PIA SUMMARY

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 the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no 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?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 31, 2012

**2. OPDIV Name:*

NIH

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200; 09-25-0156

**5. OMB Information Collection Approval Number:*

No

**6. Other Identifying Number(s):*

No

**7. System Name (Align with system item name):*

National Database for Autism Research

**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	Matthew McAuliffe, Ph.D.

**10. Provide an overview of the system:*

NDAR, the National Database for Autism Research, is a collaborative biomedical informatics system being created by the National Institutes of Health to provide a national resource to support and accelerate research in autism. *

NDAR will make it easier and faster for researchers to gather, evaluate, and share autism research data from a variety of sources. By giving researchers access to more data than they can collect on their own and making their own data collection more efficient, the time to discovery can be reduced.

**13. Indicate if the system is new or an existing one being modified:*

Existing

**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?*

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that

collect PII "permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)
Yes
17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.
**19. Are records on the system retrieved by 1 or more PII data elements?*
Yes
**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*
Yes
**23. If the system shares or discloses PII, please specify with whom and for what purpose(s):*
IIF information is not shared on research participants. However the PI's granted access to data will give permission to post their name on the NDAR Web site with the research aims. The purpose of this is facilitate transparency in how NDAR data is being used. PIs who submit information to NDAR will not have their information posted on the Web site.
**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*
The system will collect a wide variety of clinical information including images of the brain, genetics information, and data from diagnostic criteria specific to clinicians in the autism field. Recent changes to NDAR make sure that all IIF on research subjects (used to generate encrypted hashes that allow cross checking studies for the same individuals) is kept at the researcher's institution. NIH will collect IIF on PIs who submit information about research participants to NDAR. This information will be used by NIH to document, track, monitor and evaluate NIH clinical, basic, and population-based research activities. NIH will also collect IIF on PIs who wish to gain access to the information. This information will be used to document, track, monitor, and evaluate the use of NDAR datasets and to notify recipients of updates, corrections or other changes to NDAR.
**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.]):*
As part of the research protocol, all subjects will be required to fill out consents that describe how their information will be used even though NDAR will contain no IIF on research participants. If these change or expire, all participants will be contacted. PIs submitting information to NDAR and accessing information from NDAR will sign relevant agreements for submission and access, both of which include a Privacy Act notification.
**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*
Yes
**37. Does the website have any information or pages directed at children under the age of thirteen?*
No
**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
**54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:*
1) Management policies require that all new users be part of an approved site, with the request coming through a system administrator. 2) Technical Controls require that each user log in to the NDAR application with a unique user name and password. Additionally, the password is set to expire after 75 days, must be at least 8 characters long, with at least 2 of the following character types: Control Character, Number, Capital Letter. 3) Physical Controls require badged access to all server rooms, with badge lockdown policies in line with existing NIH procedures. Physical rack will be key-locked. Physical rack will be located in data center behind both biometric and keycard access with 100% identification badge check by 24/7 security guard. The Data Center is behind 3 independent 24/7 security guards that will perform identification badge checks.

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?*

No

If this is an existing PIA, please provide a reason for revision:

PIA Validation

**1. Date of this Submission:*

Aug 31, 2012

**2. OPDIV Name:*

NIH

3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):

009-25-01-05-02-3110-00

**4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):*

09-25-0200; 09-25-0156

**5. OMB Information Collection Approval Number:*

No

5a. OMB Collection Approval Number Expiration Date:

**6. Other Identifying Number(s):*

No

**7. System Name: (Align with system item name)*

National Database for Autism Research

8. System Location: (OPDIV or contractor office building, room, city, and state)

System Location:	
OPDIV or contractor office building	NIH campus, building 12B
Room	12B/2200
City	Bethesda
State	MD

**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	Matthew McAuliffe, Ph.D.

The following information will not be made publicly available:

POC Title	Staff Scientist - Project Manager
POC Organization	CIT/DCB
POC Phone	301.594.2432
POC Email	Matthew.McAuliffe@nih.gov

