

PIA SUMMARY

Note: The following questions are repeated in the long form (p.3) You only have to answer once. I have highlighted them in the long form.

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If no personally identifiable information (PII) is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

*Is this a new PIA?:	
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	
*2. OPDIV Name:	
*3. Unique Project Identifier (UPI) Number for current fiscal year:	
*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):	
*5. OMB Information Collection Approval Number:	
*6. Other Identifying Number(s):	
*7. System Name (Align with system item name):	
*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	
POC Name	
*10. Provide an overview of the system:	
*13. Indicate if the system is new or an existing one being modified:	
*17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?:	
Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or business partners, and whether provided voluntarily or collected by mandate.	

<p>Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation.</p>	
<p>*21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):</p>	
<p>*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):</p>	
<p>*30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:</p>	
<p>*31. Please describe in detail any processes in place to: (1) 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 the original collection); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) how the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.]</p>	
<p>*32. Does the system host a website?:</p>	
<p>*37. Does the website have any information or pages directed at children under the age of thirteen?:</p>	
<p>*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):</p>	
<p>*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls.:</p>	

PIA REQUIRED INFORMATION

1 HHS Privacy Impact Assessment (PIA)

The PIA determines if Personally Identifiable Information (PII) is contained within a system, what kind of PII, what is done with that information, and how that information is protected. Systems with PII are subject to an extensive list of requirements based on privacy laws, regulations, and guidance. The HHS Privacy Act Officer may be contacted for issues related to Freedom of Information Act (FOIA) and the Privacy Act. Respective Operating Division (OPDIV) Privacy Contacts may be contacted for issues related to the Privacy Act. The Office of the Chief Information Officer (OCIO) can be used as a resource for questions related to the administrative, technical, and physical controls of the system. Please note that answers to questions with an asterisk (*) will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible.

2 General Information

*Is this a new PIA?:	Yes
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	4/24/2013
*2. OPDIV Name:	NIH
*3. Unique Project Identifier (UPI) Number for current fiscal year:	Not applicable
If the system does not have a UPI, please explain why it does not:	
*4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):	
*5. OMB Information Collection Approval Number:	In process
OMB Collection Approval Number Expiration Date:	
*6. Other Identifying Number(s):	NIH OHSR Exempt Number is 11817 Smithsonian Protocol Number is HS13023
*7. System Name: (Align with system item name)	Social Genome Surveys
8. System Location: (OPDIV or contractor office building, room, city, and state)	

System Location:	
OPDIV or contractor office building	6707 Democracy Blvd
Room	Suite 203
City	Bethesda
State	Maryland

*9. System Point of Contact (POC). The System POC is the person to whom questions about the system and the responses to this PIA may be addressed:	
---	--

Point of Contact Information	
POC Name	Dave Kanney, Laura Koehly, Chris Marcum
The following information will not be made publicly available:	
POC Title	System Developer- Dave Kanney
POC Organization	NHGRI
POC Phone	301.435.6076
POC Email	davidk@mail.nih.gov
*10. Provide an overview of the system:	The system will be used to conduct research surveys. These surveys are being conducted to help researchers understand how people think and feel about issues related to genetics and health.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1	System Characterization and Data Configuration
11. Does HHS own the system?:	Yes
If no, identify the system owner:	
12. Does HHS operate the system?:	Yes
If no, identify the system operator:	
*13. Indicate if the system is new or an existing one being modified:	New
14. Identify the life-cycle phase of this system:	Requirements Analysis
15. Have any of the following major changes occurred to the system since the PIA was last submitted?:	
Please indicate "Yes" or "No" for each category below:	Yes/No
Conversions	No
Anonymous to Non-Anonymous	No
Significant System Management Changes	No
Significant Merging	No
New Public Access	No
Commercial Sources	No
New Interagency Uses	No
Internal Flow or Collection	No
Alteration in Character of Data	No
16. Is the system a General Support System (GSS), Major Application (MA) or Minor	Minor Application

