Privacy Impact Assessment Form

v 1.47.4

Question Answer

1. OPDIV: NIH
2. PIA Unique Identifier: P-4977306-113940

2a Name: NCI Electronic Individual Development Plan

1. The subject of this PIA is which of the following?

3a Identify the Enterprise Performance Lifecycle Phase of the system.

3b Is this a FISMA-Reportable system?

Does the system include a Website or online

General Support System (GSS) Major Application

Minor Application (stand-alone) Minor Application (child) Electronic Information Collection Unknown

Operations and Maintenance

Yes No

Yes

1. application available to and for the use of the general

public? No

1. Identify the operator.

Agency

Contractor

POC Title Director

1. Point of Contact (POC):

POC Name Jonathan Wiest

POC Organization Center for Cancer Training POC Email jonathan.wiest@nih.gov

POC Phone 240-276-5628

1. Is this a new or existing system?

New

Existing

1. Does the system have Security Authorization (SA)?

Yes

No

8a Date of Security Authorization

Dec 31, 2018

11 Describe the purpose of the system.

The electronic Individual Development Plan (eIDP) system is used by training programs across National Cancer Institute

|  |  |  |
| --- | --- | --- |
| 12 | Describe the type of information the system willcollect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.) | The majority of the Personally Identifiable Information (PII) information comes from NIH Enterprise Directory (NED), the NIH Fellowship Payment System (FPS), and NIH nVision.Personally Identifiable Information (PII) includes name, email, |
| 13 | Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily. | The electronic Individual Development Plan (eIDP) system is used by training programs across National Cancer Institute (NCI) organizations to help Cancer Research Training Award |
| 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 NameE-Mail Address Phone Numbers Medical Notes  Certificates Education Records  Military Status Foreign Activities  Taxpayer ID GenderRace and ethnicity |  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 PatientsOther |  |
| 17 | How many individuals' PII is in the system? | 500-4,999 |  |
| 18 | For what primary purpose is the PII used? | The PII information used by the eIDP system identifies NCI Trainees and Fellows that need to create an Individual Development Plan (IDP). The PII data is used to identify the NCI staff. The gender and race of the staff is used for aggregate data reporting. |  |
| 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 42 U.S.C. 241(d), 281. and disclosure specific to the system and program. |
| Are records on the system retrieved by one or more Yes22 PII data elements? No |
| Published: 09-25-0216 NIH Electronic Directory (NED)Identify the number and title of the Privacy ActSystem of Records Notice (SORN) that is being used Published: 22a to cover the system or identify if a SORN is beingdeveloped.Published: In Progress |
| Directly from an individual about whom the information pertains In-Person Hard Copy: Mail/Fax Email Online Other Government SourcesWithin the OPDIV  Other HHS OPDIV23 Identify the sources of PII in the system. State/Local/Tribal Foreign Other Federal Entities Other Non-Government Sources Members of the Public  Commercial Data Broker  Public Media/Internet Private Sector Other |
| Identify the OMB information collection approval An OMB collection approval number is not needed as the eIDP 23a number and expiration date. Website/Database only uses the PII of federal employees forinternal use only. |
|  Yes24 Is the PII shared with other organizations?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. | PII data is sourced from existing, assess and approved NIH systems (NED, FPS, NIH nVision). Trainees will enter additional PII information that is not found in any NIH systems (gender, race, and ethnicity, at their option). The Trainees will submit the completed IDP for approval. The individuals will review all data that the system stores prior to their approval of the final submitted IDP.Sources systems maintain their own HHS Approved Privacy Impact Assessments, including all legal authorities documented. |
| 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. | It is optional for the Trainees to complete an IDP. However, this can potentially disqualify them from the fellowship program since it is a requirement of the program.Information that is pulled from source systems offer opt-out options during their PII submission processes. All source systems maintain their own HHS Approved PIAs, with legal authorities documented. |
| 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. | NCI Trainees will have the opportunity to view changes to their PII information during the IDP renewal process. They will go through a submission and approval process for IDP renewals. They will know when a change occurs during the renewal period.Information that is pulled from source systems obtain consent during their PII submission processes. All source systems maintain their own HHS Approved PIAs, with legal authorities documented. |
| 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. | The eIDP System source of most of the PII data is from NIH systems. The additional PII information requested from the Trainee is optional. The Trainee does not have to enter the optional PII data. The Trainee can update their PII information by logging into NED and/or contacting their Administrative Officer to update incorrect PII data. |
| 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 PIA review will be conducted each time major eIDP functionalities are released that utilizes addition data (NED, nVision) or new PII data beyond the data included in the previous PIA. Minimally, a PIA review will be conducted yearly. |