**10. Provide an overview of the system: (Note: The System Inventory form can provide additional information for child dependencies if the system is a GSS)*

NDAR, the National Database for Autism Research, is a collaborative biomedical informatics system being created by the National Institutes of Health to provide a national resource to support and accelerate research in autism. *

NDAR will make it easier and faster for researchers to gather, evaluate, and share autism research data from a variety of sources. By giving researchers access to more data than they can collect on their own and making their own data collection more efficient, the time to discovery can be reduced.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1 System Characterization and Data Configuration

11. Does HHS own the system?

Yes

11a. If no, identify the system owner:

Name: Matthew McAuliffe
Component: HHS/NIH/CIT/DCB
Address: 12 South Dr, Building 12A, Rm 2041
Bethesda MD 20817
Phone: 301-594-2432
Email: Matthew.McAuliffe@nih.gov
FAX:

12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No)

Yes

12a. If no, identify the system operator:

**13. Indicate if the system is new or an existing one being modified:*

Existing

14. Identify the life-cycle phase of this system:

Operations/Maintenance

15. Have any of the following major changes occurred to the system since the PIA was last submitted?

Yes

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	Yes

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?

General Support System

**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

TIP: If the answer to Question 17 is “No” (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that “Employee systems,” – i.e., systems that collect PII “permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)

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 (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
Social Security Number (SSN)	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
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
Personal Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Name and address of Institutional Business Official and PI collaborators (but not displayed); information regarding patient's parents but not IIF

17a. Is this a GSS PIA included for C&A purposes only, with no ownership of underlying application data? If the response to Q.17a is Yes, the response to Q.17 should be No and only the PIA Summary must be completed.

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	No

Patients	No
Business partners/contacts (Federal, state, local agencies)	Yes
Vendors/Suppliers/Contractors	No
Other	Yes - Institutional Business Officials

**19. Are records on the system retrieved by 1 or more PII data elements?*

Yes

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 (for purposes other than contacting federal employees)	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
Personal Mailing Address	No
Personal 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
Personal 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 the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*
Yes
21a. 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?

Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	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
Personal Mailing Address	Yes
Personal 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
Personal 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):*

IIF information is not shared on research participants. However the PI’s granted access to data will give permission to post their name on the NDAR Web site with the research aims. The purpose of this is facilitate transparency in how NDAR data is being used. PIs who submit information to NDAR will not have their information posted on the Web site.

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?

Yes

26a. If yes, please describe the process for allowing individuals to have a choice. If no, please provide an explanation.

Research study specific consent forms even though research subject information is not included in NDAR as IIF. PIs will have a choice on whether to agree to the terms and conditions for access and submission.

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

27a. 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

28a. 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:

Users with access to PII	Yes/No/N/A	Purpose
User	No	
Administrators	Yes	Adding new patients for studies and insuring no duplicate entries
Developers	Yes	testing and development
Contractors	Yes	testing and development
Other	No	

**30. Please describe in detail: (1) The information the agency will collect, maintain, or disseminate (clearly state if the information contained in the system ONLY represents federal contact data); (2) Why and for what purpose the agency will use the information; (3) Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory:*

The system will collect a wide variety of clinical information including images of the brain, genetics information, and data from diagnostic criteria specific to clinicians in the autism field. Recent changes to NDAR make sure that all IIF on research subjects (used to generate encrypted hashes that allow cross checking studies for the same individuals) is kept at the researcher's institution.
NIH will collect IIF on PIs who submit information about research participants to NDAR. This information will be used by NIH to document, track, monitor and evaluate NIH clinical, basic, and population-based research activities.

NIH will also collect IIF on PIs who wish to gain access to the information. This information will be used to document, track, monitor, and evaluate the use of NDAR datasets and to notify recipients of updates, corrections or other changes to NDAR.

