

# Privacy Impact Assessment Form

v 1.43

Status 

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a 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.

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 POC Name POC Organization POC Email POC Phone 

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.

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? <span style="float: right;"><input checked="" type="radio"/> Yes <input type="radio"/> No</span>		
15 Indicate the type of PII that the system will collect or maintain.	<input type="checkbox"/> Social Security Number <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Name <input checked="" type="checkbox"/> Photographic Identifiers <input type="checkbox"/> Driver's License Number <input type="checkbox"/> Biometric Identifiers <input checked="" type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> Vehicle Identifiers <input checked="" type="checkbox"/> E-Mail Address <input checked="" type="checkbox"/> Mailing Address <input checked="" type="checkbox"/> Phone Numbers <input type="checkbox"/> Medical Records Number <input type="checkbox"/> Medical Notes <input type="checkbox"/> Financial Account Info <input type="checkbox"/> Certificates <input type="checkbox"/> Legal Documents <input checked="" type="checkbox"/> Education Records <input type="checkbox"/> Device Identifiers <input type="checkbox"/> Military Status <input checked="" type="checkbox"/> Employment Status <input type="checkbox"/> Foreign Activities <input type="checkbox"/> Passport Number <input type="checkbox"/> Taxpayer ID <input type="text"/> <input type="text"/> <input type="text"/>	
16 Indicate the categories of individuals about whom PII is collected, maintained or shared.	<input type="checkbox"/> Employees <input checked="" type="checkbox"/> Public Citizens <input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies) <input type="checkbox"/> Vendors/Suppliers/Contractors <input type="checkbox"/> Patients Other <input type="text"/>	
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	

21	Identify <b>legal authorities</b> 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?	<input checked="" type="radio"/> Yes <input type="radio"/> 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: <input type="text"/> Published: <input type="text"/> Published: <input type="text"/> <input type="checkbox"/> In Progress
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains <input type="checkbox"/> In-Person <input type="checkbox"/> Hard Copy: Mail/Fax <input type="checkbox"/> Email <input checked="" type="checkbox"/> Online <input type="checkbox"/> Other Government Sources <input type="checkbox"/> Within the OPDIV <input type="checkbox"/> Other HHS OPDIV <input type="checkbox"/> State/Local/Tribal <input type="checkbox"/> Foreign <input type="checkbox"/> Other Federal Entities <input type="checkbox"/> Other Non-Government Sources <input type="checkbox"/> Members of the Public <input type="checkbox"/> Commercial Data Broker <input type="checkbox"/> Public Media/Internet <input type="checkbox"/> Private Sector <input type="checkbox"/> Other
23a	Identify the OMB information collection approval number and expiration date.	<input type="text"/>
24	Is the PII shared with other organizations?	<input type="radio"/> Yes <input checked="" type="radio"/> No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	<input type="checkbox"/> Within HHS <input type="checkbox"/> Other Federal Agency/Agencies <input type="checkbox"/> State or Local Agency/Agencies <input type="checkbox"/> 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.

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?	<input checked="" type="radio"/> Voluntary <input type="radio"/> 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.	<table border="1"> <tr> <td><input checked="" type="checkbox"/> Users</td> <td>Only the user who submitted the PII can access it.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Administrators</td> <td>Program Administrators require access to the information so as to determine program eligibility and to correspond with applicants.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Developers</td> <td>Developers (contractors) may have access to data as they troubleshoot issues within the application.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Contractors</td> <td>Developers (contractors) may have access to data as they troubleshoot issues within the application.</td> </tr> <tr> <td><input type="checkbox"/> Others</td> <td></td> </tr> </table>	<input checked="" type="checkbox"/> Users	Only the user who submitted the PII can access it.	<input checked="" type="checkbox"/> Administrators	Program Administrators require access to the information so as to determine program eligibility and to correspond with applicants.	<input checked="" type="checkbox"/> Developers	Developers (contractors) may have access to data as they troubleshoot issues within the application.	<input checked="" type="checkbox"/> Contractors	Developers (contractors) may have access to data as they troubleshoot issues within the application.	<input type="checkbox"/> Others	
<input checked="" type="checkbox"/> Users	Only the user who submitted the PII can access it.											
<input checked="" type="checkbox"/> Administrators	Program Administrators require access to the information so as to determine program eligibility and to correspond with applicants.											
<input checked="" type="checkbox"/> Developers	Developers (contractors) may have access to data as they troubleshoot issues within the application.											
<input checked="" type="checkbox"/> Contractors	Developers (contractors) may have access to data as they troubleshoot issues within the application.											
<input type="checkbox"/> 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.										

