Department of Health and Human Services
National Institutes of Health
OD/OM/Office of Management Assessment

NIH Privacy Impact Assessment (PIA) Guide

September 1, 2011

Change History

Version	Date of Issue	Author(s)	Description of Change(s)
[1.00]	[10/24/2007]		First version
[2.00]	[06/07/2010]		Second version
[3.00]	[08/04/2010]		Third Version
[4.00]	[08/31/2011]		Fourth Version

Table of Contents

1 Introduction 3

2 What is a PIA? 4

3 Complying with the PIA Requirement 4

4 Privacy Act Requirements 4

5 When to Conduct a PIA 6

6 How to Complete a PIA 7

6.1 PIA Roles and Responsibilities 7
6.2 Creating the PIA Form in SPORT 7
6.3 Tips for Completing the PIA Form 8
6.4 Reviewing and Promoting the PIA 9
6.5 Exporting and Downloading the PIA 10
6.6 Things to Consider 11
7 The Summary IT System PIA Questions 11

8 The Complete IT System PIA Questions 17

9 The TPWA PIA Questions 28

10 Conclusion 38

11 Appendix A: NEAR/NCAT/HEAR/SPORT Access Form 40

12 Appendix B: IT System PIA Form Template 41

13 Appendix C: TPWA PIA Form Template 58

14 Appendix D: HHS, NIH, and Government-wide SORNs 64

15 Appendix E: Sample IT System PIA (with PII) 66

16 Appendix F: Sample IT System PIA (without PII) 84

17 Appendix G: Sample TPWA 102

18 Appendix H: References 107

19 Appendix I: Acronyms 111

1 Introduction

Title II of the *E-Government Act of 2002 (E-Government Act)* requires federal agencies to conduct privacy impact assessments (PIAs) before developing or procuring information technology (IT) systems that collect, maintain, or disseminate personally identifiable information (PII). Additional requirements include making PIAs publicly accessible and posting a machine-readable privacy notice on publicly facing websites. Title III of the *E-Government Act*, known as the *Federal Information Security Management Act* (FISMA), superseded and made permanent the provisions of the *Government Information Security Reform Act of 2000* (GISRA). FISMA also amends the *Paperwork Reduction Act (PRA) of 1995* by adding a new subchapter on information security that requires certain program management, evaluation, and reporting activities, such as performing annual self-assessments and conducting an independent assessment by each agency's Inspector General (IG).

On January 21, 2009, the Director of the Office of Management and Budget (OMB) released a memorandum entitled the *Open Government Directive* that requires specific actions to implement the principles of transparency, participation, and collaboration amongst executive departments and federal agencies. Transparency is defined as providing the public with information about what the government is doing by making information available online in an open medium or format that can be retrieved, downloaded, indexed, and searched by commonly used web search applications. Participation is defined as contribution by the public of ideas and expertise so the federal government can make policies with the benefit of information that is widely dispersed in society (e.g., Websites such as Facebook or blogs). Collaboration is defined as the encouragement of partnerships and cooperation within the federal government, across levels of government and between the government and private institutions to fulfill the agency's core mission activities. Following the issuance of the *Open Government Directive*, OMB released Memorandum (M)-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications,*" in June of 2010 which expanded the scope of PIA requirements to include assessing Third-Party Websites and Applications (TPWAs) and the unique practices these technologies have for collecting PII, communicating with the public, and disseminating information. The Department of Health and Human Services (referred to as HHS or "the Department") adapted the IT System PIA form to assess TPWAs in accordance with OMB M-03-22, "*Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*".

In response to these requirements the National Institutes of Health (NIH) updated Manual Chapter (MC) 1745-1, "Privacy Impact Assessments," in June of 2011. This MC reinforces HHS' requirement for the completion of PIAs for both IT Systems and TPWAs, and details NIH employee roles and responsibilities in support of this process. For more information regarding NIH's PIA policy, please review NIH MC 1745-1, available at http://www3.od.nih.gov/oma/manualchapters/management/1745-1/.[1]

[1] The NIH PIA Policy, MC 1745-1, is currently being updated and a new version will be published in July/August of 2011.

2 What is a PIA?

The PIA is an analysis tool designed to identify any privacy risks associated with information that is collected, processed, stored, and/or transmitted by an IT System or TPWA to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy. The PIA is used to determine the risks and effects of collecting, maintaining and disseminating PII in an electronic IT System used by multiple users (e.g., network, server, and database) or through the use of a TPWA. In addition, a PIA examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks.

A PIA must be conducted on all IT Systems and uses of TPWAs, even if PII is not being collected, processed, stored, and/or transmitted. According to federal requirements and OMB guidance, HHS is responsible for providing proper protections for PII collected or contained within IT Systems and TPWAs. A detailed breakdown of the legislation regarding PIAs can be found in the HHS Information Assurance Privacy Impact Assessment (PIA) Guide at: http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/PIA/pia_sop.pdf.

3 Complying with the PIA Requirement

Completing a PIA will assist NIH with incorporating privacy protections into each stage of an IT System or TPWA life cycle.

Per NIH MC 1745-1, PIAs are completed by IT System and TPWA Owners/Managers (referred to hereafter as System Owner(s)/Manager(s)) in consultation with the NIH Institute or Center (IC) Privacy Coordinator, and Information Systems Security Officer (ISSO) via the HHS Security and Privacy Online Reporting Tool (SPORT). PIAs must be promoted to the NIH Senior Official for Privacy (SOP) for quality review to ensure completion and accuracy. The SOP will submit the finalized PIA to the HHS Senior Agency Official for Privacy (SAOP). The HHS SAOP will in turn complete an independent review of the PIA prior to public posting on the HHS website at: http://www.hhs.gov/pia/nih/index.html.

To assess whether IT Systems or TPWAs are compliant with federal and Departmental requirements, System Owners/Managers, Institutes and Centers (IC) Privacy Coordinators, and other designated PIA Authors and PIA Reviewers should use the PIA methodology detailed in this guide. The Department and NIH will assess compliance through its automated PIA form that is hosted in SPORT. HHS requires that a PIA be completed for all IT Systems and all uses of TPWAs regardless of whether or not these systems contain PII. IT Systems or TPWAs in development, and those that only contain PII on federal employees, must also meet this requirement. Please note that the full IT System PIA is not required for systems that only contain PII on federal employees. For those IT Systems, the requirement is limited to completing the PIA Summary and the Website Hosting Practices Tab in SPORT. However, the adapted PIA form must be completed for all uses of TPWAs.

4 Privacy Act Requirements

The Privacy Act of 1974, as amended, defines a Privacy Act record as "any item, collection, or group of information ***about an individual*** that is maintained by an agency, including, but not limited to, ***education, financial transactions, medical history, and criminal or employment***

history and that contains ***name, or the identifying number, symbol, or other identifying particular*** assigned to the individual, ***such as a finger or voice print or a photograph*** (5 U.S.C. § 552a(a)(4)).” Other examples of personal information or personal identifiers include, but are not limited to: age, date of birth, Social Security Number (SSN), sex, gender, medical credentials, military rank, home address/phone/e-mail address, and patient identification or protocol study number.

A System of Records Notice (SORN) refers to the notice which describes the purpose of the information collection, the legal authority to collect information, the categories of information collected, maintained, retrieved, and used within a set of records, the categories of individuals for whom the information is collected, to whom the information can be disclosed, etc. A SORN Number is the number assigned to the Privacy Act SORN (also referred to as the Systems Notice) for reference in the Federal Register. The SORNs are written broadly to cover information collections subject to the Privacy Act. If a collection of records that includes Privacy Act information is proposed for operation and is NOT covered under an existing SORN, a new SORN must be developed and posted in the Federal Register 40 days prior to collection of data. If no existing SORN covers the proposed data collection, the System Owner/Manager must work with the IC Privacy Coordinator to put one in place. Otherwise, the system of records is unauthorized and must not be operated under penalty of law.

Generally, the Privacy Act SORN requirement applies when:

- A group of records (more than one)[2] is present in paper or electronic form;
- The records contain information about an individual; and,
- The information is designed to be retrieved by a name or other personal identifier.

Determining Privacy Act applicability requires the exercise of judgment in many cases. System Owners/Managers are encouraged to contact their IC Privacy Coordinator in case of any uncertainty to ensure that they are properly advised on the extent to which they must consider privacy in their collections of data.

There are three types of SORNs that can be cited to cover record systems: Internal, Government, and Central. Internal notices are owned by individual federal agencies to cover their internal records (e.g., HHS, NIH and other Operating Divisions (OPDIVs)). They can also appear as “umbrella” SORNs that cover a multitude of internal system records. Internal NIH SORNs begin with 09-25-xxxx, while Departmental SORNs typically begin with 09-90-xxxx. Government SORNs may be used by all federal agencies to cover government-wide record systems (e.g., OPM, OGE, EEOC, FEMA, GSA, etc.) even if the physical records contained within the record system belong to the respective federal agency. The Office of Personnel Management (OPM) retains some authority over records covered under Government SORNs (e.g. during an appeal process). Government SORNs begin with GOVT-1, 2, etc. Central SORNs cover systems of records that are owned by OPM, who maintains full responsibility for the central record systems (e.g., Personnel Investigations Records). However, copies of these

[2] If you only have a single document, or your file contains publicly available information, it is not considered to be a group of records. In addition, Privacy Act systems of records only cover government records, or contracts to manage government records.

records may be maintained by individual federal agencies. Central notices begin with CENTRAL-1, 2, etc.

All internal NIH SORNs, as well as HHS SORNs commonly referenced at NIH, can be found through the NIH Office of the Senior Official for Privacy (OSOP) website, or by visiting http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm.

5 When to Conduct a PIA

The HHS Information Security Program Policy, dated December 15, 2004, requires NIH to:

- Conduct PIAs on all Departmental IT Systems as instructed by OMB Memorandum (M)-03-22 that includes, but is not limited to, the collection of new PII or when the Department develops, acquires, and/or buys new IT Systems to handle collections of PII. PIAs must all be reviewed and updated when a major change occurs to a system (further reinforced by the "HHS Information Security Program Privacy Policy Memorandum", dated November 20, 2006). According to OMB M-03-22, a major change is defined as a modification to an IT System that affects the access controls, type of data collected, IT System interconnection, information sharing, or alternation of business processes.[3] This requirement extends to the development and maintenance of TPWAs.
- Maintain soft copies of all PIAs and submit electronically both parts of the IT System PIA (Analysis Worksheets and PIA Summary) to the SAOP. This policy was implemented as required by Section 208(b) of the E-Government Act of 2002 (Public Law 107-347, U.S.C. Title 44, Chapter 36) and is consistent with the intent of OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

In addition, the Department released a memorandum entitled *Implementation of OMB M-10-22 and M-10-23*, which requires OPDIVs to complete a PIA for each use of a TPWA. The HHS SAOP has revised the Department's PIA methodology and standard operating procedures to accommodate TPWAs in the first quarter of Fiscal Year (FY) 2011 and will review annually thereafter. To first determine if a Website or web application is a TPWA, the Department released the following questionnaire for NIH to follow:

1. Is the Website or application part of authorized law enforcement, national security, or intelligence activities?

[3] OMB M-03-22 provides the following general examples of a major change:
Conversions: When converting paper-based records to electronic IT Systems or TPWAs.
Anonymous to Non-Anonymous: When functions applied to existing information collection change anonymous information into PII.
Significant IT System or TPWA Management Changes: When new uses, including application of new technologies, significantly change how PII is managed in the IT System or TPWA.
Significant Merging: When agencies adopt or alter business processes so that government databases holding PII are merged, centralized, matched with other databases, or otherwise significantly manipulated.
New Public Access: When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic IT System or TPWA.
More information regarding the definition and examples of a major change can be found at: http://www.whitehouse.gov/omb/memoranda_m03-22.

If the answer is "Yes;" it is not a TPWA. If the answer is "No;" continue to Question 2.

2. Is the Website or application for internal activities that do not involve the public? Yes or No.
If the answer is "Yes;" it is not a TPWA. If the answer is "No;" continue to Question 3.

3. Does HHS/NIH/IC own, operate, or control the Website or application? Yes or No.
If the answer is "Yes;" it is not a TPWA. If the answer is "No;" continue to Question 4.

4. Does another federal department or agency own, operate, or control the Website or application? Yes or No.
If the answer is "Yes;" it is not a TPWA. If the answer is "No;" continue to Question 5.

5. Is the Website or application owned, controlled, or operated by a nongovernment entity or a contractor acting on behalf of HHS? Yes or No.
If the answer is "Yes;" continue to Question 6. If the answer is "No;" it is not a TPWA.

6. Is the Website or application used by the IC to engage with the public for the purposes of implementing the principles of the Open Government Directive? Yes or No.
If the answer is "Yes;" the Website or application is a TPWA. If the answer is "No;" it is not a TPWA.

6 How to Complete a PIA

This guide outlines a standard approach for conducting a PIA for all NIH IT Systems and TPWAs, including developmental, operational, FISMA, contractor-owned, or grantee, and including IT general support systems (GSS), major applications (MA), and non-major applications. All NIH IT Systems or TPWAs should have a current PIA to ensure compliance with the *E-Government Act of 2002*, OMB guidance, HHS policy and guidance, and NIH policy.

6.1 PIA Roles and Responsibilities

PIAs are completed by a System Owner/Manager, who will serve as the PIA Author. The PIA Author should work in consultation with the IC Privacy Coordinator, ISSO, Web Master, PRA Liaison, Records Liaison and other key stakeholders, as applicable. Any of these stakeholders may also serve as the PIA Reviewer. In addition, the role of the PIA Promoter may have responsibilities for coordinating all PIAs throughout the IC and the point of contact for submission to the NIH OSOP. Other roles in the NIH PIA process are outlined in the NIH PIA Policy, NIH MC 1745-1, available at: http://oma.od.nih.gov/manualchapters/management/1745-1/.

6.2 Creating the PIA Form in SPORT

Users must be granted access to SPORT in order to complete the PIA. This is accomplished by completing page two of the NIH Certification and Accreditation Tool (NCAT)/Security and Privacy Online Reporting Tool (SPORT) New System Request Form, found at: https://sps.nihcio.nih.gov/OCIO/NIH/NCAT/Shared%20Documents/NCAT-NEAR-HEAR-

SPORT_New_System_Creation_Form.pdf[4].
In order to request access, the following information must be provided for each user:

- Name;
- Active Directory User ID;
- Desired role (e.g., PIA Reviewer – user with read only access to the PIA information);
- PIA Promoter – user who will promote the system to the NIH Senior Official for Privacy; PIA Owner (Author) – user with the ability to edit the PIA information, and
- Any other necessary additional information.

Once the form has been completed the request may be submitted by using the 'Submit via Email' button found on the form, or by sending the form to NIH FISMA Support at: NIHSport@mail.nih.gov.

To create a new PIA in SPORT, the PIA Author should notify NIH FISMA Support of the intent to complete a PIA. The request must include the NIH IC name, the name of the IT System or TPWA, and the name the OPDIV that will track the PIA (e.g. NIH National Cancer Institute (NCI)/Facebook/Cancer.gov). Once the request is submitted, the NIH FISMA Program Support will create a new PIA form in SPORT for use by the IC. The requested PIA form can be found in SPORT at https://sport.hhs.gov/prosight/.

