06.1 HHS Privacy Impact Assessment (Form) / NIH NCI DCP Cancer Prevention Fellowship Program Application System (Item)

Primavera ProSight

Form Report, printed by: Hayn, Craig, **Mar 28, 2013**

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:*

Feb 4, 2013

**2. OPDIV Name:*

NIH

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

09-25-0158

**5. OMB Information Collection Approval Number:*

N/A

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

N/A

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

NIH NCI Division of Cancer Prevention (DCP) Cancer Prevention Fellowship Program (CPFP) Application System

**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	Nicole Hollis

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

The CPFP Application System is a web-based application designed to allow people to apply to the Fellowship Program and to the NCI Summer Curriculum in Cancer Prevention. The Application System also provides tools to the NCI Cancer Prevention Fellowship Program and the NCI Center for Global Health (CGH) so they may process applications and evaluate the applicant pool.

The Fellowship Program application requires an applicant to provide contact information, citizenship, education/transcripts, a personal statement of research goals, a curriculum vitae, and an indication of how they heard about the CPFP. Additionally, the applicant must request letters of reference and possibly other supporting documentation through the application website. Requests are fulfilled when designated individuals upload the requested supporting documentation. Members of the Scientific Education Committee (SEC) review applications to aid in the selection of fellows. The SEC consists of scientists from within and outside the NCI with expertise in the field of cancer prevention and control. With input from the SEC, the CPFP selects candidates to interview and offers fellowship positions to the most highly qualified candidates.

The Summer Curriculum application requires an applicant to provide contact information, a curriculum vitae, a letter of nomination (and possibly additional supporting documentation), and indicate course requests. CPFP staff primarily evaluates domestic candidates and

CGH staff evaluates international candidates and approves/rejects course requests.

The CPFP Application System limits user access by username and password. Within the system, users have varying levels of restriction to edit, submit, review, and evaluate applications.

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

Existing

**17. Does/Will the system collect, maintain (store), disseminate and/or pass through PII within any database(s), record(s), file(s) or website(s) hosted by this system?*

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

Yes

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

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):*

the system discloses PII internally to CPFP staff in order to evaluate applicant qualifications; Individuals who have been asked to provide supporting documentation have access to PII to identify the applicant for whom they are being asked to provide documentation; SEC members have access to PII for randomly selected group of applications to evaluate applicant quals for the program. CGH Staff has access to PII from international applications for evaluation and to process visas.

**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. The agency collects a variety of PII from prospective fellowship applicants and is from non-federal staff. See number 2 below.

2. Information is used as follows: Contact information is necessary to contact the applicant about the status of their application. Demographic information is used to construct a summary overview of the composition of the applicant pool. Applicants may provide gender and race voluntarily.
Citizenship documentation is used by CPFP staff to validate that the applicant is authorized to work in the U.S. Education and transcripts are used by CPFP staff and SEC reviewers to evaluate current and past academic performance. Basic contact information (name, e-mail, city/state/country of current residence) and degrees are used by contributors to identify applicants who request supporting documentation from them. Personal Statement of Research Goals, Curriculum Vitae, and Supporting Documentation are reviewed by CPFP staff and SEC reviewers to evaluate applicant qualifications. Social Security Numbers are collected only for applicants selected for interviews and are used by CPFP staff to make travel arrangements. Personal photographs are collected only for applicants selected for interviews and are used by CPFP staff and SEC members to identify interviewees during and following interviews.

3. There is PII in the system.

4. Applying to the Cancer Prevention Fellowship Program is voluntary, but in order for the application to be processed, much of the information is required before the application may be submitted.

**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.]):*

An application-specific privacy statement is available from all application pages. It notifies individuals that the primary use of collected information is to "evaluate an applicant's qualifications for postdoctoral training at the National Cancer Institute's Cancer Prevention Fellowship Program and to process the application." Additionally, the Privacy Statement indicates the following routine uses for information disclosure:

In rare circumstances, information may be used to respond to congressional inquiries regarding constituents who have applied to the Cancer Prevention Fellowship Program.

Information may be used to respond to hospitals and other healthcare organizations seeking verification of training for physicians and other scientists who enroll in the Cancer Prevention Fellowship Program. Some requested information will be used for internal program evaluation -- to improve the program and the application process -- and will not be used in the evaluation of the applicant. Information that will not be used in applicant evaluation is indicated in the online application.

Information that is used for internal program evaluation is provided only in aggregate form.

Furthermore, the Privacy Statement indicates that "application for this program is voluntary; however, for us to process your application, you must complete the required fields." By providing the information, the applicant is giving consent for the information to be used as stated on the website.

