Describe training system users receive (above and beyond general security and privacy awareness training).	Additional training may be required, depending on the study and specific study function. As an example, Bloodborne Pathogens training would be required if blood samples were to be collected. Based on the current study protocol, required additional training is not anticipated.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	(•) Yes ( ) No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1B "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 3000-G-3, which allows records to be kept as long as they are useful in scientific research. The system falls under the Privacy Act System of Records Notice 09-25-0200. As this is an epidemiologic cohort study, there are currently no plans to destroy the data.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Electronic study data are stored on server clusters, hosted at the University of Minnesota data centers. The Office of Information Technology (OIT) closely manages and monitors these centers. Facility access is limited to data center staff, system administrators, storage engineers, facility support and janitorial staff. Access controls entail personnel submitting a formal request to access a data center server room, a security card to enter the facility, and a center staff signing them in. All access logs are reviewed monthly and rights annually. Multiple server monitoring tools (e.g., Qualys, Zabbix, scripts) are utilized providing real time alerts of any errors, downtime, and security issues. Network traffic flows are analyzed by the University Information Security (UIS) department for security events. The data disaster recovery setup is twofold: data are replicated off site frequently and backups are created regularly on a set schedule.

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	( ) Yes ( ) No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	( ) Yes ( ) No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	( ) Yes ( ) No
Reviewer Notes		

Save

	Reviewer Questions	Answer
4	Does the PIA appropriately describe the PII quality and integrity of the data?	○ Yes ○ No
Reviewer Notes		
5	Is this a candidate for PII minimization?	○ Yes ○ No
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	○ Yes ○ No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	○ Yes ○ No
Reviewer Notes		
8	Does the PIA raise any concerns about the security of the PII?	○ Yes ○ No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	○ Yes ○ No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	○ Yes ○ No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	○ Yes ○ No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	○ Yes ○ No
Reviewer Notes		
General Comments		

Save

OPDIV Senior Official for Privacy Signature		HHS Senior Agency Official for Privacy	