6.3 Tips for Completing the PIA Form

The PIA Author may begin with either the PIA Summary tab for IT System PIAs, or the PIA Required Information tab for TPWA PIAs. IT System PIA Summary questions are taken directly from the full IT System PIA form, and, as such, will auto-populate the rest of the form if completed in the PIA Summary tab, and vice versa. To continue completion of the form, the PIA Author can then move through each tab to complete information. ***It is important to note that all questions found on the TPWA PIA form must be completed before the TPWA PIA can be reviewed and promoted to the NIH SOP.***

In general, suggested guidelines for completing the PIA form include:

Here are some suggested guidelines to follow when preparing a TPWA PIA:

- Write concisely and in a way that is easily understood by the general public; avoid technical jargon;
- Define each acronym the first time it is used; use the acronym alone in all subsequent references;
- Clearly define technical terms and references;

[4] The NIH Certification and Accreditation Tool (NCAT) is a NIH system used to track our system inventory from a Certification & Accreditation (C&A) boundary/FISMA perspective. It includes all IT systems that require a C&A or are minor systems covered within the C&A boundaries of a parent system. NCAT collects some basic privacy information for C&A purposes, including references to Privacy Act Systems of Record Notices (SORNs) and an upload of the Privacy Impact Assessment (PIA) form pulled from the HHS Security and Privacy Online Reporting Tool (SPORT) used to create and track PIAs.

- Conduct interviews or review documentation to ensure that the TPWA PIA accurately represents how the OPDIV is using the TPWA and any information exchanges;
- Include complete information for references to governmental publications and other documents (e.g., OMB M-03-22);
- Ensure that information in the PIA is consistent with information in OMB Exhibit 300 and OMB Exhibit 53. Coordinate with personnel who complete these forms to ensure consistency;
- Leverage existing documentation; items such as SORN or requirements documents can be useful sources of information. (However, do not substitute a SORN for a PIA, even though much of the information in a PIA may be in a SORN as well. The PIA is distinct in terms of the information required, the format in which the information should be presented, and when updates must be performed.); and,
- Remember that a PIA is a public document, so do not include sensitive/confidential information or information that could allow a potential threat source to gain unauthorized access into the OPDIV account (e.g., do not provide overly-detailed information on access controls).

The PIA Author should refer to the IC Privacy Coordinator for all privacy-related questions. For security-related questions, the PIA Author should consult the IC ISSO. The PIA Author should consult with the IC Records Liaison with all records retention-related questions. For website-related questions, the PIA Author should consult with the IC Webmaster. To determine if the system requires an OMB clearance number, the PIA Author should consult with the OMB Project Clearance Liaison.

To assist IT System and TPWA Owners/Managers in completing the PIA form:

- A list of IC Privacy Coordinators can be found at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3
- A list of IC ISSOs can be found at: http://ocio.nih.gov/nihsecurity/scroster.html
- A list of IC Records Liaisons can be found at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=2
- A list of OMB Project Clearance Liaisons can be found at: http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcllist.htm.

6.4 Reviewing and Promoting the PIA

Once the PIA form is completed, the PIA Reviewer or a designee must review the PIA for completeness and accuracy. The PIA Reviewer must then promote the PIA via the Approval/Demotion page, and send notification to the NIH SOP that the PIA is complete. Once the PIA is promoted to the NIH SOP, it will undergo a final review prior to either promotion to the Department or demotion to the PIA Reviewer with a comments matrix via email. If changes are made to an IT System or TPWA PIA independent of a requested review, PIA Authors must inform the PIA Reviewers, who, in turn, must review the updates and provide notification to the NIH SOP of the changes by sending an email to privacy@mail.nih.gov.

Before promoting the IT System or TPWA PIA:

- Answer all multiple choice questions;
- For all applicable ‘If yes…’ questions, indicate either a Yes or No response and answer completely;
- As you complete each tab, click ‘Submit’ to save work and prevent loss of data;
- Provide enough detailed information to answer each question thoroughly (e.g., list the specific data elements collected by an IT System or TPWA);
- Leverage existing documentation (e.g., SORN, C&A, OMB Request for Clearance, Records Retention Schedule);
- Do not substitute a SORN for a PIA, even though much of the information in a PIA may be included in the SORN as well;
- Prior to promoting the PIA, ensure that both the system point of contact (POC) and PIA Reviewer’s names and contact information are indicated; and,
- Review responses for spelling errors. This can be done through the spell check feature, next to the ‘Submit’ button. Remember, PIA Summaries will be posted publicly.

6.5 Exporting and Downloading the PIA

In order to export a copy of the PIA for records purposes, or to download the PIA to a local machine, there are two options:

Option 1 -

- Once logged in to SPORT, open the desired PIA.
- Click on the “Forms” tab.
- Click on “Form” on the far left of the dark gray toolbar.
- Hold down the “CTRL” button and select “Export.”
- A window will appear named “Export Setting Window.”
- Continue to hold down the “CTRL” button and click “OK” from the Export Setting Window to export the PIA.
- Once the PIA is exported, click on “File,” and then “Save As” to save the PIA as a Microsoft Word or XML document.

Option 2 -

- Once logged in to SPORT, open the desired PIA.
- Click on the “Scorecard” tab.
- Click on “Scorecard” on the far left of the dark gray toolbar.
- Hold down the “CTRL” button and select “Export.”
- A window will appear named “File Download Window.”
- From here there are two options. The PIA can either be exported or directly saved without opening or viewing the PIA.
- To export the PIA, continue to hold down the “CTRL” button and click “Open” from the File Download Window to export the PIA.
- Once the PIA is exported you can click on “File,” and then “Save As” to save the PIA as a Microsoft Word or XML document.

- To directly save the PIA, continue to hold down the "CTRL" button and click "Save" from the File Download Window.
- Name and save the file as needed.

6.6 Things to Consider

IC Privacy Coordinators should maintain a soft copy of the PIA in the event of a temporary SPORT outage, or if copies require internal distribution to System Owners/Managers without SPORT access. In addition, ICs must periodically review PIAs to ensure that they are in compliance with current system practices. Remember, a PIA is a living document that must be updated when a major change in the system occurs. Periodic reviews of the PIA will ensure that changes in a system's management, operational, or technical environment that may impact PII are captured as required by law and HHS and NIH policy. Since PIAs are validated by the Department annually, NIH requires that System Owners/Managers, IC Privacy Coordinators, and ISSOs review the PIAs annually to ensure accuracy of all information.

When an IT System or TPWA is no longer in use, the IC Privacy Coordinator should notify FISMA Tool Accounts at NIHSport@mail.nih.gov, as well as the NIH SOP at privacy@mail.nih.gov, in order to officially remove the system from SPORT. If the IT System or TPWA contains information requiring disposal according to the NIH Records Schedule, the System Owner/Manager, in consultation with the IC Privacy Coordinator, should contact the IC Records Liaison.

7 The Summary IT System PIA Questions

The following required questions represent the information necessary to complete ONLY the IT System PIA Summary. This information will be used to generate an IT System PIA Summary, which will be posted online to the HHS PIA Website. PIA Authors and PIA Reviewers may use the following as assistance when completing and reviewing the questions found on the IT System PIA Form Summary tab.

IT System PIA Summary Questions Tab

Question	Guidance
Is this a new PIA?	Using the pull-down menu, indicate whether the IT System is new or if it's an existing IT System for which you are now modifying the PIA.
If this is an existing PIA, please provide a reason for revision:	If this is an existing PIA, use the pull-down menu to select an appropriate reason for this revision.
***1. Date of this Submission:**	For all PIAs, the date of submission is the final date that the PIA is completed and ready for submission to the NIH SOP. If the PIA is demoted and information is changed, or the PIA is validated for reporting purposes, the date of submission should be adjusted to reflect the changes before being promoted again.
***2. OPDIV Name:**	Use the scroll down menu to select the IT System for which you are completing a PIA. When notified of the

	existence of an IT System, the OPDIV Name will be listed automatically by the Center for Information Technology (CIT) as HHS/NIH/Institute.
***4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):**	A SORN describes the Privacy Act system of records, and the categories of PII collected, maintained, retrieved, and used within the IT System. It provides information to the public on various characteristics of the IT System (e.g., description, purpose, data collection, notification, retention and disposal) and how NIH intends to manage and protect the IT System. The SORN Number is that which is assigned to the Privacy Act SORN (also referred to as the Systems Notice). If the IT System is subject to the Privacy Act, then a SORN must be cited (refer to Section IV of this guide for more information). Work with the IC Privacy Coordinator to determine which SORN appropriately covers the IT System. A list of IC Privacy Coordinators can be located at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3. NIH Privacy Act System Notices can be located by visiting the OSOP Privacy Website at: http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm.
***5. OMB Information Collection Approval Number:**	The Paperwork Reduction Act of 1995 requires agencies to obtain approval from OMB prior to soliciting and/or obtaining identical information from ten or more members of the public in multiple forms. OMB approval is required whether the federal agency collects the information itself or uses an outside agent or contractor. OMB requires 90-120 days to approve new information collections and renew existing approvals. The OMB Information Collection Approval Number should be identical to the one OMB assigned pursuant to having been filed under the Paperwork Reduction Act and is sometimes referred to as an OMB control number. It would only apply if the IT System maintains data as part of an approved OMB information collection from 10 or more members of the general public. You can click on the Office of Extramural Research (OER) Intranet website at: http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcllist.htm to obtain a list of NIH Information Collection Clearance Officers, and get more information about whether an IT System has been approved for OMB

	information collection.
***6. Other Identifying Number(s):**	The Other Identifying Number would only be listed if the IC chose to assign an internal tracking number to the IT System, such as IC-1, IC-2, IC-3, and so on.
***7. System Name (Align with system item name):**	The HHS Enterprise Architecture Repository (HEAR) has been implemented to serve as the authoritative source of the inventory of IT Systems. HEAR will ensure that when IT Systems are created, renamed, moved or deleted, their records will be available in SPORT and other tracking/reporting systems at HHS. A process has been implemented at NIH that will automatically synchronize the appropriate naming scheme for SPORT based on the IT System name in the NIH Enterprise Architecture Repository (NEAR). NEAR is the authoritative source for IT System names at NIH. Within NEAR, the IC Name is collected separately from the System Name. As required by SPORT, when the HHS Enterprise Architecture Repository (HEAR) sends the System Name field to SPORT, it will automatically add the “NIH IC” to the front of the name.
***9. System Point of Contact (POC):**	The System Point of Contact is the person to whom questions about the PIA, characterization of the IT System, and data categorization may be addressed. Only the name of the POC will be made publicly available. When choosing an IT System POC, list the System Owner/Manager or qualified individual who is most knowledgeable about the IT System and its functions.
***10. Provide an overview of the IT System:**	Please provide a brief, but detailed explanation of the IT System. The explanation should include its purpose, characteristics (i.e., what information the IT System collects), a legal justification if one exists, and any other important information about the IT System.
***13. Indicate if the system is new or an existing one being modified:**	Refer back to the initial question at the beginning of the PIA Summary for the proper response.
***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?**	This question seeks to identify any, and all, personal information associated with the IT System. This includes any PII, whether or not it is subject to the Privacy Act. This also includes NIH employees, the general public, research subjects, grantees, contractors or business partners and research collaborators whose information has been obtained voluntarily or by mandate and is contained within the IT System. Later questions will try to clarify the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If this IT System contains PII, all remaining questions on the

	PIA form tabs must be completed prior to signature and promotion.
***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.**	Please indicate either a Yes or No response. If this is a Major Application (MA), Minor Application (child) or Minor Application (stand-alone) the answer should be No. If the IT System is a GSS, only answer Yes if this is a GSS PIA included for C&A purposes only, with no ownership of underlying application data.
***19. Are records on the system retrieved by 1 or more PII data elements?**	*Note: 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.* If Yes, a Yes or No response for each category is required. In addition to providing insights into the functionality of an IT System, this question verifies the applicability of the Privacy Act. Therefore, if the IT System is subject to the Privacy Act (see Question 21), information must be retrieved by name or another personal identifier.
***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).**	If the IT System includes a group of records containing PII designed to be retrieved by a name or other identifier, the Privacy Act applies to the information collection. If the Privacy Act applies, the IT System requires the completion of the full PIA (all tabs must be completed) and a SORN must be cited in Question 4. In the case of records pertaining to government employees and their work information, OMB M-03-22 indicates that information in identifiable form (personally identifiable information) about government personnel generally is protected by the Privacy Act. In addition, OMB M-06-20 indicates that employee identifiable information should be scrutinized to the same extent as information regarding members of the public.
***23. If the system shares or discloses PII, please specify with whom and for what purpose(s):**	In addition to any routine disclosure practices for the IT System, an IT System which references an NIH umbrella SORN will have additional potential disclosure practices. Please reference the Routine Uses contained in the SORN indicating the potential disclosures of PII. Therefore, if the IT System is subject to the Privacy Act, the response to this question (and Question 21) should be yes, and a brief explanation of disclosure practices found in the SORN should be included in your response.
***30. Please describe in detail: (1) The information the agency will**	Regardless of whether or not the IT System collects PII, a full response is required that addresses all points of the

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.	question. This question also attempts to determine if a Privacy Act notification statement is required. If personal information is collected, you must address the following six points: • What is the Government's Authorization? (Public Law, Statute, Executive Order, etc.) • What information is collected? • What is the purpose of the information collection? • What are the routine uses for disclosure of the information to others? • *Can the information be provided on a voluntary basis, or is it mandatory? • *If mandatory, what effect, if any, will there be if the information is not provided? * If the IT System does not contain PII, these points do not need to be addressed. A legal authority is required for a Privacy Act system of records. The legal authority can be researched by the IC Privacy Coordinator. An example would be PHS Act Section 301, but check to see which statute or executive order was granted to the Agency, Institute, Clinical Research Program, etc. which authorizes the collection of PII. The IC legislative office is an excellent resource for this information.
***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]).**	*Note: Please describe in what format individuals will be given notice of consent (e.g., written notice, electronic notice). If the IT System does not contain PII, please state that in the response box. Do not leave the question unanswered.* This question contains multiple parts, all of which must be answered in the response. Since the PIA Summary will be posted on the HHS Internet, please ensure that all parts of the question are clearly addressed in your response.