Application?:	
*17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?:	Yes, PII is transmitted but it is only used to reference other questions and it is only temporarily stored.
Note: This question seeks to identify any, and all, personal information associated with the system. This includes any PII, whether or not it is subject to the Privacy Act, whether the individuals are employees, the public, research subjects, or whether it is personal information about business partners, and whether provided voluntarily or collected by mandate. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation.	
Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.	
Categories:	Yes/No
Name	Yes
Date of Birth	No
Social Security Number (SSN)	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	No
Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Age, Gender, Race/Ethnicity, Zip Code

18. Please indicate the categories of individuals about whom PII is collected, maintained, disseminated and/or passed through. Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII. Please answer "Yes" or "No" to each of these choices (NA in other is not applicable).

Categories:	Yes/No
Employees	No
Public Citizen	Yes
Patients	No
Business partners/ contacts (Federal, state, local agencies)	No
Vendors/ Suppliers/ Contractors	No
Other	No

19. Are records on the system retrieved by one or more data elements?:

No

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	No
Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No

Other	No
20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?:	Yes
21. Is the system subject to the Privacy Act? (If response to Q.19 is Yes, response to Q.21 must be Yes and a SORN number is required for Q.4):	No
21 A. If yes, but a SORN has not been created, please provide an explanation:	

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?:	No
---	----

Please indicate "Yes" or "No" for each category below:	Yes/No
Name	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	No
Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No

Other	No																		
*23. If the system shares or discloses PII please specify with whom and for what purpose(s):	No																		
24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?:	No																		
25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?:	No																		
26. Are individuals notified how their PII is going to be used?:	No																		
If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation:																			
27. Is there a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate?:	No																		
If yes, please describe briefly the notification process. If no, please provide an explanation:																			
28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?:	No																		
If yes, please describe briefly the review process. If no, please provide an explanation:																			
29. Are there rules of conduct in place for access to PII on the system?:	Yes																		
Please indicate "Yes," "No," or "N/A" for each category. If yes, briefly state the purpose for each user to have access:																			
<table border="1"> <thead> <tr> <th>Users with access to PII</th> <th>Yes/No/N/A</th> <th>Purpose</th> </tr> </thead> <tbody> <tr> <td>User</td> <td>No</td> <td></td> </tr> <tr> <td>Administrators</td> <td>No</td> <td></td> </tr> <tr> <td>Developers</td> <td>No</td> <td></td> </tr> <tr> <td>Contractors</td> <td>No</td> <td></td> </tr> <tr> <td>Other</td> <td>No</td> <td></td> </tr> </tbody> </table>		Users with access to PII	Yes/No/N/A	Purpose	User	No		Administrators	No		Developers	No		Contractors	No		Other	No	
Users with access to PII	Yes/No/N/A	Purpose																	
User	No																		
Administrators	No																		
Developers	No																		
Contractors	No																		
Other	No																		
*30. Please describe in detail: (1) the information the agency will collect, maintain, or disseminate; (2) why and for what purpose the agency will use the information; (3) in this description, explicitly indicate whether the information contains PII; and (4) whether submission of personal information is voluntary or mandatory:	Individuals are asked to submit a consent form prior to PII collection. PII submission is voluntary and is only used as a means to reference other survey questions. PII is only temporarily stored.																		
*31. Please describe in detail any processes in	PII is not retained in the system, therefore, there is no need to																		

place to: (1) 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 the original collection); (2) notify and obtain consent from individuals regarding what PII is being collected from them; and (3) how the information will be used or shared. (Note: Please describe in what format individuals will be given notice of consent [e.g., written notice, electronic notice, etc.])

notify and obtain consent.