**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:*

The IMS computer center consists of two co-location facilities. One is located in Baltimore MD and the other is located 60 miles away in Sterling VA. Both of these facilities are SAS-70 type II certified facilities which provide 24x7 security and monitoring for physical entry and environmental hazards. The internal IMS network is protected at all entry points by firewalls and intrusion detection devices.

IMS has Standard Operating Procedures (SOPs) governing the storage and transmission of all data types including PII. Transmission of data outside of the data center is secured using standard SSL or HTTPS based protocols. IMS has developed a data transfer facility utilizing the HTTPS protocol that allows for secure transfer data between the client and IMS. The storage of data that is deemed sensitive must be commensurate with the level of Confidentiality, Availability and Integrity required as specified in a PIA or other assessment document. Physical controls such as user/group authorization, encryption of data at rest, and weekly security/virus scans are employed in the data center to ensure continued data security while at IMS. All IMS employees are required to read, agree to, and sign a confidentiality agreement at the time of employment. They must also complete yearly security trainings. Additionally, employees that act as gate keepers to the data center such as network and database administrators are required to have security clearances while performing their job.

IMS continually monitors all of its systems for anomalies which could indicate a security breach or other issue with the systems. SOPs and a disaster recovery plan are in place that detail actions system administrators and other responsible parties must take in the event of a security incident, unplanned downtime or disaster. Also, IMS does weekly system scans with a vulnerability scanner to ensure all systems are patched to an acceptable level.

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:*

Feb 4, 2013

**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):

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

09-25-0158

**5. OMB Information Collection Approval Number:*

N/A

5a. OMB Collection Approval Number Expiration Date:

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

N/A

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

NIH NCI Division of Cancer Prevention (DCP) Cancer Prevention Fellowship Program (CPFP) Application System

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

System Location:	
OPDIV or contractor office building	Information Management Services, Inc.
Room	c/o Qwest CyberCenter/Baltimore Technology Park
City	Sterling and Baltimore
State	VA and MD, respectively

**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	Nicole Hollis

The following information will not be made publicly available:

POC Title	Program Specialist
POC Organization	NCI Cancer Prevention Fellowship Program
POC Phone	301-435-2757
POC Email	hollisn@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 CPFP Application System is a web-based application designed to allow people to apply to the Fellowship Program and to the NCI Summer Curriculum in Cancer Prevention. The Application System also provides tools to the NCI Cancer Prevention Fellowship Program and the NCI Center for Global Health (CGH) so they may process applications and evaluate the applicant pool.

The Fellowship Program application requires an applicant to provide contact information, citizenship, education/transcripts, a personal statement of research goals, a curriculum vitae, and an indication of how they heard about the CPFP. Additionally, the applicant must request letters of reference and possibly other supporting documentation through the application website. Requests are fulfilled when designated individuals upload the requested supporting documentation. Members of the Scientific Education Committee (SEC) review applications to aid in the selection of fellows. The SEC consists of scientists from within and outside the NCI with expertise in the field of cancer prevention and control. With input from the SEC, the CPFP selects candidates to interview and offers fellowship positions to the most highly qualified candidates.

The Summer Curriculum application requires an applicant to provide contact information, a curriculum vitae, a letter of nomination (and possibly additional supporting documentation), and indicate course requests. CPFP staff primarily evaluates domestic candidates and CGH staff evaluates international candidates and approves/rejects course requests.

The CPFP Application System limits user access by username and password. Within the system, users have varying levels of restriction to edit, submit, review, and evaluate applications.

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:

N/A

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

No

12a. If no, identify the system operator:

Information Management Services, Inc. (IMS)

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

Existing

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

Operations/Maintenance

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

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 (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?*

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	Yes
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	Yes
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Gender, Race, Birth Place, Citizenship Document (I-551 Visa Stamp), Unofficial Transcripts, CV.

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

**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	

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.

N/A

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

22. Does the system share or disclose PII with other divisions within this agency, external agencies, or other people or organizations outside the agency?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No
SSN	No
Photographic Identifiers	Yes
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 URLs	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Unofficial Transcripts, Personal Statement of Research Goals, Curriculum Vitae

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

the system discloses PII internally to CPFP staff in order to evaluate applicant qualifications; Individuals who have been asked to provide supporting documentation have access to PII to identify the applicant for whom they are being asked to provide documentation; SEC members have access to PII for randomly selected group of applications to evaluate applicant quals for the program. CGH Staff has access to PII from international applications for evaluation and to process visas.

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)?