***32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices section must be completed regardless of the presence of PII.)**	Please indicate a Yes or No response.
***37. Does the website have any information or pages directed at children under the age of thirteen?**	*Note: 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?* In accordance with the Children's Online Privacy Protection Act (COPPA), all agency websites directed at children under the age of 13 must ensure that proper privacy protections are in place, including parental consent. Refer to NIH Manual Chapter 2805, "NIH Web Page Privacy Policy," for more information on the protection of children at: http://www3.od.nih.gov/oma/manualchapters/management/2805/.
***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 the SORN):**	If the IT System contains PII, and has the appropriate policies or guidelines in place, please indicate a Yes response. If the IT System does not have the proper policies or guidelines in place, or if it does not contain PII, then answer No to this question. Contact your IC Records Liaison for more information on which NIH Records Retention Schedule pertains to the information collection. A list of IC Records Liaisons can be accessed from OMA's webpage at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=2. In addition, if an IT System has a SORN in place it should contain language indicating retention and destruction methods.
***54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:**	Since only the PIA Summary will be posted on the HHS Internet, please ensure that all parts of the question are clearly answered in your response. If the IT System is covered by a SORN, contact your IC Privacy Coordinator or refer to the NIH Privacy Act SORN website at: http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm for more information and language regarding the safeguards for the IT System. If the IT System does not have the proper controls in place or it does not contain PII, then answer No to this question.

8 The Complete IT System PIA Questions

Once the above questions have been answered, the IT System PIA Summary section is complete. If the response for question 17 is Yes, indicating the IT System contains PII, the IT System will require a full PIA. The following section looks at each individual question and provides additional guidance on the necessary response.[5] PIA Authors and PIA Reviewers may use the following as assistance when completing and reviewing the questions found on the IT System PIA Form ONLY.

PIA Required Information Tab

Question	Guidance
Is this a new PIA?	Answered previously on the PIA Summary.
If this is an existing PIA, please provide a reason for revision:	Answered previously on the PIA Summary.
***1. Date of this Submission:**	Answered previously on the PIA Summary.
***2. OPDIV Name:**	Answered previously on the PIA Summary.
3. Unique Project Identifier (UPI) Number for current fiscal year (Data is auto-populated from the System Inventory form, UPI table):	The UPI number is used to report IT investments during the budget process and ensure the integration of strategic planning, budgeting, procurement, and the management of IT investments in support of the agency's mission and business needs. It reflects information such as the OPDIV and office where the investment project was initiated, the type of investment, and other information. The UPI number is used by OMB to track the system through the PIA, C&A, and Plan of Action and Milestones (POA&M) processes. The number is attached to Exhibit 53s and described in Exhibit 300s, which are submitted to OMB prior to major investment and budget requests. The number is long and appears as follows: 009-25-xx-xx-xx-xxxx-xx-xxx-xxx. If the IT System does not have a UPI number, check with the NIH Information Security Awareness Office (ISAO) within CIT at NIHSport@mail.nih.gov to confirm. If the IT System you are assessing has gone through a major change that has created new privacy risks, you may find the UPI number reported previously on an Exhibit 53 has been rolled up to a more inclusive Exhibit 300, in which case the IT System PIA would need to cite the new UPI. Otherwise, if the IT System has not undergone a major change, the UPI number would remain the same.

[5] Questions on the full form with an asterisk (*) were answered previously under the Summary tab and will be submitted to the Office of Management and Budget (OMB) and made publicly available in accordance with OMB Memorandum (M) 03-22 at: http://www.whitehouse.gov/omb/memoranda/m03-22.html. In addition, those fields already answered will auto-populate into the full IT System PIA Form.

***4. Privacy Act System of Records Notice (SORN) Number (If response to Q.21 is Yes, a SORN number is required for Q.4):**	Answered previously on the PIA Summary.
***5. OMB Information Collection Approval Number:**	Answered previously on the PIA Summary.
5a. OMB Collection Approval Number Expiration Date:	This question was not required in the PIA Summary. If not certain, check with the IC Information Collection Clearance Liaisons.
***6. Other Identifying Number(s):**	Answered previously on the PIA Summary.
***7. System Name (Align with system item name):**	Answered previously on the PIA Summary.
8. System Location (OPDIV or contractor office building, room, city, and state):	Indicate the NIH or Contractor office building, room, city and state where the IT System is physically located, or the server is hosted.
***9. System Point of Contact (POC):**	Answered previously on the PIA Summary.
***10. Provide an overview of the IT System:**	Answered previously on the PIA Summary.

System Characterization and Data Categorization Tab

Question	Guidance
11. Does HHS own the system?	If NIH owns the IT System or funds a contract to design, develop or implement the IT System, answer Yes.
11a. If no, identify the System Owner:	If NIH does NOT own the IT System or fund a contract to design, develop or implement the IT System, identify the name of the IT System Owner/Manager.
12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No):	If NIH operates the IT System, answer Yes. If a contractor operates or manages the IT System on behalf of NIH, answer No.
12a. If no, identify the system operator.	If NIH does NOT operate the IT System, identify the name of the system operator.
***13. Indicate if the system is new or an existing one being modified:**	Answered previously on the PIA Summary.
14. Identify the life-cycle phase of this system:	Indicate the appropriate phase from the drop-down menu.
15. Have any of the following major changes occurred to the system since the PIA was last submitted?	Indicate Yes or No in each of the boxes. If this is a new system, the responses will be No.

16. Is the system a General Support System (GSS), Major Application (MA), Minor Application (child) or Minor Application (stand-alone)?	Refer to OMB Circulars A-11 and A-130 for definitions. They are located at URLs: http://www.whitehouse.gov/omb/circulars/a11/current_year/a11_toc.htmlandhttp://www.whitehouse.gov/omb/circulars_a130_a130trans4/.With respect to NIH enterprise systems and systems considered to be "extensions" of enterprise systems, generally, the rule of thumb is: If it is an enterprise system owned and maintained by NIH (including directing how it is used and by whom, and ensuring security for the system) then the centralized office should prepare the PIA. If, however, the centralized office has no control over an "extension" system that is owned and operated by an IC, the IC system should have a PIA completed on it as well.
***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?**	Answered previously on the PIA Summary.
***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.**	Answered previously on the PIA Summary.
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).	*Note: NIH considers grantees and principal investigators to be business partners.* A Yes or No response for each category is required.
***19. Are records on the system retrieved by 1 or more PII data elements?**	*Note: If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.* A Yes or No response for each category is required. In addition to providing insights into the functionality of an IT System, this question verifies the applicability of the Privacy Act. Therefore, if the IT System is subject to the Privacy Act (see Question 21),

	information must be retrieved by name or another personal identifier.
20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?	Please indicate a Yes or No response.
***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).**	Answered previously on the PIA Summary. For more information on Privacy Act applicability, please see Section IV of this guide.
21a. If yes, but a SORN has not been created, please provide an explanation.	If the system is subject to the Privacy Act, the law requires that a SORN be published in the Federal Register. If a SORN has not been created, include a brief explanation indicating why this has not been done.

Information Sharing Practices Tab

Question	Guidance
22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency:	*Note: If Yes, please identify the category of PII shared or disclosed. If the category of personal information is not listed, please check Other and identify the category.*
***23. If the system shares or discloses PII, please specify with whom and for what purpose(s):**	Answered previously on the PIA Summary.
12. Does HHS operate the system? (If the system is operated at a contractor site, the answer should be No):	If NIH operates the IT System, answer Yes. If a contractor operates or manages the IT System on behalf of NIH, answer 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?	Please indicate a Yes or No response. No record contained within a system of records may be disclosed to an agency or non-federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency.
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)?	Change management, incident response, and continuity of operations procedures should all include communications plans or procedures that explicitly address how to inform users, organizations, and other stakeholders of changes to this IT System that affect their activities or operations. If the process for notifying data users is unwritten, the appropriate

	response is No.
26. Are individuals notified how their PII is going to be used?	Please indicate a Yes or No response.
26a. If yes, describe the process for allowing individuals to have a choice. If no, please provide an explanation.	If Yes, provide a brief but thorough description of how individuals are notified. For IT Systems that are subject to the Privacy Act, and collect information from members of the public, System Owners/Managers must post a Privacy Act notification statement at the point at which personal information is provided by an individual, or requested by NIH, such as on a manual or electronic form, or on a website. See Section IV for more information on Privacy Act applicability. A Privacy Act notification statement should address the following criteria: • What is the Government Authorization (Public Law, Statute, Executive Order, etc.) authorizing the information collection? • What information is collected? • What is the purpose of the information collection? • What are the routine uses for disclosure of the information to others? • Can the information be provided on a voluntary basis, or is it mandatory? • If mandatory, what effect, if any, will there be if the information is not provided?
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?	Please indicate a Yes or No response.
27a. If yes, briefly describe the notification process. If no, please provide an explanation.	If Yes, provide a brief description of the types of recourse given to members of the public whose personal information may appear in government IT Systems. In accordance with the Privacy Act, all IT Systems subject to the Privacy Act must have notification procedures contained within the SORN. The SORN indicates the procedures by which members of the public may contact System Owners/Managers to identify or make changes to the information about them that is contained within the IT System. System

	Owners/Managers should reference the SORN to review the language for the appropriate response, and ensure that the procedures specified are properly in place. For systems which contain PII but are not subject to the Privacy Act, it is considered a best practice to have proper complaint procedures in place for individuals whose information might be contained within the IT System, in order to ensure the data's integrity.
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?	Please indicate a Yes or No response.
28a. If yes, briefly describe the review process. If no, please provide an explanation.	If Yes, provide a brief but thorough description of the review process. If no, please provide a brief but through description of why there are no review processes in place. NIH ICs should have a system for periodic management review of the PII housed in our IT Systems. An internal system audit is an example of a process for reviewing the integrity and accuracy of NIH data.
29. Are there rules of conduct in place for access to PII on the system?	Please indicate a Yes or No response. If Yes, indicate Yes or No for all categories of users of the IT System and provide a description of the users' roles as they pertain to the IT System. *Note: All NIH IT Systems should have roles and responsibilities established for each user role associated with the system. Pursuant to FISMA, all major IT Systems, GSS, and other applications which contain sensitive data must have a C&A completed on them. As part of the C&A package, the System Security Plan (SSP) contains a description of user privileges. Consult the IC ISSO for more information.*
***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)**	Answered previously on the PIA Summary.

Explicitly indicate whether the information contains PII; and (4) Whether submission of personal information is voluntary or mandatory.	
***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]).**	Answered previously on the PIA Summary.

Website Hosting Practices Tab

Question	Guidance
***32. Does the system host a website? (Note: If the system hosts a website, the Website Hosting Practices must be completed regardless of the presence of PII.)**	This question includes additional fields not required in the PIA Summary. Please indicate a Yes or No for each field and an internet site URL if applicable.
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?	Please indicate a Yes or No response. If the IT System hosts a Website and does not meet the exceptions listed in OMB M-03-22, then indicate a Yes response. If the IT System does not host a Website or if it does host a Website and meets the exceptions/exclusions listed from OMB M-03-22, then indicate a No response. For a list of exceptions/exclusions see http://www.whitehouse.gov/omb/memoranda_m03-22/ section III part C.
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	NIH ICs and other components must post clear privacy policies on top-level/principal websites, including NIH and IC-level sites, major on-line public resource sites and any other known major public entry points, as well as any webpage that collects or posts personal information.

OMB M-03-22 and Title II and III of the E-Government Act) is required. Has a website privacy policy been posted?	Privacy policy links must be clearly labeled and easy to access by all visitors to a Website. If the privacy statement is combined with other mandated or recommended website statements or information, the link should be labeled accordingly, e.g., Privacy Act notification statement. For more information regarding the NIH Website Privacy Policy, refer to NIH Manual Chapter 2805, "Web Page Privacy Policy" at: http://www3.od.nih.gov/oma/manualchapters/management/2805/. You may also view the NIH Website Privacy Policy Statement at: http://www.nih.gov/about/privacy.htm.
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)?	Please indicate a Yes or No response.
35a. If no, please indicate when the website will be P3P compliant:	Per the E-Government Act of 2002, all agency Websites should have machine-readable privacy policies. NIH System Owners/Managers should consult with the IC Privacy Coordinators and the ISSOs to ensure that their Websites are P3P compliant. For more information about Machine-Readable Privacy Policy and P3P compliance, refer to the following link for a list of frequently asked questions: http://intranet.hhs.gov/it/docs/privacy/MRFAQ/MRPP_FAQ.html.
36. Does the website employ persistent tracking technologies?	Please indicate a Yes or No response. If Yes, indicate a Yes or No response for each category of persistent tracking technology. "Cookies" track computer use. "Session cookies" track the user's activities through a single website and are an approved use of cookies by HHS and NIH. "Persistent cookies" track the activities of users over time and across different websites. Federal policy states that federal agencies and their contractors may not use persistent cookies on federal websites unless numerous conditions are met. If a justification exists for a particular IT System, the IC must submit a written request to the NIH SOP, who, in turn, must request approval from HHS before the persistent tracking technology can be installed and used. Refer to NIH Manual Chapter 2805, "Web Page Privacy Policy," to learn more about the use and Departmental approval of persistent cookies at: http://www3.od.nih.gov/oma/manualchapters/management/2805/.

***37. Does the website have any information or pages directed at children under the age of thirteen?**	Answered previously on the PIA Summary.
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?	A unique privacy policy must be present for each Website that collects information about children that clearly describes the process for obtaining parental consent.
38. Does the website collect PII from individuals?	Please indicate a Yes or No response. If Yes, indicate a Yes or No response for each category listed. All categories with a Yes response to Question 38 should also be a Yes response to Question 17. Please double-check to make sure Question 17 accounts for the Yes responses provided in Question 38. As a reminder, in the event that a Website collects information from members of the public, a Privacy Act notification statement must be posted at the point at which personal information is provided by an individual, or requested by NIH. See Section IV of this guide, and Question 26 guidance for more information.
39. Are rules of conduct in place for access to PII on the website?	Please indicate a Yes or No response. The rules of conduct should also be contained within the C&A SSP.
40. Does the website contain links to sites external to HHS that owns and/or operates the system? Please indicate a Yes or No response.	Please indicate a Yes or No response.
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.	If Yes, provide a brief but thorough description of what the disclaimer states.

Administrative Controls Tab (Security Requirements)

Question	Guidance
41. Has the system been certified and accredited (C&A)?	Please indicate a Yes or No response.
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):	If yes, please enter the C&A completion date. Since HHS uses SPORT to report on security and privacy, the IT Systems for which C&A data has been populated previously will auto-populate into these fields. If there is no data entered, please complete the fields.

41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?	If the system requires a C&A and one has not been completed, please indicate when the C&A is scheduled for completion. Almost all Major-Applications require a C&A, as well as GSS and other applications that house information determined to be sensitive in nature. Contact your IC ISSO if you have questions about whether or not the system requires a C&A.
42. Is there a system security plan for this system?	Please indicate a Yes or No response. If a C&A has been completed on the IT System, check with your IC ISSO to verify that an SSP was completed with the C&A package.
43. Is there a contingency (or backup) plan for the system?	Please indicate a Yes or No response. This information should also appear in the IT System's C&A package.
44. Are files backed up regularly?	Please indicate a Yes or No response. This information should also appear in the IT System's C&A package.
45. Are backup files stored offsite?	Please indicate a Yes or No response. This information should also appear in the IT System's C&A package.
46. Are there user manuals for the system?	Please indicate a Yes or No response. This information should also appear in the IT System's C&A package.
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?	Please indicate a Yes or No response.
48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?	Please indicate a Yes or No response. Contracts to design, develop, and implement Websites and databases, for instance, must contain Federal Acquisition Regulation (FAR) clauses pertaining to the Privacy Act. Contact the IC Contracting Officer to ensure the applicable FAR clauses are cited in the contract, and that a SORN is attached to the contract for compliance by prime and sub-contractors working on behalf of the federal government.
49. Are methods in place to ensure least privilege (i.e., "need to know") and accountability?	Please indicate a Yes or No response.
49a. If yes, specify method(s).	If yes, provide a brief but thorough description.
***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 the SORN):**	Answered previously on the PIA Summary.
50.a If Yes, please provide some	This question includes additional fields not required in the

detail about these policies/practices:	PIA Summary. If yes, please provide a brief, but detailed description of retention and destruction practices for the PII contained in the IT System. For Privacy Act systems of records, records retention and disposal procedures should be indicated within the SORN cited for the system. If the IT System is not subject to the Privacy Act and does not have a SORN in place, consult with the IC Records Liaison to ascertain the appropriate records retention and disposal schedule for the IT System.

