|  |  |
| --- | --- |
|  |  |
| 1. OPDIV | National Institutes of Health |
| 2. PIA Unique Identifier |  |
| 2a. Name | NIGMS Scientific Information Reporting System (SIRS) |
| 3. The subject of this PIA is which of the following? | Minor Application (child) |
| 3a. Identify the Enterprise Performance Lifecycle Phase of the system. | Operational |
| 3b. Is this a FISMA-Reportable system? | No |
| 4. Does the system include a Website or online application available to and for the use of the general public? | No |
| Accept / Reject Status | Undefined |
|  |  |
| Question 4 Comment |  |
|  |  |
| 5. Identify the operator. | Agency |
| 6. Point of Contact (POC) |
| POC Title | Project Manager  |
| POC Name | Christy Tran |
| POC Organization | NIGMS |
| POC Email | christy.tran@nih.gov |
| POC Phone | 301 594 2680  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 6 Comment |  |
|  |  |
| 7. Is this a new or existing system? | New |
| 8. Does the system have Security Authorization (SA)? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 8 Comment |  |
|  |  |
| 8a. Date of Security Authorization | 5/15/2018 |
|  |  |
| 9. Indicate the following reason(s) for updating this PIA. Choose from the following options. | PIA Validation (PIA Refresh/Annual Review)  |
| Other |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 9 Comment |  |
|  |  |
|  |  |
| 10. Describe in further detail any changes to the system that have occurred since the last PIA. | The National Institutes of Health (NIH) implemented an NIH-wide information technology (IT) realignment, which requires all IT resources to reevaluate related privacy controls. As a result of the realignment, this system is now subset of the NIGMS Information Technology Infrastructure System (NITI). The SIR’s functions remain unchanged. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 10 Comment |  |
|  |  |
| 11. Describe the purpose of the system. | SIRS replaced the functionality of APRSIS, a non-NIGMS System. SIRS support the tracking of NIGMS grants through the submittal of grantee Annual Progress Reports (APRs). It will provide NIGMS the ability to generate internal reports and have easy access to data necessary for Congressional reporting. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 11 Comment |  |
|  |  |
| 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: grant data; research data; institutional profile data; personnel roster data; evaluation data; publication data; subproject data; research highlight data and facility data. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 12 Comment |  |
|  |  |
| 13. Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily. | SIRS is a web application developed and managed by NIGMS. Access to the system is restricted to NIGMS staff / IRMB support staff and grantees with NIH Commons accounts. Data from the system is maintained in the NIGMS Oracle Databases. SIRS collects and maintains grant and research data provided by the grantee, in addition to grant information provided by IMPAC II. The research information includes specifics like evaluation updates regarding significant unexpected outcomes; presentation information; and the reporting of at least 3 notable scientific advances. SIRS will also collect and maintain contact data on personnel from the institution. The contact information collected will include name, business e-mail addresses and business phone numbers. The data collected in SIRS will be maintained in SIRS and will not be shared with other systems.  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 13 Comment |  |
|  |  |
| 14. Does the system collect, maintain, use or share PII? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 14 Comment |  |
|  |  |
|  |  |
| 15. Indicate the type of PII that the system will collect or maintain. | NameE-Mail AddressPhone NumbersDegreesPosition TitleResearch Data |
|  |  |
|  |  |
|  |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 15 Comment |  |
|  |  |
| 16. Indicate the categories of individuals about whom PII is collected, maintained or shared. | Public Citizens |
|  |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 16 Comment | Principal Investigators - Contact Information; and Institutions - Research data |
|  |  |
| 17. How many individuals' PII is in the system? | 100-499 |
| Accept / Reject Status | Undefined |
|  |  |
| Question 17 Comment |  |
|  |  |
| 18. For what primary purpose is the PII used? | Principal Investigators: To identify and contact grantees; Institutions: To support the annual reporting process. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 18 Comment |  |
|  |  |
| 19. Describe the secondary uses for which the PII will be used (e.g. testing, training or research) | Principal Investigators: The PII /contact information is only utilized to contact the Principal Investigators.Institutions: The PII / research information is only utilized to track grant success. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 19 Comment |  |
|  |  |
| 20. Describe the function of the SSN. | Not Applicable.  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 20 Comment |  |
|  |  |
| 20a. Cite the legal authority to use the SSN. | Not Applicable.  |
| 21. Identify legal authorities governing information use and disclosure specific to the system and program. | The legal authority to operate and maintain this Privacy Act records system is 5. U.S.C. 301; 42 U.S.C. 217a, 241, 282(b)(6), 284a, and 288. 48 CFR Subpart 15.3 and Subpart 42.15. |
