Save

Privacy Impact Assessment Form

v 1.43

Status: Draft   Form Number: F-54643   Form Date: 9/18/2013 10:56:01 AM

	Question	Answer
1	OPDIV:	TEST
2	PIA Unique Identifier:	P-5860043-506903
2a	Name:	Test 9-18-01
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 ● 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 ○ Contractor
6	Point of Contact (POC):	POC Title: Application Development Lead POC Name: Sandy Desautels POC Organization: NIDDK / EO / CTB POC Email: desautes@niddk.nih.gov POC Phone: 301-827-2001
7	Is this a new or existing system?	● New ○ Existing
8	Does the system have Security Authorization (SA)?	● Yes ○ No
8a	Date of Security Authorization	
11	Describe the purpose of the system.	To gather registration information related to NIDDK sponsored programs.

Save

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 collects and stores information from applicants applying for NIDDK sponsored programs.
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 stores information from applicants applying for NIDDK sponsored programs. Information is used by NIDDK staff to determine eligibility for identified programs and to accept applicants into the programs. The information is permanently stored.
14	Does the system collect, maintain, use or share **PII**?	● Yes ○ No
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 ☒ 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
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
17	How many individuals' PII is in the system?	500-4,999
18	For what primary purpose is the PII used?	To identify eligibility and to correspond with applicants.
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.	N/A
20a	Cite the **legal authority** to use the SSN.	N/A

Save

21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	
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: 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.	
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 □ Other Federal Agency/Agencies □ State or Local Agency/Agencies □ Private Sector
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)).	None. No information is disclosed.

Save

24c	Describe the procedures for accounting for disclosures	None. No information is disclosed.	
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.	Public notification on web site.	
26	Is the submission of PII by individuals voluntary or mandatory?	● Voluntary ○ Mandatory	
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 decline to provide PII. However, submission of PII is a condition of being accepted into NIDDK sponsored programs.	
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.	Individuals will be contacted using demographic data maintained in the system and will be asked to re-consent to any changes.	
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.	Individuals will contact the program managers (administrators) who will contact the Privacy Officer and/or System Owner for resolution.	
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.	The NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Only the user who submitted the PII can access it.
		☒ Administrators	Program Administrators require access to the information so as to determine program eligibility and to correspond with applicants.
		☒ Developers	Developers (contractors) may have access to data as they troubleshoot issues within the application.
		☒ Contractors	Developers (contractors) may have access to data as they troubleshoot issues within the application.
		□ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Existing program administrators identify who may access the application. Security controls enable only identified personnel to access the administrative functions of the application where PII can be accessed. Administrative functionality is only available via the NIH network.	
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.	Users are assigned to specific roles which limit the information required to perform the duties of the role.	

Save

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.	All users must complete the mandated NIH Information Security Awareness course prior to receiving their NIH Active Directory (AD) account and password information. Thereafter, users must take an annual security awareness refresher course. Both courses require users to read and agree to follow the NIH General Information Technology Rules of Behavior.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	No specialized training is provided to the general public who use the system to apply for NIDDK sponsored programs.
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 xxxxxxxxx, which allows records to be kept as long as they are useful xxxxxxxxxx.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls include system security plan, contingency plan, files backed-up, administrator training, and access based on least privilege principle. Technical access controls include user identification and authentication, through password and PIV card, firewall, NIH VPN, intrusion detection system, and public key infrastructure. Physical controls include identification badges, key cards, cipher locks and closed circuit TV managed by NIH police force.
39	Identify the publicly-available URL:	https://forms.niddk.nih.gov
40	Does the website have a posted privacy notice?	● Yes ○ No
40a	Is the privacy policy available in a machine-readable format?	● Yes ○ No
41	Does the website use web measurement and customization technology?	● Yes ○ No
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	

Technologies	Collects PII?
□ Web beacons	○ Yes ○ No
□ Web bugs	○ Yes ○ No
□ Session Cookies	○ Yes ○ No
□ Persistent Cookies	○ Yes ○ No
Other...	○ Yes ○ No

Save

42	Does the website have any information or pages directed at children under the age of thirteen?	○ Yes ● No
43	Does the website contain links to non- federal government websites external to HHS?	○ Yes ● No

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		
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

Save

	Reviewer Questions	Answer
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	

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