Technical Controls Tab

Question	Guidance
51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?	Please indicate a Yes or No response. If Yes, a Yes or No response for each category of technical controls listed is required. This information should also appear in the IT System's C&A package and could include controls such as user ID/passwords, encryption, and biometrics.
52. Is there a process in place to monitor and respond to privacy and/or security incidents?	Please indicate a Yes or No response.
52a. If yes, briefly describe the process.	If Yes, provide a brief but thorough description of the procedures in place for handling suspected and confirmed incidents. Consult with your IC Privacy Coordinator and IC ISSO as necessary.

Physical Access Tab

Question	Guidance
53. Are physical access controls in place?	Please indicate a Yes or No. If Yes, a Yes or No response for each category of physical controls listed is required. This information should also appear in the system's C&A package, and can include categories such as guards, close-circuit TV, and physical locks.
***54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls.**	Answered previously on the PIA Summary.

Approval - Promotion/Demotion Tab

If the PIA is complete and accurate, circulate it internally within the respective IC to obtain clearance/ approval. This can be done manually, by printing the PIA and routing it for approval, or electronically, by exporting the PIA to Word and e-mailing it. Those with access to SPORT can review the PIA electronically, and offer comments. Refer to section 6 of this guide for more information on exporting/downloading a PIA from SPORT.

Question	Guidance
1. System Information	Please provide the IT System Name. This should match the answer to Question 7 and the IT System Item Name at the top of the PIA.
2. PIA Reviewer	The PIA Reviewer role should typically be assigned to the appropriate IC Privacy Coordinator, who reviews the submitted PIA for completeness and accuracy. If changes are necessary following the review of the PIA, the PIA Reviewer will request changes by indicating comments in SPORT and demote the PIA to the System Owner/Manager for correction. Once approved, the PIA Reviewer should promote the PIA to the NIH SOP by selecting Promote from the drop-down menu, adding any applicable comments, entering his or her name and contact information, and selecting the correct date in the appropriate boxes.
3. Senior Official for Privacy Approval/Promotion or Demotion	The NIH SOP will review the PIAs once approved at the IC-level, and will either Demote it back to the IC for revisions, or promote it to the Department for approval.
4. OPDIV Senior Official for Privacy or Designee Approval	The NIH SOP will include the appropriate contact information to this section prior to submission to the Department.
5. Department Approval to Publish to the Web	Once the PIA is approved at the Department level, NIH will be notified of the publication date, and the Summary will be posted on the HHS website at: http://www.hhs.gov/pia/nih/index.html.

9 The TPWA PIA Questions

The following required questions represent the information necessary to complete the TPWA PIA for transmission by the NIH SOP and to the Department.[6] PIA Authors and PIA Reviewers may use the following as assistance when completing the questions found on the TPWA PIA Form ONLY.

General Information Section

Question	Guidance
***1. TPWA Name:**	Use the scroll down menu to select the TPWA for which

[6] Questions on the form with an asterisk (*) will be used by the Department to generate a TPWA PIA summary, which will be posted to the Department's public PIA Website.

	you are completing a PIA. When notified of the existence of a TPWA, the NIH Prosight FISMA Coordinator will list the TPWA within the 06.4 HHS PIA TPWA_PIA" link in SPORT. The TPWA PIA Form automatically for population. The TPWA name should follow the format "OPDIV name/ name of TPWA/ and name of OPDIV use of the TPWA" (e.g., NIH/NationalCancer Institute(NCI)/Facebook/Cancer.gov). This construction should reflect the same name for which the form is titled in SPORT.
2. Is this a new PIA?	Using the pull-down menu, indicate whether the TPWA is new or if it's an existing IT System for which you are now modifying the PIA.
2a. If this is a revision of an existing PIA, please provide a reason for revision.	If the answer to Question 2 is No then briefly explain the reason why the PIA is being revised. Common examples include: revising the PIA as part of annual review process or revising the PIA to reflect changes to NIH's use of the TPWA.
3. Date of this Submission:	For all PIAs, the date of submission is the final date that the PIA is completed and ready for submission to the NIH SOP. If the PIA is demoted and information is changed, or the PIA is validated for reporting purposes, the date of submission should be adjusted to reflect the changes before being promoted again.
***4. OPDIV Name:**	Use the scroll down menu to select the TPWA for which you are completing a PIA. When notified of the existence of a TPWA, the NIH will be listed automatically by the CIT as HHS/NIH/Institute.
***5. Unique Project Identifier (UPI) Number for current fiscal year (if applicable):**	The UPI number is used to report IT investments during the budget process and ensure the integration of strategic planning, budgeting, procurement, and the management of IT investments in support of the agency's mission and business needs. It reflects information such as the OPDIV and office where the investment project was initiated, the type of investment, and other information. The UPI number is used by OMB to track the system through the PIA, C&A, and POA&M processes. The number is attached to Exhibit 53s and described in Exhibit 300s, which are submitted to OMB prior to major investment and budget requests. The number is long and appears as follows: 009-25-xx-xx-xx-xxxx-xx-xxx-xxx. If unsure that the TPWA requires a UPI number, check with the NIH ISAO within CIT at: NIHSport@mail.nih.gov to confirm. Generally, the use of a TPWA would not require a UPI number if, for example, no Exhibit 300 exists or the use of the TPWA is not classified as a "Major

	Investment." If the use of TPWA has a UPI number, this number must be included in the PIA to ensure proper tracking and submission of information to OMB. The Department should be especially careful to ensure that the correct UPI number has been included. The format of the UPI number is established in OMB Circular A-11, Section 53.8. The number reflects information such as the OPDIV and office where the investment project was initiated, the type of investment, and other information. Not all uses of TPWAs will have a UPI number. Only uses that are affiliated with an Exhibit 300 or 53 will have a UPI number.
***6. Will the use of a TPWA create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?**	A SORN describes the Privacy Act system of records, and the categories of PII collected, maintained, retrieved, and used within an information collection. Each use of a Third-Party Website and Application should be assessed to determine the impact of the Privacy Act on the TPWA. If a SORN is required and a SORN number is under development or does not exist, answer Yes. Not all uses of TPWAs create a requirement for a SORN. If the TPWA is not subject to the Privacy Act and does not require a SORN, answer No (refer to Section IV of this guide for more information). Work with the IC Privacy Coordinator to determine which SORN appropriately covers the IT System. A list of IC Privacy Coordinators can be located at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3. NIH Privacy Act System Notices can be located by visiting the OSOP Privacy website at: http://oma.od.nih.gov/ms/privacy/pa-files/read02systems.htm.
***6a. If yes, indicate the SORN number or describe plans to put one in place:**	If the answer to Question 6 is Yes, provide the number of the applicable SORN or describe the plans to update a SORN in place. Completed SORNs must be publicly posted to the Internet. Most OPDIV SORNs can be found at: http://www.hhs.gov/foia/privacy/sorns.html.
***7. Will the use of a TPWA create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?**	The introduction of social media technologies leave federal agencies with an invaluable method of interacting with popular web application platforms. However, federal agencies must be cognizant that leveraging social media creates new information that will need to be managed like other agency information resources. There are general uses of social media that may require an Information Collection Request (ICR) and an OMB Control Number, required by the PRA prior to operating a TPWA within NIH. However, the application of the PRA depends upon

	the circumstance in which PII is collected from members of the public. According to the OMB Memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, agencies may use social media and technologies to promote open government in many ways without triggering the PRA. For example: • General solicitations: Under the general solicitations exclusion, the PRA does not apply to notices published in the Federal Register or other publications that request public comments on proposed regulations, or any general requests for comments "regardless of the form or format thereof." A general solicitation may have a degree of specificity. For example, a general solicitation may pose a series of specific questions designed to elicit relevant public feedback, but the solicitation may not be a survey and the responses should be unstructured. • Feedback requests: Under existing OMB policy, agency uses of general or undifferentiated "suggestion boxes" are not covered by the PRA. Similarly, an agency does not trigger the PRA's requirements when it posts its email address or uses an application for brainstorming or idea-generating on its Website to enable the public to submit feedback. However, if an agency requests information from respondents beyond name and email or mailing address (e.g., age, sex, race/ethnicity, employment, or citizenship status), this request is covered by the PRA because it seeks information beyond what is "necessary" for self-identification of the respondent. The PRA does not apply to posts that allow members of the public to provide general or unstructured feedback about a program (such as a standard Federal Register notice, a request for comments on a report or proposed initiative, or a request for ideas, comments, suggestions, or anything else that might improve the program). • Electronic subscriptions to agency notifications or publications: OMB does not consider mailing addresses collected for agency mailing lists to be information subject to the PRA. Similarly, an agency is not collecting information when it collects email addresses for agency updates, alerts, publications, or email subscription services; mobile phone numbers for text notification lists; or addresses for Really Simple

Syndication (RSS) feeds, which allow individuals to customize and subscribe to updates from Websites. If, however, the agency requests a member of the public to provide additional information (e.g., age, sex, race/ethnicity, employment, or citizenship status) beyond what is necessary to ensure proper transmission of responses, the collection of that additional information is covered under the PRA.

- Public meetings: Under current OMB policy, agencies do not trigger the PRA's requirements by hosting a public meeting. For purposes of the PRA, OMB considers interactive meeting tools—including but not limited to public conference calls, webinars, blogs, discussion boards, forums, message boards, chat sessions, social networks, and online communities — to be equivalent to in-person public meetings. However, activities that go beyond the scope of in-person public meetings or hearings are subject to the PRA. For example, focus groups, whether conducted in person or done via webinar, are subject to the PRA. Similarly, if an agency takes the opportunity of a public meeting to distribute a survey, or to ask identical questions of 10 or more attendees, the questions count as an information collection.
- Wikis and collaborative drafting platforms: Wikis are an example of a web-based collaboration tool that generally does not trigger the PRA because they merely facilitate interactions between the agencies and the public. However, some uses of wiki technologies are covered by the PRA, such as using a wiki to collect information that an agency would otherwise gather by asking for responses to identical questions (e.g., posting a spreadsheet into which respondents are directed to enter compliance data).
- 'Like' items: Like items that are not subject to the PRA include those collected to create user accounts or profiles for agency Websites; items collected to allow users to customize or influence the appearance of an agency Website; or ratings and rankings of postings or comments by Website users. Further, contests conducted by the agency asking the public for ideas to improve current practices under a statute that it administers, for potential solutions to a scientific, technological, social, or other problem, or for innovations (e.g., video and software applications) that

	might advance an agency's mission, is not subject to the PRA. However, if the contest takes the form of a structured response (i.e., series of questions that entrants must answer to take part in the contest), or it collects demographic information about the entrants, the information collected as a part of the contest is subject to the PRA. Additionally, items necessary to complete a voluntary commercial transaction (i.e., information that is necessary for the selection, payment, or delivery of an item, or to identify the person ordering an item) are not, subject to the PRA if used solely for the purpose of completing a commercial transaction. Similarly, agency use of web-based applications to conduct such transactions is not subject to the PRA. However, if information is required or requested about a person's qualifications to participate in the transaction (e.g., a person's employment status as a member of law enforcement) or a person's sex or age, the information is subject to the PRA if it is beyond what is necessary to complete the sale. You can click on the Office of Extramural Research (OER) Intranet website at: http://odoerdb2.od.nih.gov/oer/policies/project_clearance/pcb.htm to obtain a list of NIH Information Collection Clearance Officers, and get more information about whether the IT System has been approved for OMB information collection.
***7a. If yes, indicate the OMB approval number and approval number expiration date or describe the plans to obtain OMB clearance:**	If the answer to Question 7 is Yes provide the number of the applicable OMB Approval Number or describe the plans to update an OMB Approval Number currently in place.
8. Does the TPWA contain Federal records?	Each use of a TPWA should be assessed to determine if the TPWA maintains federal records. If the TPWA maintains federal records, the NIH Records Liaisons should be able to assist in determining applicable records requirements. If the TPWA does not contain federal records, answer No.
***9. Point of Contact (POC).**	The POC is the person to whom questions about the use of the TPWA and the responses to the PIA may be addressed. Provide the name, title, location, and telephone number of an individual. Please note the POC's information will be made publicly available.
***10. Describe the specific**	NIH may use TPWAs to maximize opportunities to

purpose for the OPDIV's use of the TPWA:	engage and communicate with the public. The PIA's primary purpose is to convey the privacy/security implications of using a TPWA. The PIA provides the PIA Author with an opportunity to explain the reasoning behind why a TPWA is being used and its importance to the NIH/IC mission.

Requirements Section

Question	Guidance
11. Have the third-party's privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?	Prior to utilizing a TPWA, the Privacy IC must evaluate the privacy policies of the third-party to determine if there are any risks to a user that would preclude the IC from utilizing the tool to engage the public. Examples of a potential risk could include a third-party's release of personal information for commercial purposes (e.g., Facebook could change its privacy policy at any time during the day, but unless a memorandum is in place Facebook does not have to notify).
12. Describe alternative means by which the public can obtain comparable information or services if they choose not to use the TPWA:	According to OMB M-10-23, members of the public should not be required to use a TPWA solely to obtain information or services. NIH must provide members of the public with an alternative means to get the same information or services being offered by the TPWA.
13. Does the TPWA have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?	NIH must clearly identify the ownership or sponsorship of TPWA uses through Department, NIH or IC branding. Branding is not required to be an official agency seal or logo; however, the image must clearly indicate a government presence. Contact the HHS Center for New Media for information on agency logo and branding requirements/restrictions or visit: http://newmedia.hhs.gov/standards/index.html#Branding2.
14. How does the public navigate to the TPWA from the OPDIV: (i) an external hyperlink from an HHS Website or Website operated on behalf of HHS; (ii) incorporated or embedded on HHS Website; or (iii) Other?	This question addresses how NIH alerts members of the public that a link, embedded hyperlink, or other navigation tool will take them from a government website to a TPWA. Select whether the NIH: (i) provides an external hyperlink to the TPWA from the NIH Website or a Website operated on behalf of the NIH; (ii) incorporates or embeds the TPWA on the NIH Website; or (iii) utilizes another approach to inform members of the public.
14a. If other, please describe how	If the answer to Question 14 is Other, the PIA Author

the public navigates to the TPWA:	must provide a description of the approach.
14b. If the public navigates to the TPWA via an external hyperlink, is there an alert to notify the public that they are being directed to a nongovernmental Website:	If the answer to Question 14 is “External Hyperlink from an HHS Website or Website operated on behalf of HHS,” identify if the Website or application contains an alert notifying the user that the information and/or processes of the TPWA are not controlled by the Department.