**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.])*

As part of the research protocol, all subjects will be required to fill out consents that describe how their information will be used even though NDAR will contain no IIF on research participants. If these change or expire, all participants will be contacted.
PIs submitting information to NDAR and accessing information from NDAR will sign relevant agreements for submission

and access, both of which include a Privacy Act notification.

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

**32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of PII)*

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	Yes/ No	If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.
Internet	Yes	http://ndar.nih.gov/...publicweb/
Intranet	No	
Both	No	

33. Does the system host a website that is accessible by the public and does not meet the exceptions listed in OMB M-03-22?

Note: OMB M-03-22 Attachment A, Section III, Subsection C requires agencies to post a privacy policy for websites that are accessible to the public, but provides three exceptions: (1) Websites containing information other than "government information" as defined in OMB Circular A-130; (2) Agency intranet websites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees); and (3) National security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act.).

Yes

34. If the website does not meet one or more of the exceptions described in Q. 33 (i.e., response to Q. 33 is "Yes"), a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?

Yes

35. If a website privacy policy is required (i.e., response to Q. 34 is "Yes"), is the privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?

Yes

35a. If no, please indicate when the website will be P3P compliant:

36. Does the website employ tracking technologies?

Yes

Please indicate "Yes", "No", or "N/A" for each type of cookie 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

37a. 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?

No

Please indicate “Yes” or “No” for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	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
Personal Mailing Address	No
Personal 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
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	No

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

No

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

No

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

ADMINISTRATIVE CONTROLS

1	Administrative Controls

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.

41. Has the system been certified and accredited (C&A)?

Yes

41a. If yes, please indicate when the C&A was completed:

Jul 16, 2010

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)?

Yes

49a. If yes, please specify method(s):

Sudo is used to limit privilege to service being administered by personnel.

**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

50a. If yes, please provide some detail about these policies/practices:

Details: Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1B "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 3000-G-3, which allows records to be kept as long as they are useful in scientific research. Collaborative Perinatal Project records are retained in accordance with item 3000-G-4, which does not allow records to be destroyed. Refer to the NIH Manual Chapter for specific conditions on disposal or retention instructions.

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

Please indicate “Yes” or “No” for each category below:	Yes/No
User Identification	Yes
Passwords	Yes
Firewall	Yes
Virtual Private Network (VPN)	Yes
Encryption	Yes
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

52a. If yes, please briefly describe the process:

standard CIT security and PII policy and procedures.

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	Yes
Identification Badges	Yes
Key Cards	Yes
Cipher Locks	No
Biometrics	Yes
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:*

1) Management policies require that all new users be part of an approved site, with the request coming through a system administrator.
2) Technical Controls require that each user log in to the NDAR application with a unique user name and password. Additionally, the password is set to expire after 75 days, must be at least 8 characters long, with at least 2 of the following character types: Control Character, Number, Capital Letter.
3) Physical Controls require badged access to all server rooms, with badge lockdown policies in line with existing NIH procedures.

Physical rack will be key-locked.

Physical rack will be located in data center behind both biometric and keycard access with 100% identification badge check by 24/7 security guard. The Data Center is behind 3 independent 24/7 security guards that will perform identification badge checks.

APPROVAL/DEMOTION

1	System Information
System Name:	National Database for Autism Research

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	Added Ph.D. to Matthew McCauliffe's name as POC (in 2011 update)
Approval/Demotion Point of Contact:	Michele France, NIH/CIT/PECO
Date:	Aug 31, 2012

3	Senior Official for Privacy Approval/Promotion or Demotion
Promotion/Demotion:	Promote
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:	Karen Plá
Date:	Sep 28, 2012

5	Department Approval to Publish to the Web
Approved for web publishing	Yes
Date Published:	Sep 1, 2009
Publicly posted PIA URL or no PIA URL explanation:	http://www.hhs.gov/pia/nih.html

PIA % COMPLETE

1	PIA Completion	
PIA Percentage Complete:	100.00
PIA Missing Fields:	