| 22. Are records on the system retrieved by one or more PII data elements? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 22 Comment |  |
|  |  |
|  |  |
| 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: | 09-25-0036 (Inherited via IMPAC 2 SORN) |
| Published: |  |
| Published: |  |
| In Progress | Undefined |
|  |  |
| 23. Identify the sources of PII in the system. | Government Sources – Within the OpDiv |
| Accept / Reject Status | Undefined |
|  |  |
| Question 23 Comment |  |
|  |  |
| 23a. Identify the OMB information collection approval number and expiration date. | OMB# 0925-0735 03/31/2019 |
| 24. Is the PII shared with other organizations? | No |
| Accept / Reject Status | Undefined |
|  |  |
| Question 24 Comment |  |
|  |  |
|  |  |
| 24a. Identify with whom the PII is shared or disclosed and for what purpose. |
| Within HHS | No |
|  |  |
| Other Federal Agency/Agencies | No |
|  |  |
| State or Local Agency/Agencies | No  |
|  |  |
| Private Sector | No |
|  |  |
| 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)). | Not applicable. |
| 24c. Describe the procedures for accounting for disclosures. | Not applicable.  |
|  |  |
| 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. | Individuals are aware as part of the grant application process that they will be required to provide information for yearly progress reports submitted to the NIH. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 25 Comment |  |
|  |  |
| 26. Is the submission of PII by individuals voluntary or mandatory? | Voluntary |
| Accept / Reject Status | Undefined |
|  |  |
| Question 26 Comment |  |
|  |  |
| 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. | Submission is voluntary since application to receive grants from the Institutional Development Awards (IDeA) program and The Native American Research Centers for Health (NARCH) initiative is voluntary.  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 27 Comment |  |
|  |  |
| 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. | There will be no substantive changes to data uses. Information is collected in order to evaluate the progress of grantees and compile reports on the status of each program. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 28 Comment |  |
|  |  |
| 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 can submit an IT help desk ticket which is sent to the NIGMS Information Resources Management Branch (IRMB) to report any issues. Individuals also have the option to be directed to the IC’s privacy policy page which includes an e-mail address where users can direct their concerns. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 29 Comment |  |
|  |  |
| 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. | Principal Investigators (PI): Data is obtained from IMPAC II and when PI's submit their annual progress reports annually and they have the opportunity to update their contact information to ensure integrity, accuracy and availability. Institutions: Research data is submitted annually. During the submission process, data can be changed to support accuracy and relevancy. After the submission process, the data cannot be changed. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 30 Comment |  |
|  |  |
| 31. Identify who will have access to the PII in the system and the reason why they require access. |
| Users | Yes (external PIs and internal NIGSM Users)  |
|  |  |
| Administrators | Yes |
|  |  |
| Developers | Yes |
|  |  |
| Contractors | Yes |
|  |  |
| Others | Undefined |
|  |  |
| 32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | External Users - Principal Investigators and Institutions will only have access to their respective contact and research data in the production system. Internal NIGMS staff will have access to all the data, including PII, in the production system. The system developers and administrators, who are direct contractors supporting NIGMS, have access to the production system. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 32 Comment |  |
|  |  |
| 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. | Determinations are made based on Role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 33 Comment |  |
|  |  |
| 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. | According to NIH policy, all personnel (employees and direct contractors) must complete the annual mandatory security, privacy and information management awareness training prior to the use of, or access to, information systems. There are four categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, and Records Management). |
| Accept / Reject Status | Undefined |
|  |  |
| Question 34 Comment |  |
|  |  |
| 35. Describe training system users receive (above and beyond general security and privacy awareness training). | External Users are exempt from training due to access provided by Era Commons accounts. All NIGMS Staff, including the SIRS System Administrators and Developers are required to take the general security and privacy awareness training. In addition. SIRS System Administrators and Developers are considered personnel with IT Security responsibilities. These individuals are required to take additional security training.  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 35 Comment |  |