Notice Practices Section

Question	Guidance
15. Has the OPDIV Privacy Policy been updated to describe the use of a TPWA?	The term “Privacy Policy,” refers to a single, centrally located statement of the Website’s privacy standards and processes, which is accessible from an IC’s official homepage. The Privacy Policy should be a consolidated explanation of NIH’s general privacy-related practices that pertain to its official Website and its other online activities. It must be updated to include required information about the use of a TPWA.
15a. Provide a hyperlink to the OPDIV Privacy Policy:	Provide the hyperlink for the Privacy Policy that informs the public of NIH’s use of the TPWA.
16. Is an OPDIV Privacy Notice posted on the TPWA?	A “Privacy Notice” is a brief description of how the Privacy Policy will apply in a specific situation. The Privacy Notice must be prominently displayed on the TPWA used by the IC. Please note, the use of some TPWAs may make it difficult to post a Privacy Notice due to technical limitations. The IC should make their best efforts to ensure that a Privacy Notice is posted when it is feasible.
16a. Confirm that the OPDIV’s Privacy Notice contains all the following elements: **i. An explanation that the Website or application is not government-owned or government-operated;** **ii. An indication of whether and how the OPDIV will maintain, use, or share PII that becomes available;** **iii. An explanation that by using the TPWA to communicate with the OPDIV, individuals may be providing**	If the answer to Question 16 is Yes provide a confirmation that the Privacy Notice includes the required content. See Implementation of OMB M-10-22 and M-10-23 dated December 21, 2010 for more information about the required content and placement of the Privacy Notice.

nongovernmental third-parties with access to PII; **iv. A link to the official OPDIV Website; and** **v. A link to the OPDIV Privacy Policy.**	
16b. Is the OPDIV's Privacy Notice prominently displayed at all locations on the TPWA where the public might make PII available?	If the answer to Question 16 is Yes, provide a confirmation that the Privacy Notice is prominently placed at all locations on the TPWA where the public might make PII available. Please note that the requirement refers to situations in which the public might make PII available according to OMB M-10-23. Per OMB M-10-23 the term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the Website or applications. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Information Collection and Use Practices Section

Question	Guidance
***17. Is PII collected by the OPDIV from the TPWA?**	"Collecting PII" is defined by the Department as any act, whether by humans or a technology, to collect or obtain any PII that is requested or made available through the TPWA with or without the consent of the user for any period of time (for example, if ICs are copying and pasting comments that include PII into a file for other uses, that is considered a collection.)
***18. Will the TPWA make PII available to the OPDIV?**	Please note that the OMB definition of "make PII available" is very broad, therefore it is likely that any use of a TPWA by the IC is making PII available to the IC. Third-Party Websites or Applications that use features such as an option to become a "follower," "fan," to comment or to allow users to post and/or display names of the visitors, is considered to be making PII available to the IC. If the TPWA will not make PII available to the IC, answer No. Please note this question refers to the activities of the IC, not the activities of the TPWA.
***19. Describe the PII that will be collected by the OPDIV from the Third-Party Website or**	The purpose of this question is to clearly outline to the public the type of PII that is collected or that will likely be made available to the IC through the public's use of the

Application and/or the PII which the public could make available to the OPDIV through the use of the TPWA, and the intended or expected use of the PII?	TPWA and to identify how the IC will use that information. As a best practice, the PIA Author can categorize the PII under the appropriate heading of "PII Collected" or "PII Likely to be Made Available," and indicate what the IC intends to do with each type of PII. If an IC does not use the PII that was collected or made available, it is recommended that the answer "Does Not Use PII" be included versus No or N/A. It is also recommended that the PIA Author ensure that the answer considers the situation in which a visitor to the TPWA could submit their own PII using a commenting or similar feature of the TPWA, and how this information may be used. A common example would be if a member of the public used the TPWA to provide information about him/herself to the IC. Within this scenario, it is often unpredictable what PII the public might make available to the IC. Therefore, it is recommended that the PII within this scenario be captured as "Unsolicited PII from the Public" and indicate how the PII may be used. If the IC takes action to remove unsolicited PII, it should be noted.

Information Sharing and Maintenance Practices Section

Question	Guidance
***20. Describe the type of PII from the TPWA that will be shared, with whom the PII will be shared, and the purpose of the information sharing:**	The purpose of this question is to outline the type of PII collected (name, email address, etc.) or made available to the IC through the use of a TPWA, to whom the PII will be shared (whether the sharing is internal to HHS or is to parties outside of HHS), and the business purpose for sharing the PII. If the IC does not share any PII, indicate this by stating "No PII is Shared" versus stating No or N/A.
***20a. If PII is shared, how are the risks of sharing PII going to be mitigated?**	If the answer to Question 20 is Yes, provide a description for how any risks associated with sharing the PII are mitigated. Within the answer, describe any applicable administrative, technical, or operational controls that help minimize the risks associated with the information sharing. If the IC does not share PII, indicate this by stating "No PII is Shared" versus stating No or N/A.
***21. Will the PII from the TPWA be maintained by the OPDIV?**	If the IC plans to maintain the PII from the TPWA, answer "YES." Although not defined by OMB, for the purpose of this document, the term "maintain" implies that the PII (in any format) is actively maintained for a specific period of time. For example, the creation of back-up tapes for the

	purposes of business continuity and business resumption, information contained within emails, or any other process that creates a temporary record should be included within the description of how the IC plans to "maintain" the PII from the TPWA. For example, if comments posted to the TPWA are being saved in a file, the comments are being exported, and/or screen shots are being saved, that is considered maintaining PII. If the IC does not maintain the PII from the TPWA, answer No.
***21a. If PII will be maintained, indicate how long the PII will be maintained:**	If the answer to Question 21 is Yes, describe how long the IC plans to maintain the PII. A complete response will indicate the timeframe records will be maintained per record schedule guidance. For more information about the appropriate timeframes for maintaining records, please consult the appropriate IC Records Management Officer who may be found at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=2. If the OPDIV does not maintain the PII from the TPWA, answer "No PII is Maintained" versus stating No or N/A.
***22. Describe how PII that is used or maintained will be secured:**	Provide a description of the applicable physical, technical, or management controls that will be used to secure the PII being used or maintained by the IC. As a best practice, this question should not have an answer as No or N/A. If an IC does not use or maintaining any PII from the TPWA, indicate this by stating "No PII Used or Maintained".
***23. What other privacy risks exist and how will they be mitigated?**	ICs should assess additional privacy risks and make plans to mitigate these risks. As a best practice, the answer to this question should not be No or N/A. Any use of a TPWA does introduce some new privacy risks. For example, a TPWA that allows individuals to provide comments introduces the privacy risk that members of the public could provide their own PII. A means for managing this risk could be the development of policies and procedures to monitor and moderate comments. Other examples of common privacy risks include changes in technology or modifications to the TPWA's privacy policies.

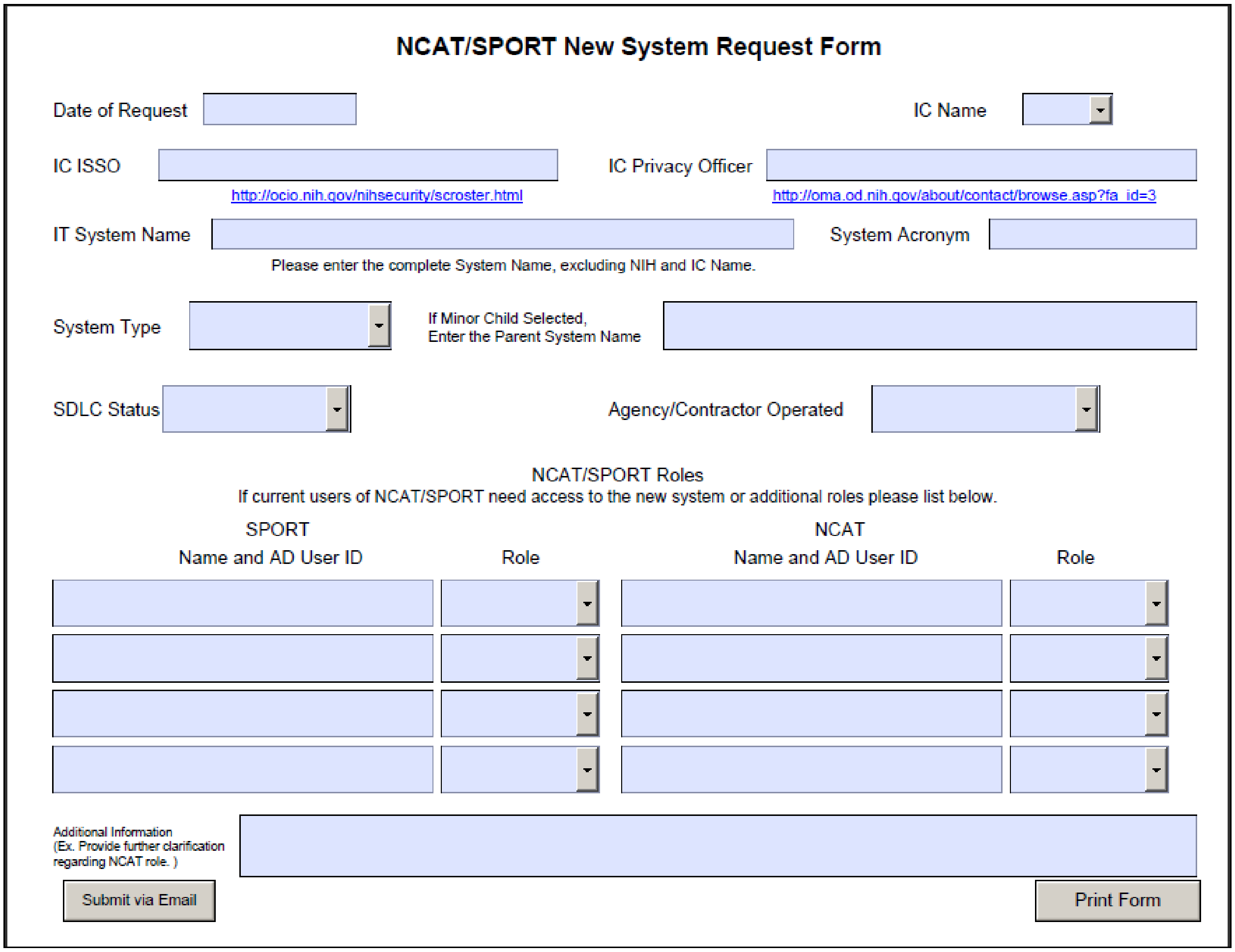
10 Conclusion

NIH must perform thorough PIAs to satisfy the requirements of the *E-Government Act* and OMB Memoranda as set forth in Departmental and NIH policy. An accurate PIA presents NIH with the opportunity to assess its compliance with the requirements of the Privacy Act, *E-Government*

Act of 2002, FISMA, COPPA, and other federal laws, and policies. Furthermore, because the IT System and TPWA PIA Summaries are made publicly available, the Department and NIH are presented with an opportunity to assure the public that it is providing government services in a manner that considers the sensitivity of the personal information it receives.

11 Appendix A: NEAR/NCAT/HEAR/SPORT Access Form

The NIH Certification and Accreditation Tool (NCAT) is a NIH system used to track our system inventory from a Certification & Accreditation (C&A) boundary/FISMA perspective. It includes all IT systems that require a C&A or are minor systems covered within the C&A boundaries of a parent system. NCAT collects some basic privacy information for C&A purposes, including references to Privacy Act Systems of Record Notices (SORNs) and an upload of the Privacy Impact Assessment (PIA) form pulled from the HHS Security and Privacy Online Reporting Tool (SPORT) used to create and track PIAs.



NCAT/SPORT New System Request Form

Date of Request

IC Name

IC ISSO

http://ocio.nih.gov/nihsecurity/scroster.html

IC Privacy Officer

http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

IT System Name

Please enter the complete System Name, excluding NIH and IC Name.

System Acronym

System Type

If Minor Child Selected,
Enter the Parent System Name

SDLC Status

Agency/Contractor Operated

NCAT/SPORT Roles

If current users of NCAT/SPORT need access to the new system or additional roles please list below.

SPORT Name and AD User ID	Role	NCAT Name and AD User ID	Role

Additional Information
(Ex. Provide further clarification regarding NCAT role.)

Submit via Email

Print Form

Figure 1. NEAR/NCAT/HEAR/SPORT Access Form Screenshot

12 Appendix B: IT System PIA Form Template

06.1 HHS Privacy Impact Assessment (Form)	(Item)	Primavera ProSight

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?	
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	
*2. OPDIV Name:	
*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:

Point of Contact Information	
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. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents federal contact data (i.e., federal contact name, federal address, federal phone number, and federal email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary is required). If the system contains a mixture of federal contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

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?

*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)

*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):

*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:
*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]):
*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)
*37. Does the website have any information or pages directed at children under the age of thirteen?
*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 the SORN)
*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

PIA REQUIRE 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?

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 (Data is auto-populated from the System Inventory form, UPI table):

*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:

5a. OMB Collection Approval Number Expiration Date:

*6. Other Identifying Number(s):

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

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

System Location:	
OPDIV or contractor office building	
Room	
City	
State	

*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	

The following information will not be made publicly available:

POC Title	
POC Organization	
POC Phone	
POC Email	

*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)

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1	System Characterization and Data Configuration

11. Does HHS own the system?

11a. If no, identify the System Owner:

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

12a. If no, identify the system operator:

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

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

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	

Anonymous to Non-Anonymous	
Significant System Management Changes	
Significant Merging	
New Public Access	
Commercial Sources	
New Interagency Uses	
Internal Flow or Collection	
Alteration in Character of Data	

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

*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. Later questions will try to understand the character of the data and its applicability to the requirements under the Privacy Act or other legislation. If the information contained in the system ONLY represents business contact data (i.e., business contact name, business address, business phone number, and business email address), it does not qualify as PII, according to the E-Government Act of 2002, and the response to Q.17 should be No (only the PIA Summary is required). If the system contains a mixture of business contact information and other types of PII, the response to Q.17 should be Yes (full PIA is required).

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)	
Date of Birth	
Social Security Number (SSN)	
Photographic Identifiers	
Driver’s License	
Biometric Identifiers	
Mother’s Maiden Name	

Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web Uniform Resource Locator(s) (URL)	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

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	
Public Citizen	
Patients	
Business partners/contacts (Federal, state, local agencies)	
Vendors/Suppliers/Contractors	
Other	

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

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)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver’s License	
Biometric Identifiers	
Mother’s Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

*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)

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?	

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

Other	

*23. If the system shares or discloses PII please specify with whom and for what purpose(s):

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?

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)?

26. Are individuals notified how their PII is going to be used?

26a. 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?

