**NICHD Data and Specimen Hub (DASH)**

|  |  |
| --- | --- |
|  |  |
| 1. OPDIV | National Institutes of Health |
| 2. PIA Unique Identifier |  |
| 2a. Name | NICHD Data and Specimen Hub (DASH) |
| 3. The subject of this PIA is which of the following? | General Support System |
| 3a. Identify the Enterprise Performance Lifecycle Phase of the system. | Implementation |
| 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? | Yes |
| Accept / Reject Status | Undefined |
|  |  |
| Question 4 Comment |  |
|  |  |
| 5. Identify the operator. | Agency |
| 6. Point of Contact (POC) | |
| POC Title | Applications CTO |
| POC Name | Archana Mohale |
| POC Organization | NICHD |
| POC Email | mohalea@mail.nih.gov |
| POC Phone | 301-594-2353 |
| 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 | 11/20/2015 |
|  |  |
| 9. Indicate the following reason(s) for updating this PIA. Choose from the following options. |  |
| Other |  |
| Accept / Reject Status |  |
|  |  |
| Question 9 Comment |  |
|  |  |
|  |  |
| 10. Describe in further detail any changes to the system that have occurred since the last PIA. | None |
| Accept / Reject Status | Undefined |
|  |  |
| Question 10 Comment |  |
|  |  |
| 11. Describe the purpose of the system. | To enable searching and sharing of study data from the National Institute of Child Health and Human Development (NICHD) funded research. |
| 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 will collect and maintain personal information from individuals requesting accounts. |
| 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. | The system maintains study research data. It will collect and maintain personal information from individuals requesting accounts. |
| 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. | Name, E-Mail Address, Phone Numbers, Mailing Address |
|  |  |
|  |  |
|  |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 15 Comment |  |
|  |  |
| 16. Indicate the categories of individuals about whom PII is collected, maintained or shared. | Public Citizens, Business Partners/Contacts (Federal State and local agencies) |
|  |  |
| Accept / Reject Status | Undefined |
|  |  |
| Question 16 Comment |  |
|  |  |
| 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? | To identify individuals requesting data or sharing data. |
| 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) | The data may be used in support of future initiatives. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 19 Comment |  |
|  |  |
| 20. Describe the function of the SSN. | N/A |
| Accept / Reject Status | Undefined |
|  |  |
| Question 20 Comment |  |
|  |  |
| 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. | United States Congress, Privacy Act of 1974, 5 U.S.C. Section 552a.  United States Congress, Public Health Service Act 42 U.S.C. Section 241, 242, 248, 281, 282, 284, 285a, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285l, 285m, 285n, 285o, 285p, 285q, 287, 287b, 287c, 289a, 289c, and; 44 U.S.C. Section 310l |
| 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: | 09-25-0200 Clinical, Basic and Population based |
| Published: |  |
| Published: |  |
| In Progress | No |
|  |  |
| 23. Identify the sources of PII in the system. | Online, Members of the Public |
| Accept / Reject Status | Undefined |
|  |  |
| Question 23 Comment |  |
|  |  |
| 23a. Identify the OMB information collection approval number and expiration date. | Office of Management and Budget (OMB) approval is in process. |
| 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 |  |
|  |  |
| 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)). |  |
| 24c. Describe the procedures for accounting for disclosures. |  |
|  |  |
| 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 required to enter the information themselves. |
| 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. | The collection of information is required for the creation of an account. Individuals may browse or search studies without creating an account. However, in order to request or submit data, they must enter their information and create an account. |
| 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. | Email will be used for necessary notifications. |
| 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 contact the system administrators. |
| 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. | Individuals have access to their profile in the system and can make any changes needed to their personally identifiable information (PII) through the profile page. |
| 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 | No |
|  |  |
| Administrators | Yes |
|  | To resolve account queries or disputes, or to assist with password resets or updates and email registered users as necessary. |
| Developers | No |
|  |  |
| Contractors | No |
|  |  |
| Others | No |
|  |  |
| 32. Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | The principles of least privileged access are applied. The system uses roles and each role has different access levels. Default role has least privilege. Approval by system administrator is needed to change role. |
| 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. | N/A |
| 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. | All system owners, managers, operators, contractors and/or program managers take annual NIH security and privacy training. Administrators are required to take role-based training which has training specific to their responsibilities. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 34 Comment |  |
|  |  |
| 35. Describe training system users receive (above and beyond general security and privacy awareness training). | System owners, managers, and operators are also required to take role-based 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 National Institute of Standards and Technology (NIST) Special Publication 800-122 guidelines are followed. Accounts are classified from active to inactive status after a period of 6 months of inactivity. Inactive accounts are reviewed by the system owner on a yearly basis and are deactivated or deleted from the system by the system administrator as per system owner request. |
| 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. | Access to account information is provided only to authorized administrators of the system through a Virtual Private Network (VPN) connection using multi-factor authentication. Transactions are audited and stored. Administrative, technical and physical security controls follow NIST 800-53 rev4 which requires monthly scanning and annual re-accreditation. |
| Accept / Reject Status | Undefined |
|  |  |
| Question 38 Comment |  |
|  |  |
|  |  |
|  |  |
| 39. Identify the publicly-available URL. | https://dash.nichd.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? | Yes |
|  |  |
| 41. Does the website use web measurement and customization technology? | Yes |
| 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 | Yes |
| Collects PII? | No |
| Web Bugs | No |
| Collects PII? | No |
| Session Cookies | No |
| Collects PII? | No |
| Persistent Cookies | No |
| Collects PII? | No |
| Other ... | No |
| Collects PII? | No |
|  |  |
| 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? |  |
|  |  |
| 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? |  |
|  |  |
|  |  |
|  | |
| **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 |  |
|  | |
| OPDIV Senior Official for Privacy Signature |  |
| HHS Senior Agency Official for Privacy |  |