|  |  |  |  |
| --- | --- | --- | --- |
| 31 Identify who will have access to the PII in the system and the reason why they require access. | Users | Trainees, mentors, administrative officers complete and view the eIDP as it goes through the system. |  |
| Administrators | Responsible for access control. |
| Developers | Testing and customer defect resolution. |
|  Contractors |  |
|  Others |  |
| Describe the procedures in place to determine which All requests for access to the eIDP system will be assigned an32 system users (administrators, developers, appropriate profile (role) and approved by the System Owner contractors, etc.) may access PII. before being implemented by the technical support team. |
| Describe the methods in place to allow those with33 access to PII to only access the minimum amount of Role based access controls are used to limit users' access to PIIinformation necessary to perform their job. based on their defined job function and system role. |
| Identify training and awareness provided to The NIH Security Awareness Training course is used to satisfy personnel (system owners, managers, operators, this requirement. According to NIH policy, all personnel who contractors and/or program managers) using the use NIH applications must attend security awareness training34 system to make them aware of their responsibilities every year. There are four categories of mandatory IT trainingfor protecting the information being collected and (Information Security, Counterintelligence, Privacy Awareness, maintained. and Records Management). Training is completed on the[http://irtsectraining.nih.gov](http://irtsectraining.nih.gov/) site with valid NIH credentials. |
| Describe training system users receive (above and35 beyond general security and privacy awareness training). | None. |  |
| Do contracts include Federal Acquisition Regulation36 and other appropriate clauses ensuring adherence to privacy provisions and practices? |  Yes No |  |
| Describe the process and guidelines in place with37 regard to the retention and destruction of PII. Cite specific records retention schedules. | NCI’s mission related training records are currently “unscheduled” and all related records should be retained permanently until such time as our agency records schedule is officially modified.NIH has a proposed Records Retention Schedule currently in the approval process with the National Archives and Records Administration (NARA). With a proposed disposition instruction of destroying 5 years after the cutoff of course material after it is superseded or becomes obsolete. Longer retention is authorized if required for business use. |  |

|  |
| --- |
| Administrative Controls: Access to administrative features of the system will be controlled by Information System Security Officer (ISSO) and access permissions will be reviewed periodically to ensure that users are aged out of the system.Technical Controls: it is operated within the NCI's LAN GSS, which provides numerous technical security controls on behalfDescribe, briefly but with specificity, how the PII will of its customers including firewalls, IDS/IPS, vulnerability38 be secured in the system using administrative, scanners, centralized patching, host-based malware detectiontechnical, and physical controls. and prevention, and log aggregation and analyses.The system is operated inside the NCI Managed Data Center, within a dedicated federally leased building with armed guards, badge access, video surveillance.Physical Controls: TThe system is operated inside the NCI Managed Data Center, within a dedicated federally leased building with armed guards, badge access, video surveillance. |
| General Comments | This component is under the NCI Local Network General Support System (NCI Local Network GSS), whose Universal Unique Identifier (UUID) is: 93F1C7DB-B2F0-4282-9FAD-7168D5B63F91. |
| Ralph D. Digitally signed by RalphOPDIV Senior Official D. French -Sfor Privacy Signature French -S Date: 2019.01.28 08:42:57-05'00' | HHS Senior Bridget M.Digitally signed by Bridget M. Guenther -SDN: c=US, o=U.S. Government, ou=HHS, ou=OS, ou=People,Agency Official 0.9.2342.19200300.100.1.1=2001734030,for Privacy Guenther -S cn=Bridget M. Guenther -SDate: 2019.02.01 20:45:13 -05'00' |