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?

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?

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		
Administrators		
Developers		

Contractors		
Other		

*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:

*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.])

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)

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		
Intranet		
Both		

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.).

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?

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)?

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

36. Does the website employ tracking technologies?

Please indicate “Yes”, “No”, or “N/A” for each type of cookie below:	**Yes/No/N/A**
Web Bugs	
Web Beacons	
Session Cookies	
Persistent Cookies	
Other	

*37. Does the website have any information or pages directed at children under the age of thirteen?

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?

Please indicate “Yes” or “No” for each category below:	**Yes/No**
Name (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	

Driver's License	
Biometric Identifiers	
Mother's Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

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

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

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)?
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?
43. Is there a contingency (or backup) plan for the system?
44. Are files backed up regularly?
45. Are backup files stored offsite?
46. Are there user manuals for the system?
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?
48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?
49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?
49a. 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 the SORN):
50a. 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?

Please indicate “Yes” or “No” for each category below:	Yes/No
User Identification	
Passwords	
Firewall	
Virtual Private Network (VPN)	
Encryption	
Intrusion Detection System (IDS)	
Common Access Cards (CAC)	
Smart Cards	
Biometrics	
Public Key Infrastructure (PKI)	

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

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

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Please indicate “Yes” or “No” for each category below:	Yes/No
Guards	
Identification Badges	
Key Cards	
Cipher Locks	

Biometrics	
Closed Circuit TV (CCTV)	

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

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:	

PIA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	
PIA Missing Fields:	

13 Appendix C: TPWA PIA Form Template

06.4 Third Party Web PIA (Form)	Primavera ProSight

Form Report, printed Feb 8, 2011

TPWA_PIA

1	Overview
The PIA determines if Personally Identifiable Information (PII) is contained within a system, the kind of PII involved, what is done with that information, and how the PII is protected. OPDIV/STAFFDIV uses of third-party Websites or applications are subject to requirements based on privacy laws, regulations, and guidance. The Department of Health and Human Services (HHS) Privacy Act Officer may be contacted for issues related to the Freedom of Information Act (FOIA) and/or the Privacy Act. Respective HHS 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.	
This Privacy Impact Assessment is to be completed in accordance with Office of Management and Budget (OMB) Memorandum (M) 03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 and OMB M-10-23 Guidance for Agency Use of Third-Party Websites and Applications. For complete background and guidance, please read the Standard Operating Procedures (SOPs) for the Privacy Impact Assessment for Third-Party Websites of Applications prior to completing this PIA.	
Questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to OMB and public posting in accordance with OMB M-03-22 and OMB M-10-23.	

2	General Information
1. Third-Party Website or Application Name:	
2. Is this a new PIA?	
2a. If this is a revision of an existing PIA, please provide a reason for revision:	
3. Date of this Submission:	
4. OPDIV Name:	
5. Unique Project Identifier (UPI) Number for current fiscal year (if applicable):	

6.Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?	
6a. If yes, indicate the SORN number or describe the plans to put one in place:	
7. Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?	
7a. If yes, indicate the OMB approval number and approval number expiration date or describe the plans to obtain OMB clearance:	
8. Does the third-party Website or application contain Federal records?	

***9. Point of Contact (POC). The POC is the person to whom questions about the responses to the third-party Website or application PIA may be addressed:**

Point of Contact Information	
Name	
Title	
Location	
Phone Number	

10. Describe the specific purpose for the OPDIV use of the third-party	

Website or application:	

3	Requirements
11. Have the third-party's privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?	
12. Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:	
13. Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?	
14. How does the public navigate to the third-party Website or application from the OPDIV: (i) an external hyperlink from an HHS Website or Website operated on behalf of HHS; (ii) incorporated or embedded on HHS Website; or (iii) Other?	
14a. If other, please describe how the public navigates to the third-party Website or application:	
14b. If the public	

navigates to the third-party Website or application via an external hyperlink, is there an alert to notify the public that they are being directed to a nongovernmental Website?	

4	Notice Practices
15. Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?	
15a. Provide a hyperlink to the OPDIV Privacy Policy:	
16. Is an OPDIV Privacy Notice posted on the third-party Website or application?	
16a. Confirm that the Privacy Notice contains all of the following elements: (i) An explanation that the Website or application is not government-owned or government-operated; (ii) An indication of whether and how the OPDIV will maintain, use, or share PII that becomes available; (iii) An explanation that by using the third-party Website or application to communicate with the OPDIV, individuals may be providing nongovernmental third-parties with access to PII; (iv) A link to the official OPDIV Website; and (v) A link to the OPDIV Privacy Policy.	

16b. Is the OPDIV's Privacy Notice prominently displayed at all locations on the third-party Website or application where the public might make PII available?	

5	Information Collection & Use Practices
17. Is PII collected by the OPDIV from the third-party Website or application?	
18. Will the third-party Website or application make PII available to the OPDIV?	
19. Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:	

6	Information Sharing & Maintenance Practices
20. Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:	
20a. If PII is shared, how are the risks of sharing PII mitigated?	
21. Will the PII from the third-party Website or application be maintained by the	

OPDIV?	
21a. If PII will be maintained, indicate how long the PII will be maintained:	
22. Describe how PII that is used or maintained will be secured:	
23. What other privacy risks exist and how will they be mitigated?	

TPWA % COMPLETE

1	PIA Completion
PIA Percentage Complete:	
TPWA_Missing_Fields:	

14 Appendix D: HHS, NIH, and Government-wide SORNs

Internal NIH Systems

09-25-0005, *Library Operations and NIH Library User I.D. File*, HHS/NIH
09-25-0007, *NIH Safety Glasses Issuance Program*, HHS/NIH/ORS
09-25-0011, *Blood Donor Records*, HHS/NIH/CC
09-25-0012, *Candidate Healthy Volunteer Records*, HHS/NIH/CC
09-25-0014, *Student Records*, HHS/NIH/OD/OIR/OE
09-25-0033, *Fellowships Awarded by Foreign Organizations*, HHS/NIH/FIC
09-25-0034, *Scholars-in-Residence Program*, HHS/NIH/FIC
09-25-0036, *Extramural Awards and Chartered Advisory Committees* (IMPAC 2), *Contract* Information (DCIS), and *Cooperative Agreement Information*, HHS/NIH
09-25-0041, *Scientists Requesting Hormone Distribution*, HHS/NIH/NIDDK
09-25-0054, *Property Accounting* (Card Key System) HHS/NIH/ORS
09-25-0078, *Consultant File*, HHS/NIH/NHLBI
09-25-0087, *Senior Staff*, HHS/NIH/NIAID
09-25-0099, *Patient Medical Records*, HHS/NIH/CC
09-25-0105, *Health Records of Employees, Visiting Scientists, Fellows, and Others Who Receive Medical Care Through the Employee Health Unit*, HHS/NIH/ORS
09-25-0106, *Office of the NIH Director and Institute/Center Correspondence Records*, HHS/NIH/OD
09-25-0108, *Guest Researchers, Special Volunteers, and Scientists Emeriti*, HHS/NIH/OHRM
09-25-0115, *Curricula Vitae of Consultants and Clinical Investigators*, HHS/NIH/NIAID
09-25-0118, *Professional Services Contractors*, HHS/NIH/NCI
09-25-0121, *Senior International Fellowships Program*, HHS/NIH/FIC
09-25-0124, *Pharmacology Research Associates*, HHS/NIH/NIGMS
09-25-0140, *International Scientific Researchers in Intramural Laboratories at the National Institutes of Health*, HHS/NIH/FIC/ORS/DIRS
09-25-0156, *Records of Participants in Programs and Respondents in Surveys Used to Evaluate Programs of the Public Health Service*, HHS/PHS/NIH/OD
09-25-0158, *Records of Applicants and Awardees of the NIH Intramural Research Training Awards Program*, HHS/NIH/OD/OIR/OE
09-25-0160, *United States Renal Data System* (USRDS), HHS/NIH/NIDDK
09-25-0165, *National Institutes of Health (NIH) Office of Loan Repayment and Scholarship (OLRS) Records System*, HHS/NIH/OD
09-25-0166, *Radiation and Occupational Safety and Health Management Information Systems*, HHS/NIH/ORS
09-25-0167, *National Institutes of Health (NIH) TRANSHARE Program*, HHS/NIH/OD
09-25-0168, *Invention, Patent, and Licensing Documents Submitted to the Public Health Service by its Employees, Grantees, Fellowship Recipients, and Contractors*, HHS/NIH/OD [revised 10/3/06]
09-25-0169, *Medical Staff-Credentials Files*, HHS/NIH/CC
09-25-0200, *Basic and Population-based Research Studies of the National Institutes of Health* (NIH), HHS/NIH/OD
09-25-0202, *Patient Records on PHS Beneficiaries (1935-1974) and Civilly Committed Drug*

Abusers (1967-1976) Treated at the PHS Hospitals in Fort Worth, Texas, or Lexington, Kentucky, HHS/NIH/NIDA
09-25-0203, *National Institute on Drug Abuse, Intramural Research Program, Federal Prisoner and Non-Prisoner Research Files,* HHS/NIH/NIDA
09-25-0207, *Subject-Participants in Pharmacokinetic Studies on Drugs of Abuse and on Treatment Medications*, HHS/NIH/NIDA
09-25-0208, *Drug Abuse Treatment Outcome Study* (DATOS), HHS/NIH/NIDA
09-25-0209, *Subject-Participants in Drug Abuse Research Studies on Drug Dependence and in Research Supporting Investigational New Drug and New Drug Applications*, HHS/NIH/NIDA
09-25-0210, *Shipment Records of Drugs of Abuse to Authorized Researchers*, HHS/NIH/NIDA
09-25-0211, *Intramural Research Program Records of In-and Out-Patients with Various Types of Alcohol Abuse and Dependence, Relatives of Patients with Alcoholism, and Healthy Volunteers*, HHS/NIH/NIAAA
09-25-0213, *Employee Conduct Investigative Records*, HHS/NIH/OD/OM/OA/OMA
09-25-0216, *NIH Electronic Directory*, HHS/NIH (to be renamed NIH Enterprise Directory, and amended to include a proposed new use for emergency notification purposes.)
09-25-0217, *NIH New Business System* (NBS), HHS/NIH

Internal HHS Systems

09-90-0008, *Conflict of Interest Records*, HHS/OS/ASPER
09-90-0018, *Personnel Records in Operating Offices*, HHS/OS/ASPER
09-90-0020, *Suitability for Employment Records*, HHS/OS/ASPER (to be renamed HHS Personnel Security, and amended to be compliant with the new I.D. badge procedure under HSPD-12)
09-90-0024, *Unified Financial Management System*, HHS/OS
09-90-0039, *National Disaster Claims Processing System*
09-90-0777, *Identification and Credentialing Issuance Station and System*, HHS/OCID (in draft form - to cover personal identity verification (PIV) card holders as well as short-term employees, temporary guests and visitors)

Government Systems

OGE/GOVT-1, *Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records*
OGE/GOVT-2, *Executive Branch Confidential Financial Disclosure Reports*
OPM/GOVT-1, *General Personnel Records*

15 Appendix E: Sample IT System PIA (with PII)

06.1 HHS Privacy Impact Assessment (Form) / NIH NCI Employee Database Internet Edition (Item)	Primavera ProSight

Form Report, printed by: Seymour, Kristina, Jul 5, 2011

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:

Jul 30, 2010

*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):

09-90-0018

*5. OMB Information Collection Approval Number:

No

*6. Other Identifying Number(s):

N/A

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

NIH NCI Employee Database Internet Edition (EDie)

*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	Bob Barber

*10. Provide an overview of the system:

EDie is a web-based application that allows institutes to accurately maintain individual employee, contractor, and volunteer information, as well as plan for, monitor, and report on workforce staffing levels.

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

New

*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.

No

*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):

Information is intended for internal senior administrative use only and will not be shared with other entities. Refer to SORN 09-90-0018.

*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:

EDie is a web-based application that allows institutes to accurately maintain individual employee, contractor, and volunteer information, as well as plan for, monitor, and report on workforce staffing levels. All information collected is pertinent to a personnel file and represents only federal contact data. The EDie system does contain PII data as described in question 17 of the PIA. There are many uses for this information: (a) tracking a time-limited appointment to ensure renewals are done in a timely manner thereby avoiding any break in service; (b) ensuring that allocated FTE ceilings are maintained; (c) ensuring salary equality for various hiring mechanisms; (d) the ability to provide reports requested by the NIH Director; (e) maintaining lists of non FTEs, special volunteers, contractors, etc. Information is mandatory at time of hire.
*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.]):
Information is collected from documents provided by employees (CV, resumes, etc.) at the time of appointment; it is provided in personnel packages submitted through channels in order to effect a hire. This information is put into Capital HR and Fellowship Payment System (FPS) and subsequently downloaded into EDie. Individuals are notified of the collection and use of data as a part of the hiring process. Changes to the system or use of the information is relayed to employees via official notices from HR and the system owner. 1) N/A: EDie is not the point of original collection of this data. 2) EDie is a reporting system which inherits PII data from other official HR systems. Currently, no users have access to SSN, DOB, and Home address thru the EDie application. 3) We do not expect any significant changes to the system functions related to PII; If this happens, HR and the system owners will notify all affected employees electronically (e-mail).
*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:
Access to sensitive data fields is limited on need to know basis. Each user signs a security statement and received a password. Any violations result in loss of access to system. Information is also secured by separation of duties, and intrusion detection system, firewalls, locks and background investigations. A comprehensive IRT capability is also maintained. This

systems falls under System of Records Notice 09-90-0018.

EDie employs access control policies (NIHNet single sign-on) and access enforcement mechanisms (access control lists) for authentication. Additionally, access enforcement mechanisms are employed at the application level in the form of user assigned groups to further increase security within EDie. Each group has different access privileges. Access can be restricted by content and organization.

From a Physical Access perspective, the Executive Boulevard building is accessible to the public during regular business hours. There is one security guard on duty during regular business hours (8:00 AM -6:00 PM weekdays). The guard is retained by NCI to make frequent foot patrols of the entire building and surrounding areas (including the basement and garage), and one security guard desk at the entrance to the building. Due to the shared roles of offices housed in the building, it is not possible to verify that all NIH visitors to NCI offices have a proper NIH ID badge, or to require non-NIH visitors to sign a visitor log and be escorted. There is an administrative assistant stationed inside the front door of the NCI offices during regular business hours.

There is a guard on patrol duty through midnight on weekdays. Access to the building and elevators is restricted by access card on nights and weekends. Cardkeys, cipher locks, and/or keys are required for access to the NCI suites, the computer room, and rooms containing communications equipment. Access to the computer room and rooms containing communications equipment is limited to a small number of personnel.

Departing employees and contractors are required to turn in their identification badges, cardkeys, and keys as part of the exit process. NCI Administrative Officer is responsible for the control and return of keys and the reporting of stolen keys. NCI Cardkey Coordinators are responsible for the control and return of cardkeys and the reporting of lost/stolen cardkeys.