|  |  |
| 36. Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 36 Comment |  |
|  |  |
| 37. Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules. | The majority of PII is collected from IMPAC II and is administered by ERA commons. PII not collected through IMPAC II is evaluated in accordance with the NARA record retention schedule: E-0002, Official case files of funded grants, unfunded grants, and award applications, appeals and litigation records: DAA-0443-2013-0004-0002.  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 37 Comment |  |
|  |  |
| 38. Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | Website access will be managed via NTFS and Single Sign-On. The server on which the Administrative interface is hosted will be available only on the NIGMS internal network and is protected by AD account and password. The web front end is hosted on a server in the NIGMS Public DMZ and is protected by AD account and password and sits behind NIH enterprise Single Sign-On. Only users with access will be able to access the system. Active Directory will be employed for internal user authentication and external users will use Commons accounts. Additionally, various physical access control measures are in place to protect the system / data including the implementation of ID badges, guard stations at specific locations and the utilization of key card access at specific entry points / during specific hours. Specifically, the system code / Hdw components are located in a secure room with restricted Card Key access in Building 12. The data is contained in Oracle and is only accessible with role-based access. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 38 Comment |  |
|  |  |
|  |  |
|  |  |
| 39. Identify the publicly-available URL. | https://sirs.nigms.nih.gov |
| Accept / Reject Status | Undefined |
|  |  |
| Question 39 Comment |  |
|  |  |
| 40. Does the website have a posted privacy notice? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 40 Comment |  |
|  |  |
|  |  |
| 40a. Is the privacy policy available in a machine-readable format? | No |
|  |  |
| 41. Does the website use web measurement and customization technology? | No  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 41 Comment |  |
|  |  |
|  |  |
| 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). |
| Web Beacons | No |
| Collects PII? | Undefined |
| Web Bugs | No |
| Collects PII? | Undefined |
| Session Cookies | No |
| Collects PII? | Undefined |
| Persistent Cookies | No |
| Collects PII? | Undefined |
| Other ... |  |
| Collects PII? | Undefined |
|  |  |
| 42. Does the website have any information or pages directed at children under the age of thirteen? | No |
| Accept / Reject Status | Undefined |
|  |  |
| Question 42 Comment |  |
|  |  |
|  |  |
| 42a. Is there a unique privacy policy for the website, and does the unique privacy policy address the process for obtaining parental consent if any information is collected? | Not applicable |
|  |  |
| 43. Does the website contain links to non-federal government websites external to HHS? | No |
| Accept / Reject Status | Undefined |
|  |  |
| Question 43 Comment |  |
|  |  |
|  |  |
| 43a. Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS? | Not applicable |
|  |  |
|  |  |
|  |
| **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. |
| 1. Are the questions on the PIA answered correctly, accurately, and completely? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 1 Comment |  |
|  |  |
| 2. Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 2 Comment |  |
|  |  |
| 3. Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 3 Comment |  |
|  |  |
| 4. Does the PIA appropriately describe the PII quality and integrity of the data? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 4 Comment |  |
|  |  |
| 5. Is this a candidate for PII minimization? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 5 Comment |  |
|  |  |
| 6. Does the PIA accurately identify data retention procedures and records retention schedules? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 6 Comment |  |
|  |  |
| 7. Are the individuals whose PII is in the system provided appropriate participation? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 7 Comment |  |
|  |  |
| 8. Does the PIA raise any concerns about the security of the PII? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
| Accept / Reject Status | Undefined |
|  |  |
| Question 8 Comment |  |
|  |  |
| 9. Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
| Accept / Reject Status | Undefined |
|  |  |
| Question 9 Comment |  |
|  |  |
| 10. Is the PII appropriately limited for use internally and with third parties? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 10 Comment |  |
|  |  |
| 11. Does the PIA demonstrate compliance with all Web privacy requirements? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 11 Comment |  |
|  |  |
| 12. Were any changes made to the system because of the completion of this PIA? | Undefined |
| Reviewer Notes |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 12 Comment |  |
|  |  |
| General Comments |  |
|  |
| Status and Approvals |
| IC Status | Undefined |
| OSOP Status | Undefined |
| OPDIV Senior Official for Privacy Signature |  |
| HHS Senior Agency Official for Privacy |  |