Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-10120 | Form Date: 10/22/2019 10:06:39 AM

	Question	Answer
1	OPDIV:	NIH
2	PIA Unique Identifier:	P-1180397-810301
2a	Name:	National Cancer Institute Communications Fellowship Website
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: Management and Program Analyst POC Name: Kelly Holliday POC Organization: NCI POC Email: kelly.holliday@nih.gov POC Phone: 240.276.6637
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	Sep 30, 2019

Save

11	Describe the purpose of the system.	The NCI Communications Fellowship (NCF) Program gives highly qualified graduate students and recent graduate degree recipients the opportunity to participate in vital communications projects in a one-year fellowship in one of many offices that make up the National Cancer Institute (NCI). To that end, the system consists of a public website describing the program, a secure application form where candidates can apply for the program, and a set of tools for Office of Workforce Planning and Development (OWPD) staff to manage the application process.
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 information about potential NCF candidates, including name, addresses, phone numbers, email addresses, educational history, transcript, and resumes. The information is used to evaluate candidates for the NCF program. NCF uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The system consists of a public website describing the program, a secure application form where candidates can apply for the program, and a set of tools for OWPD staff to manage the application process. The system collects information about potential NCF candidates, including name, addresses, phone numbers, email addresses, educational history, transcripts, and résumés. The information is used to evaluate candidates for the NCF program. Completed applications are stored on the system for 1 year, and then are archived by Center for Biomedical Informatics and Information Technology (CBIIT). NCF uses specific login information to assign permissions/user roles which is considered Personally Identifiable Information (PII). However, this is done by using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), formally known as the Active Directory (AD), which combines the identity and authentication tools and capabilities used throughout the NIH enterprise. The IMS has its own approved PIA on record, including all legal authorities documented.
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 ☐ Date of Birth ☒ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☒ Certificates ☐ Legal Documents ☒ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Other...If an applicant is a permanent resident, a Green Card number is required for registration with the system. Resume
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?	100-499
18	For what primary purpose is the PII used?	To ensure the NCF candidates are eligible for the fellowship.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
20	Describe the function of the SSN.	N/A
20a	Cite the **legal authority** to use the SSN.	N/A
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	42 U.S. Code 282 - Director of National Institutes of Health.
22	Are records on the system retrieved by one or more PII data elements?	◉ Yes ○ No

Save

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:	09-25-0108 (Personnel: Guest Researchers, Special Volunteers, and Scientists Emeriti)
		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.	Currently have clearance that expires 7/31/19. OMB No. 0925-0046.	
24	Is the PII shared with other organizations?	○ Yes ◉ No	
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.	Applicants willingly provide their PII in their NCF application.	
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.	In order to apply for the program, all PII listed above must be provided. Individuals may choose to opt out of the program.	

Save

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.	This system has undergone one significant change to the design and functionality in 2017, and changes were made outside of the application cycle so they did not affect current applicants. There was no need to notify previous applicants as their PII was already archived.
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.	Applicants may notify the program if they believe their PII is inaccurate on a current application during the application cycle. The program will make the appropriate changes to the application or notify the Center for Biomedical Informatics and Information Technology (CBIIT) Business Application Support team to make the changes in the system. No process currently exists for when an individual believes that their PII has been inappropriately obtained, used, or disclosed, because such a case is unprecedented in the program.
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 data is reviewed by OWPD staff during the application period for completeness and accuracy.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: Users or applicants, only have access to their own PII. ☒ Administrators: OWPD staff review the data and manage the application process. ☒ Developers: System and testing updates. ☐ Contractors: ☒ Others: NCI host offices, access for interviewing candidates.
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The system administrators and developers are the only individuals who can grant access to system users. Users may also be removed by administrators and developers at any time if necessary.
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 NCF only requires applicants submit PII that is necessary for the fellowship position.
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.	The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	System users receive basic training from NCI Center for Biomedical Informatics and Information Technology (CBIIT) Business Application Support Team. A user guide is also available for download on the home page.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	○ Yes ◉ No

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are maintained within NCF for a time of no less than six years after a password is altered or an user account is terminated in accordance with NARA record retention schedule: 3.2.031, System access records; Systems requiring special accountability for access; DAA-GRS-2013-0006-0004 Records are maintained within NCF for one year after the system is superseded by a new iteration or when no longer needed for agency/Information Technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system in accordance with NARA record retention schedule: 3.2.010, Systems and data security records: DAA-GRS-2013-0006-0001
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	There are technical controls in place to minimize the possibility of unauthorized access, use, and dissemination of the data in the system by requiring a user ID and password for access. The server hardware that supports this application is secured with the same controls as all other apps hosted. The actual system itself has no physical controls. Administrative Controls & Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data. Physical Controls: The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.
39	Identify the publicly-available URL:	https://ncf.nci.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
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

Save

General Comments	This component is under the NCI LAN GSS, whose Universal Unique Identifier (UUID) is: 93F1C7DB-B2F0-4282-9FAD-7168D5B63F91
OPDIV Senior Official for Privacy Signature	Celeste E. Dade-vinson -S Digitally signed by Celeste E. Dade-vinson -S Date: 2019.11.12 15:34:01 -05'00'