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:

Jul 30, 2010

*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):

N/A

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

09-90-0018

*5. OMB Information Collection Approval Number:

No

5a. OMB Collection Approval Number Expiration Date:

*6. Other Identifying Number(s):

N/A

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

NIH NCI Employee Database Internet Edition (EDie)

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

System Location:	
OPDIV or contractor office building	6116 Executive Blvd.
Room	175
City	Rockville
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	Bob Barber

The following information will not be made publicly available:

POC Title	Program Analyst
POC Organization	NCI Office of Administrative Operations
POC Phone	301-435-2602
POC Email	barberb@mail.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)

EDie is a web-based application that allows institutes to accurately maintain individual employee, contractor, and volunteer information, as well as plan for, monitor, and report on workforce staffing levels.

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:

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:

New

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?

No

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), Minor Application (child) or Minor Application (stand-alone)?

Minor Application (child)

*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)	Yes
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	No
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	No

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.

No

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

*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	Yes, organization code or other HR related field (FTE/Non-FTE, Position Type, etc.)

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?

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	

*23. If the system shares or discloses PII please specify with whom and for what purpose(s):

Information is intended for internal senior administrative use only and will not be shared with other entities. Refer to SORN 09-90-0018.

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?

Not Applicable

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)?

Not Applicable

26. Are individuals notified how their PII is going to be used?

Not Applicable

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

EDie is not the official source for employee's PII; EDie is a reporting system which inherits this information from other HR systems. Currently, no users within the system have access to view this information. Generally speaking, Individuals are notified of the collection and use of PII data as a part of the hiring process. This is not specific to EDie, since it is not the originating system for this information.

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?

Yes

28a. If yes, please describe briefly the review process. If no, please provide an explanation.

EDie contains standard discrepancy reports that identify official data that is different from data stored in the system.   Additionally, AO’s are responsible for reviewing the data for quality on a routine basis.

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	Yes	To access employee information for personnel actions
Administrators	Yes	To manage the system for reporting purposes
Developers	Yes	To provide technical assistance
Contractors	Yes	Required to have background checks on all contractors
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:

EDie is a web-based application that allows institutes to accurately maintain individual employee, contractor, and volunteer information, as well as plan for, monitor, and report on workforce staffing levels. All information collected is pertinent to a personnel file and represents only federal contact data. The EDie system does contain PII data as described in question 17 of the PIA. There are many uses for this information: (a) tracking a time-limited appointment to ensure renewals are done in a timely manner thereby avoiding any break in service; (b) ensuring that allocated FTE ceilings are maintained; (c) ensuring salary equality for various hiring mechanisms; (d) the ability to provide reports requested by the NIH Director; (e) maintaining lists of non FTEs, special volunteers, contractors, etc. Information is mandatory at time of hire.

*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.])

Information is collected from documents provided by employees (CV, resumes, etc.) at the time of appointment; it is provided in personnel packages submitted through channels in order to effect a hire. This information is put into Capital HR and Fellowship Payment System (FPS) and subsequently downloaded into EDie. Individuals are notified of the collection and use of data as a part of the hiring process. Changes to the system or use of the information is relayed to employees via official notices from HR and the system owner.
1) N/A: EDie is not the point of original collection of this data.
2) EDie is a reporting system which inherits PII data from other official HR systems. Currently, no users have access to SSN, DOB, and Home address thru the EDie application.
3) We do not expect any significant changes to the system functions related to PII; If this happens, HR and the system owners will notify all affected employees electronically (e-mail).

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	No	
Intranet	Yes	
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.).

No

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?

Not Applicable

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)?

Not Applicable

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?

Not Applicable

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 (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):

Jun 8, 2011

41b. If a system requires a C&A and no C&A was completed, is a C&A in progress?

Yes

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):

Role Based Access Controls. Each user's access is individually profiled to limit access to need to know information. Sensitive information, i.e. DOB, SSN, home address are contained on one screen, and access is limited to the highest level.

*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:

Records are retained until there is no further administrative need for retention.
SOR: 09-90-0018

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	No
Intrusion Detection System (IDS)	Yes
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:

Access to and use of these records is limited to those persons whose official duties require such access. Refer to SOR: 09-90-0018.
In addition, NIH CIT incident response policies are followed. Refer to:
http://ocio.nih.gov/security/security-isso.htm#Incident_Response_and_Handling_.

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	No
Closed Circuit TV (CCTV)	No

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

Access to sensitive data fields is limited on need to know basis. Each user signs a security statement and received a password. Any violations result in loss of access to system. Information is also secured by separation of duties, and intrusion detection system, firewalls, locks and background investigations. A comprehensive IRT capability is also maintained. This systems falls under System of Records Notice 09-90-0018.

EDie employs access control policies (NIHNet single sign-on) and access enforcement mechanisms (access control lists) for authentication. Additionally, access enforcement mechanisms are employed at the application level in the form of user assigned groups to further increase security within EDie. Each group has different access privileges. Access can be restricted by content and organization.

From a Physical Access perspective, the Executive Boulevard building is accessible to the public during regular business hours. There is one security guard on duty during regular business hours (8:00 AM -6:00 PM weekdays). The guard is retained by NCI to make frequent foot patrols of the entire building and surrounding areas (including the basement and garage), and one security guard desk at the entrance to the building. Due to the shared roles of offices housed in the building, it is not possible to verify that all NIH visitors to NCI offices have a proper NIH ID badge, or to require non-NIH visitors to sign a visitor log and be escorted. There is an administrative assistant stationed inside the front door of the NCI offices during regular business hours.

There is a guard on patrol duty through midnight on weekdays. Access to the building and elevators is restricted by access card on nights and weekends. Cardkeys, cipher locks, and/or keys are required for access to the NCI suites, the computer room, and rooms containing communications equipment. Access to the computer room and rooms containing communications equipment is limited to a small number of personnel.

Departing employees and contractors are required to turn in their identification badges, cardkeys, and keys as part of the exit process. NCI Administrative Officer is responsible for the control and return of keys and the reporting of stolen keys. NCI Cardkey Coordinators are responsible for the control and return of cardkeys and the reporting of lost/stolen cardkeys.

APPROVAL/DEMOTION

1	System Information
System Name:	NIH NCI Employee Database Internet Edition (EDie)

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	
Approval/Demotion Point of Contact:	Suzy Milliard
Date:	Jul 30, 2010

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 24, 2010

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

PIA % COMPLETE

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

16 Appendix F: Sample IT System PIA (without PII)

06.1 HHS Privacy Impact Assessment (Form) / NIH NCI Cancer Genetics Services Directory (CGSD) (Item)

Primavera
ProSight

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?	
Yes	
If this is an existing PIA, please provide a reason for revision:	
*1. Date of this Submission:	
May 16, 2011	
*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):	
N/A	
*5. OMB Information Collection Approval Number:	
In process	
*6. Other Identifying Number(s):	
N/A	

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

NIH NCI Cancer Genetics Services Directory (CGSD)

*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	Margaret Beckwith, Ph.D.

*10. Provide an overview of the system:

The National Cancer Institute Cancer Genetics Services Directory (CGSD) on the NCI's Website cancer.gov is a searchable collection of information about professionals who provide services related to cancer genetics. These services include cancer risk assessment, genetic counseling, and genetic susceptibility testing. The professionals have applied to be in the directory using an online application form and have met basic criteria outlined on the form. The CGSD is posting data such as investigator name, title, biography, and work contact information that is already publicly available on institutional websites and is not posting or collecting personally identifiable information.

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

New

*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.)

No

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.

No

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

No

*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)

No

*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):

No PII in the system.

*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:

1. There are currently 567 genetics professionals listed in the directory. Approximately 30-60 new professionals are added to the directory each year. The applicants are nurses, physicians, genetic counselors, and other professionals who provide services related to cancer genetics. The information collected on the application includes name, professional qualifications, practice locations, and area of specialization. The information is updated annually using a web-based update mailer that mirrors the application form.

2. The information contained in the NCI Cancer Genetics Services Directory is published on the cancer.gov public website. It is a unique resource for cancer patients and their families who are looking for information about their family's risk of cancer and genetic counseling. Collecting applicant information such as name, title, area of expertise, biography, work contact information and verifying it annually by using the NCI CGSD web-based application form and update mailer is important for providing this information to the public and keeping it current.

3. There is no PII in the system.

4. All professionals listed in the directory voluntarily submit applications to be included.

*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.]):

There is no PII in the system.

*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)

Not Applicable

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

There is no PII in the system.

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:

May 16, 2011

*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):

N/A

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

N/A

*5. OMB Information Collection Approval Number:

In process

5a. OMB Collection Approval Number Expiration Date:

*6. Other Identifying Number(s):

N/A

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

NIH NCI Cancer Genetics Services Directory (CGSD)

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

System Location:	
OPDIV or contractor office building	6116 Executive Blvd., Suite 300A
Room	Room 3094
City	Rockville
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	Margaret Beckwith, Ph.D.

The following information will not be made publicly available:

POC Title	Acting Branch Chief
POC Organization	NCI/OCE/OCCM
POC Phone	301-594-2718
POC Email	mbeckwit@mail.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)

The National Cancer Institute Cancer Genetics Services Directory (CGSD) on the NCI's Website cancer.gov is a searchable collection of information about professionals who provide services related to cancer genetics. These services include cancer risk assessment, genetic counseling, and genetic susceptibility testing. The professionals have applied to be in the directory using an online application form and have met basic criteria outlined on the form. The CGSD is posting data such as investigator name, title, biography, and work contact information that is already publicly available on institutional websites and is not posting or collecting personally identifiable information.

SYSTEM CHARACTERIZATION AND DATA CATEGORIZATION

1	System Characterization and Data Configuration

11. Does HHS own the system?

11a. If no, identify the system owner:

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

12a. 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:

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	
Anonymous to Non-Anonymous	
Significant System Management Changes	
Significant Merging	
New Public Access	
Commercial Sources	
New Interagency Uses	
Internal Flow or Collection	
Alteration in Character of Data	

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

Minor Application (child)

*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?

No

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)	
Date of Birth	
Social Security Number (SSN)	
Photographic Identifiers	
Driver’s License	
Biometric Identifiers	
Mother’s Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web Uniform Resource Locator(s) (URL)	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

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.

No

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	
Public Citizen	
Patients	
Business partners/contacts (federal, state, local agencies)	
Vendors/Suppliers/Contractors	
Other	

*19. Are records on the system retrieved by 1 or more PII 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 (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver’s License	
Biometric Identifiers	
Mother’s Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	

Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

20. Are 10 or more records containing PII maintained, stored or transmitted/passed through this system?

*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)

No

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?

Please indicate "Yes" or "No" for each category below:	**Yes/No**
Name (for purposes other than contacting federal employees)	
Date of Birth	
SSN	
Photographic Identifiers	
Driver's License	
Biometric Identifiers	

Mother’s Maiden Name	
Vehicle Identifiers	
Personal Mailing Address	
Personal Phone Numbers	
Medical Records Numbers	
Medical Notes	
Financial Account Information	
Certificates	
Legal Documents	
Device Identifiers	
Web URLs	
Personal Email Address	
Education Records	
Military Status	
Employment Status	
Foreign Activities	
Other	

*23. If the system shares or discloses PII please specify with whom and for what purpose(s):

No PII in the system.

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?

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)?

26. Are individuals notified how their PII is going to be used?

26a. 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?

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?

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?

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		
Administrators		
Developers		
Contractors		
Other		

*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:

1. There are currently 567 genetics professionals listed in the directory. Approximately 30-60 new professionals are added to the directory each year. The applicants are nurses, physicians, genetic counselors, and other professionals who provide services related to cancer genetics. The information collected on the application includes name, professional qualifications, practice locations, and area of specialization. The information is updated annually using a web-based update mailer that mirrors the application form.

2. The information contained in the NCI Cancer Genetics Services Directory is published on the cancer.gov public website. It is a unique resource for cancer patients and their families who are looking for information about their family's risk of cancer and genetic counseling. Collecting applicant information such as name, title, area of expertise, biography, work contact information and verifying it annually by using the NCI CGSD web-based application form and update mailer is important for providing this information to the public and keeping it current.

3. There is no PII in the system.

4. All professionals listed in the directory voluntarily submit applications to be included.

*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.])

There is no PII in the system.

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	www.cancer.gov/cancertopics/genetics/directory
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.).

No

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	Yes
Web Beacons	Yes
Session Cookies	Yes
Persistent Cookies	No
Other	N/A

*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?

N/A

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	

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

Not Applicable

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)?

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?

43. Is there a contingency (or backup) plan for the system?

44. Are files backed up regularly?

45. Are backup files stored offsite?

46. Are there user manuals for the system?

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?

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to privacy provisions and practices?

49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?

49a. 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):

Not Applicable

50a. 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?

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

Encryption	
Intrusion Detection System (IDS)	
Common Access Cards (CAC)	
Smart Cards	
Biometrics	
Public Key Infrastructure (PKI)	

52. Is there a process in place to monitor and respond to privacy and/or security incidents?

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

PHYSICAL ACCESS

1	Physical Access

53. Are physical access controls in place?

Please indicate "Yes" or "No" for each category below:	**Yes/No**
Guards	
Identification Badges	
Key Cards	
Cipher Locks	
Biometrics	
Closed Circuit TV (CCTV)	

*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:

There is no PII in the system.

APPROVAL/DEMOTION

1	System Information
System Name:	NIH NCI Cancer Genetics Services Directory (CGSD)

2	PIA Reviewer Approval/Promotion or Demotion

Promotion/Demotion:	Promote
Comments:	
Approval/Demotion Point of Contact:	Suzy Milliard
Date:	May 16, 2011

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:	

PIA % COMPLETE

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

17 Appendix G: Sample TPWA

Privacy Impact Assessment (PIA) FOR THIRD-PARTY WEBSITES OR APPLICATIONS

Overview

The PIA determines if Personally Identifiable Information (PII) is contained within a system, the kind of PII involved, what is done with that information, and how the PII is protected. OPDIV/STAFFDIV uses of third-party Websites or applications are subject to requirements based on privacy laws, regulations, and guidance. The Department of Health and Human Services (HHS) Privacy Act Officer may be contacted for issues related to the Freedom of Information Act (FOIA) and/or the Privacy Act. Respective HHS 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. This Privacy Impact Assessment is to be completed in accordance with Office of Management and Budget (OMB) Memorandum (M) 03-22 *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* and OMB M-10-23 *Guidance for Agency Use of Third-Party Websites and Applications*. For complete background and guidance, please read the *Standard Operating Procedures (SOPs) for the Privacy Impact Assessment for Third-Party Websites of Applications* prior to completing this PIA.

Questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to OMB and public posting in accordance with OMB M-03-22.

General Information

1. Is this a new PIA?

☒Yes
□No

1a. If this is a revision of an existing PIA, please provide a reason for revision:

2. Date of this Submission:

01/24/11

*3. OPDIV/STAFFDIV Name:

NIH/OD/OCPL/OLIB

*4. Unique Project Identifier (UPI) Number for current fiscal year (if applicable):

N/A

*5. Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

□Yes
☒No, the Website or application is not subject to the Privacy Act.

*5a. If yes, indicate the SORN number or describe the plans to put one in place.