<p>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.</p>	<p>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.</p>													
<p>35 Describe training system users receive (above and beyond general security and privacy awareness training).</p>	<p>No specialized training is provided to the general public who use the system to apply for NIDDK sponsored programs.</p>													
<p>36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>													
<p>37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.</p>	<p>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 xxxxxxxxx.</p>													
<p>38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.</p>	<p>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.</p>													
<p>39 Identify the publicly-available URL:</p>	<p><a href="https://forms.nidDK.nih.gov">https://forms.nidDK.nih.gov</a></p>													
<p>40 Does the website have a posted privacy notice?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>													
<p>40a Is the privacy policy available in a machine-readable format?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>													
<p>41 Does the website use web measurement and customization technology?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>													
<p>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)</p>	<table border="1"> <thead> <tr> <th>Technologies</th> <th>Collects PII?</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Web beacons</td> <td><input type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td><input type="checkbox"/> Web bugs</td> <td><input type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td><input type="checkbox"/> Session Cookies</td> <td><input type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td><input type="checkbox"/> Persistent Cookies</td> <td><input type="radio"/> Yes <input type="radio"/> No</td> </tr> <tr> <td>Other... <input type="text"/></td> <td><input type="radio"/> Yes <input type="radio"/> No</td> </tr> </tbody> </table>	Technologies	Collects PII?	<input type="checkbox"/> Web beacons	<input type="radio"/> Yes <input type="radio"/> No	<input type="checkbox"/> Web bugs	<input type="radio"/> Yes <input type="radio"/> No	<input type="checkbox"/> Session Cookies	<input type="radio"/> Yes <input type="radio"/> No	<input type="checkbox"/> Persistent Cookies	<input type="radio"/> Yes <input type="radio"/> No	Other... <input type="text"/>	<input type="radio"/> Yes <input type="radio"/> No	
Technologies	Collects PII?													
<input type="checkbox"/> Web beacons	<input type="radio"/> Yes <input type="radio"/> No													
<input type="checkbox"/> Web bugs	<input type="radio"/> Yes <input type="radio"/> No													
<input type="checkbox"/> Session Cookies	<input type="radio"/> Yes <input type="radio"/> No													
<input type="checkbox"/> Persistent Cookies	<input type="radio"/> Yes <input type="radio"/> No													
Other... <input type="text"/>	<input type="radio"/> Yes <input type="radio"/> No													

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?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
4	Does the PIA appropriately describe the PII quality and integrity of the data?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
5	Is this a candidate for PII minimization?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
6	Does the PIA accurately identify data retention procedures and records retention schedules?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
7	Are the individuals whose PII is in the system provided appropriate participation?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
8	Does the PIA raise any concerns about the security of the PII?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	<input type="radio"/> Yes <input type="radio"/> No

Reviewer Questions		Answer
Reviewer Notes	<input type="text"/>	
10	Is the PII appropriately limited for use internally and with third parties?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
11	Does the PIA demonstrate compliance with all Web privacy requirements?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
12	Were any changes made to the system because of the completion of this PIA?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes	<input type="text"/>	
General Comments	<input type="text"/>	
OPDIV Senior Official for Privacy Signature	<input type="text"/>	HHS Senior Agency Official for Privacy <input type="text"/>