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

***32. Does the system host a website?:** Yes

Please indicate "Yes" or "No" for each type of site below:	Yes/ No
Internet	Yes
Intranet	No
Both	No

33. Is the website accessible by the public or other entities (i.e., Federal, state, and/or local agencies, contractors, third party administrators, etc.)?: Yes

34. Is a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) posted on the website?: Yes

35. Is the website's privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?: Yes

If no, please indicate when the website will be P3P compliant:

36. Does the website employ tracking technologies?: No

Please indicate "Yes", "No", or "N/A" for each type of cookies below:	Yes/No/N/A
Web Bugs	No
Web Beacons	No
Session Cookies	Yes
Persistent Cookies	No
Other	No

***37. Does the website have any information or pages directed at children under the age of thirteen?:** No

If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any information is collected?:

38. Does the website collect PII from individuals?:

Please indicate "Yes" or "No" for each category below:	Yes/No
Name	Yes
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Mailing Address	No
Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Age, Gender, Race/Ethnicity, Zip Code

39. Are rules of conduct in place for access to PII on the website?:

40. Does the website contain links to sites external to the OPDIV that owns and/or operates the system?:

If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by the OPDIV.:

ADMINISTRATIVE CONTROLS

1	Administrative Controls
<p>Note: This PIA uses the terms “Administrative,” “Technical” and “Physical” to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.</p>	

2	
41. Has the system been certified and accredited (C&A)?:	No
41a. If yes, please indicate when the C&A was completed (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):	
41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?:	
42. Is there a system security plan for this system?:	Yes
43. Is there a contingency (or backup) plan for the system?:	Yes
44. Are files backed up regularly?:	Yes
45. Are backup files stored offsite?:	Yes
46. Are there user manuals for the system?:	Yes
47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?:	Yes
48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?:	Yes
49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?:	
If yes, please specify method(s):.	
*50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):	Yes
If yes, please provide some detail about these policies/practices:.	

TECHNICAL CONTROLS	
---------------------------	--

1	Technical Controls				
51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?:	Yes				
<table border="1" style="width: 100%;"> <tr> <td style="background-color: #e0e0e0;">Please indicate “Yes” or “No” for each category below:</td> <td style="background-color: #e0e0e0;">Yes/No</td> </tr> <tr> <td>User Identification</td> <td>Yes</td> </tr> </table>		Please indicate “Yes” or “No” for each category below:	Yes/No	User Identification	Yes
Please indicate “Yes” or “No” for each category below:	Yes/No				
User Identification	Yes				

Passwords	Yes
Firewall	No
Virtual Private Network (VPN)	No
Encryption	No
Intrusion Detection System (IDS)	No
Common Access Cards (CAC)	No
Smart Cards	No
Biometrics	No
Public Key Infrastructure (PKI)	No
52. Is there a process in place to monitor and respond to privacy and/or security incidents?:	Yes
If yes, please briefly describe the process:	NIH Incident Response Team forwards suspected incidents to the NHGRI Information Systems Security Officer for investigation and resolution.

PHYSICAL ACCESS

1	Physical Access
53. Are physical access controls in place?:	Yes
Please indicate "Yes" or "No" for each category below:	Yes/No
Guards	No
Identification Badges	No
Key Cards	Yes
Cipher Locks	No
Biometrics	No
Closed Circuit TV (CCTV)	Yes
*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls.:	Database secured behind locked doors, login/password/id protected with very limited 'need-to-know' users.

APPROVAL/DEMOTION

1	System Information
System Name:	
2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	
Comments:	

Approval/Demotion Point of Contact:	
Date:	

3	Senior Official for Privacy Approval/Promotion or Demotion
Promotion/Demotion:	
Comments:	

4	OPDIV Senior Official for Privacy or Designee Approval
Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it	
This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):	
Name: _____	Date: _____
Name:	
Date:	

5	Department Approval to Publish to the Web
Approved for web publishing	
Date Published:	
Publicly posted PIA URL or no PIA URL explanation:	

% COMPLETE

1 PIA Completion	
PIA Percentage Complete:	
PIA Missing Fields:	