*6. Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

☐Yes
☒No, the Website or application is not subject to the PRA.

*6a. If yes, indicate the OMB approval number and approval number expiration date or describe the plans to obtain OMB clearance.

7. Does the third-party Website or application contain Federal records?

☒Yes
☐No

*8. Third-Party Website or Application Name:

NIH Institutes of Health (NIH) on Facebook

*9. Point of Contact (POC). The POC is the person to whom questions about the responses to the third-party Website or application PIA may be addressed:

Name: Dennis Rodrigues
Title: Director, OIB/PIO/OCPL/OD
Location: Building 31, Room 5B58, Bethesda, MD 20892
Phone: (301) 435-2932

*10. Describe the specific purpose for the OPDIV/STAFFDIV use of the third-party Website or application.

Facebook is a social network service and website that is free to users and generates revenue from advertising. Visitors who want to subscribe to (or become a fan of, or "like") the NIH Facebook page, must create a Facebook account at http://www.facebook.com. To create an account, the user must provide personal information, such as name, photo (optional), user name, password and email address. Users may create a personal profile with photos, lists of personal interests, contact information, and other personal information. Additionally, users may create and join common interest user groups, organized by workplace, school, or college, or other characteristics and "like pages" (formerly called "fan pages"). Users can add other users as friends and communicate with them through private or public messages and a chat feature, including automatic notifications when they update their profile. Facebook enables users to choose their own privacy settings and choose who can see specific parts of their profile. Facebook requires a user's name and profile picture to be accessible by everyone. Users can control who sees other information they have shared, as well as who can find them in searches, through their privacy settings.

Facebook was used to create three *NIH.gov* pages in order to share information about NIH with visitors and respond to comments and inquiries sent via Facebook to NIH. They are: National Institutes of Health (NIH), Research Matters Weekly, and News in Health. Many other NIH Institutes and Centers (ICs) sponsor their own Facebook pages. The privacy policies for the other IC Facebook pages are located on the individual IC web sites.

On each of the *NIH.gov* Facebook pages, *NIH.gov* staff posts news and other items of interest to citizens. If individuals have a Facebook account, they can post comments to the NIH Facebook page, ask questions or click the "like" button to indicate they would like to link to the NIH Facebook page. If they comment or click on the "like" button, personally identifying information will be visible to NIH staff and other Facebook site visitors. The amount of visible personal information will depend on the Facebook privacy settings created by the individual user. They can completely avoid displaying any personally identifiable information by not creating an account, not posting comments and not clicking on the "like" options in Facebook. NIH staff do not collect, use or disclose any information about visitors who comment on or click that they "like" the NIH Facebook sites. This information is password protected and only available to *NIH.gov* managers, members of the *NIH.gov* Communications and Web Teams, and other designated staff who require this information to perform their duties. The Facebook privacy policy is available at: http://www.facebook.com/policy.php

Requirements

11. Have the third-party's privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV/STAFFDIV use?

☒Yes
☐No

12. Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application.

Visitors can visit http://www.nih.gov and select News/News Releases/News & Events/News Releases

13. Does the third-party Website or application have appropriate branding to distinguish the OPDIV/STAFFDIV's activities from those of nongovernmental actors?

☐Yes
☒No

14. How has the OPDIV/STAFFDIV implemented the use of the third-party Website or application?

☐External hyperlink from an HHS Website or Website operated on behalf of HHS
☐Incorporated or embedded on an HHS Website
☒Other

14a. If other, please describe how the tool was implemented.

Users must visit http://www.facebook.com to create an account. They can then use the search tool to navigate to the National Institutes of Health (NIH) Facebook page from the internet or a mobile phone.

14b. If the public navigates to the third-party Website or application via an external hyperlink, is there an alert to notify the public that they are being directed to a nongovernmental Website?

☐Yes
☒No

Notice Practices

15. Has the OPDIV/STAFFDIV Privacy Policy been updated to describe the use of a third-party Website or application?

☒Yes
☐No

15a. Provide a hyperlink to the OPDIV/STAFFDIV Privacy Policy:

http://www.nih.gov/about/privacy.htm

16. Is an OPDIV/STAFFDIV Privacy Notice posted on the third-party Website or application?

☐Yes
☒No

16a. Confirm that the OPDIV/STAFFDIV's Privacy Notice includes the following:

☒ An explanation that the Website or application is not government-owned or government-operated;
☒ An indication of whether and how the OPDIV/STAFFDIV will maintain, use, or share PII that becomes available;
☒ An explanation that the public's use of the Website or application to communicate with the OPDIV/STAFFDIV, that the public may be providing nongovernmental third-parties with access to PII;
☒ A link to the official OPDIV/STAFFDIV Website; and
☒ A link to the OPDIV/STAFFDIV Privacy Policy.

16b. Is the OPDIV/STAFFDIV's Privacy Notice prominently displayed at all locations on the third-party Website or application where the public might *make PII available*?

☐Yes
☒No

Information Collection & Use Practices

*17. Is PII collected by the OPDIV/STAFFDIV from the third-party Website or application?

☒Yes
☐No

*18. Will the third-party Website or application *make PII available* to the OPDIV/STAFFDIV*?*
☒Yes
☐No

*19. Describe the PII that will be collected or the PII which the public could likely *make available* through the OPDIV/STAFFDIV's use of the third-party Website or application and the OPDIV/STAFFDIV's intended or expected use of the PII. Upon creation of an account, the user must provide their name, user name, password and email address. In addition, they may provide a location, photo and other personal information. The type of PII made available is dependent upon the privacy settings established by the user. In most cases, it includes an individual's name, hometown, home address, age, work address, phone numbers, marital status, websites, groups, organizations and charitable causes with whom the user is affiliated, political affiliation, religious beliefs, as well as family photos and personal information about family members.

Information Sharing & Maintenance Practices

*20. Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing.

NIH staff never takes possession of the personal information belonging to Facebook users. NIH does not collect, maintain, disclose or share any information about people who follow NIH on Facebook. However, as part of its Moderator Comment policy, print screen shots of advertising, spam, inflammatory or improper comments made to the *NIH.gov* Facebook sites will be saved to a spreadsheet in a folder on a password-protected shared drive, along with the name of the Facebook user, image of the individual's profile picture, and date the comment was sent. These comments will be shared with management as needed and retained as long as the mission dictates, in accordance with the NIH records disposition schedule.

*20a. If PII is shared, how will the risks of sharing PII be mitigated?
Access controls are in place to limit the shared drive to those with a valid, business need to view the information.
*21. Will the PII from the third-party Website or application be maintained by the OPDIV/STAFFDIV?
☒Yes □No
*21a. If PII will be maintained, indicate how long the PII will be maintained.
For as long as the Internet is in operation, although as more Facebook comments are posted, the newer content forces the older content to be more hidden.
*22. Describe how PII that is used or maintained will be secured.
Access to the shared database is secure from unauthorized access.
*23. What other privacy risks exist and how will they be mitigated?
Protection of PII is totally dependent upon the privacy settings established by the account holder. Facebook is a social utility designed to connect people and friends and others who work, study and live around them. It is a system designed by a third party to be an interactive forum in which people share information, potentially, personally identifiable information. Facebook.com is a privacy risk. NIH does not pretend to have any control over its operation. NIH strongly suggests HHS negotiate with GSA to implore Facebook.com to, as part of its Terms of Service Agreement, customize its user account login registration screen to include stronger privacy language warning users of potential privacy and security risks and to appropriately brand the website/application to distinguish it from those of governmental actors. Facebook should include a link incorporated or embedded on its website that informs users it is not operated on behalf of the Federal agency with which it has negotiated a TOS agreement.

18 Appendix H: References

1. Privacy Act of 1974, (5 U.S.C. 552a, as amended) (Public Law 93-579) (December 31, 1974): http://www.justice.gov/opcl/privstat.htm

2. Paperwork Reduction Act (PRA) of 1995, (44 U.S.C. 3501) (Public Law 104-13) (May 22, 1995): http://www.cio.gov/documents/paperwork_reduction_act_1995.html

3. Clinger-Cohen Act of 1996, (40 U.S.C. Section 1401) (Public Law 104-106) (February 10, 1996) (also known as the Information Technology Management Reform Act): http://www.cio.gov/Documents/it_management_reform_act_feb_1996.html

4. Computer Matching and Privacy Protection Act of 1988, (5 U.S.C. 552a(o)) (Public Law 100-53) (October 18, 1988): http://www.whitehouse.gov/omb/inforeg/final_guidance_pl100-503.pdf

5. Computer Security Act of 1987, (15 U.S.C. Chapter 7, 40 U.S.C. Section 1441) (Public Law 100-235) (January 8, 1988): http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf

6. E-Government Act of 2002 (E-GOV) Section 208, (44 U.S.C. Chapter 36) (Public Law 107-347 Title II) (December 17, 2002): http://www.mda.mil/global/documents/pdf/egov_act2002.pdf

7. Federal Information Security Management Act (FISMA) of 2002, (44 U.S.C. Chapter 35) (Public Law 107-347, Title III) (December 17, 2002): http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Federal Regulations:

Code of Federal Regulations (CFR):

1. 45 CFR, Part 5b, HHS Privacy Act Regulations: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=d8c05a9cf0b3dd219f61ecf068cb7260&rgn=div5&view=text&node=45:1.0.1.1.7&idno=45

National Institute of Standards and Technology (NIST) References:

1. Guide to NIST Information Security Documents: http://csrc.nist.gov/publications/CSD_DocsGuide.pdf

2. NIST Special Publications (SP), Complete list of NIST Publications: http://csrc.nist.gov/publications/PubsSPs.html

3. NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems and Organizations (August 2009): http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

4. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010): http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Office of Management and Budget Guidance:

OMB Circulars:

1. Office of Management and Budget Circular A-11, Section 53, Information Technology and E-Government: http://www.whitehouse.gov/omb/circulars/a11/current_year/s53.pdf

2. OMB Circular A-130, Management of Federal Information Resources (November 28, 2000): http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

OMB Memoranda:

Calendar Year 2011

1. M-11-02, Sharing Data While Protecting Privacy (November 3, 2010): http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-02.pdf

Calendar Year 2010

1. M-10-23, Guidance for Agency Use of Third-Party Websites and Applications (June 25, 2010): http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

2. M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies (June 25, 2010): http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf

3. M-10-15, FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (April 21, 2010): http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

4. M-10-06, Open Government Directive (December 8, 2009): http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

Calendar Year 2007

1. M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf

Calendar Year 2006

1. M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-19.pdf

2. M-06-16, Protection of Sensitive Agency Information (June 23, 2006): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-16.pdf

3. M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m-06-15.pdf

Calendar Year 2005

1. M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf

Calendar Year 2003

1. M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003): http://www.whitehouse.gov/omb/memoranda_m03-22/

HHS Privacy Policy and Guidance:

1. HHS General Administration Manual, Chapter 45-10, Privacy Act – Basic Requirements and Relationships: http://www.hhs.gov/hhsmanuals/gam/chapters/45-10.pdf

2. HHS General Administration Manual, Chapter 45-13, Safeguarding Records Contained in Systems of Records: http://www.hhs.gov/hhsmanuals/gam/chapters/45-13.pdf

3. HHS Privacy Impact Assessment (PIA) Standard Operating Procedures: http://oma.od.nih.gov/ms/privacy/Privacy_Impact_Assessment_SOP_Final_02102009.doc

4. HHS-OCIO Policy for Information Systems Security and Privacy (IS2P): http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/PISSP/pol_for_info_sys_sec_and_priv_hndbk_20110707.pdf

5. HHS-OCIO Policy for Information Systems Security and Privacy (IS2P) Handbook: http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/PISSP/pol_for_info_sys_sec_and_priv_hndbk_20110707.pdf

6. HHS-OCIO Policy for Privacy Impact Assessment (PIA): http://www.hhs.gov/ocio/policy/20090002.001.html

7. Privacy in the System Development Lifecycle (SDLC): http://intranet.hhs.gov/it/docs/privacy/PSDLC/Privacy_in_SDLC.html

NIH Policy, Provisions & Guidelines:

1. NIH Manual Chapter 1745, NIH Information Technology (IT) Privacy Program: http://www3.od.nih.gov/oma/manualchapters/management/1745/

2. NIH Manual Chapter 1825, Information Collection from the Public: http://www1.od.nih.gov/oma/manualchapters/management/1825

3. NIH Manual Chapter 2804, NIH Public-Facing Web Management Policy:

4. NIH Manual Chapter 2805, NIH Web Privacy Policy: http://www3.od.nih.gov/oma/manualchapters/management/2805/

5. NIH Manual Chapter 2809, NIH Social and New Media Policy:

19 Appendix I: Acronyms

ASPR	Assistant Secretary for Preparedness and Response
CAC	Common Access Cards
CC	Clinical Center
CCTV	Closed Circuit TV
CIT	Center for Information Technology
COPPA	Children’s Online Privacy Protection Act
C&A	Certification and Accreditation
DATOS	Drug Abuse Treatment Outcome Study
FAR	Federal Acquisition Regulation
FIC	Fogarty International Center
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act
GSS	General support system
HEAR	HHS Enterprise Architecture Repository
HHS	Health and Human Services
IC	Institutes and Centers
ICR	Information Collection Request
IDS	Intrusion Detection System
IG	Inspector General
IMPAC	Information for Management Planning Analysis and Coordination
ISAO	Information Security Awareness Office
ISSO	Information Systems Security Officer
IT	Information Technology
M	Memorandum
MA	Major application
MC	Manual Chapter
NBA	National Business Center
NCAT	NIH Certification and Accreditation Tool
NCI	National Cancer Institute
NEAR	NIH Enterprise Architecture Repository
NHLBI	National Heart Lung Blood Institute
NIAAA	National Institute on Alcohol Abuse and Alcoholism
NIAID	National Institute of Allergy and Infectious Diseases
NIDA	National Institute on Drug Abuse
NIDDK	National Institute of Diabetes and Digestive

	and Kidney Diseases
NIGMS	National Institute of General Medical Sciences
NIH	National Institutes of Health
OA	Office of Assessment
OCID	Office of Credentialing Issuance Station System
OCIO	Office of the Chief Information Officer
OD	Office of the Director
OE	Office of Ethics
OER	Office of Extramural Research
OHRM	Office of Human Resource Management
OIR	Office of Intramural Research
OM	Office of Management
OMA	Office of Management Assessment
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPDIV	Operating Division
ORS	Office of Research Services
OS	Office of the Secretary
OSOP	Office of the Senior Official for Privacy
PIA	Privacy impact assessment
PII	Personally identifiable information
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of contact
PRA	Paperwork Reduction Act
P3P	Platform for Privacy Preferences
RSS	Really Simple Syndication
SAOP	Senior Agency Official for Privacy
SSN	Social Security Number
SSP	System Security Plan
SOP	Senior Official for Privacy
SORN	System of records notice
SPORT	Security and Privacy Online Reporting Tool
TPWA	Third-Party Website and Application
UPI	Unique Project Identifier
USRDS	United States Renal Data System
VPN	Virtual Private Network