Yes

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

Yes

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

A link to the Privacy Statement exists on each web page. The Privacy Statement indicates that "application for this program is voluntary; however, for us to process your application, you must complete the required fields." For non-required PII, an explanation is provided in the application that indicates that the PII will be provided to reviewers only when summarizing the entire group of applicants.

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?

Yes

27a. If yes, please describe briefly the notification process. If no, please provide an explanation.

Detailed in SOR. In addition, there is a "Contact Us" feature on the website that can be used.

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.

Automated audit trails are monitored on all server-based systems deployed at IMS. All of the UNIX/Linux workstations and the Windows systems have the ability to track resources as small as a single file. File usage logging will be done for files specified by the HHS organization. Audit records and server logs will be reviewed daily for anomalies. Windows servers log user access and resource usage. An automated reporting tool will be used to analyze the server logs to look for abnormal activity. Automated audit trails also play an important part in governing the access granted to users outside the Contractor's Local Area Network (LAN). A firewall is in place that logs all incoming and outgoing connections to the LAN. This includes connections to the UNIX/Linux workstations and the Windows servers. This log will be maintain and checked for evidence of attempted unauthorized access to the Contractor's LAN.

Computer center staff performs weekly security checks of the computer center resources using a vulnerability scanner.

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	Part of their job function
Administrators	Yes	Part of their job function
Developers	Yes	On an as-needed basis to perform their job function
Contractors	Yes	On an as-needed basis to perform their job function
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. The agency collects a variety of PII from prospective fellowship applicants and is from non-federal staff. See number 2 below.

2. Information is used as follows: Contact information is necessary to contact the applicant about the status of their application. Demographic information is used to construct a summary overview of the composition of the applicant pool. Applicants may provide gender and race voluntarily.
Citizenship documentation is used by CPFP staff to validate that the applicant is authorized to work in the U.S. Education and transcripts are used by CPFP staff and SEC reviewers to evaluate current and past academic performance. Basic contact information (name, e-mail, city/state/country of current residence) and degrees are used by contributors to identify applicants who request supporting documentation from them. Personal Statement of Research Goals, Curriculum Vitae, and Supporting Documentation are reviewed by CPFP staff and SEC reviewers to evaluate applicant qualifications. Social Security Numbers are collected only for applicants selected for interviews and are used by CPFP staff to make travel arrangements. Personal photographs are collected only for applicants selected for interviews and are used by CPFP staff and SEC members to identify interviewees during and following interviews.

3. There is PII in the system.

4. Applying to the Cancer Prevention Fellowship Program is voluntary, but in order for the application to be processed, much of the information is required before the application may be submitted.

**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.])*

An application-specific privacy statement is available from all application pages. It notifies individuals that the primary use of collected information is to "evaluate an applicant's qualifications for postdoctoral training at the National Cancer Institute's Cancer Prevention Fellowship Program and to process the application." Additionally, the Privacy Statement indicates the following routine uses for information disclosure:

In rare circumstances, information may be used to respond to congressional inquiries regarding constituents who have applied to the Cancer Prevention Fellowship Program.

Information may be used to respond to hospitals and other healthcare organizations seeking verification of training for physicians and other scientists who enroll in the Cancer Prevention Fellowship Program. Some requested information will be used for internal program evaluation -- to improve the program and the application process -- and will not be used in the evaluation of the applicant. Information that will not be used in applicant evaluation is indicated in the online application.

Information that is used for internal program evaluation is provided only in aggregate form.

Furthermore, the Privacy Statement indicates that "application for this program is voluntary; however, for us to process your application, you must complete the required fields." By providing the information, the applicant is giving consent for the information to be used as stated on the website.

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	https://cpfp.cancer.gov
Intranet	No	
Both	No	

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

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

Yes

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

Yes

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

Yes

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

N/A

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	

**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?

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
SSN	Yes
Photographic Identifiers	Yes
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	Yes
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	Yes
Military Status	No
Employment Status	Yes
Foreign Activities	No
Other	Gender, Race, Birth Place, Citizenship Document (I-551 Visa Stamp), Unofficial Transcripts, Personal Statement of Research Goals, Curriculum Vitae

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

Yes

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

Yes

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.

A disclaimer notice is present for users that follow links external to HHS.

ADMINISTRATIVE CONTROLS

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:

Feb 19, 2009

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

Not Applicable

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):

Roles, rights, and log in credentials are used.

**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 and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1 - "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 4000-E-3. Refer to the NIH Manual Chapter for specific disposition instructions.

TECHNICAL CONTROLS

1 Technical Controls

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?

Yes

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

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:

System Monitoring
Automated audit trails are monitored on all server-based systems deployed at IMS. All of the UNIX/Linux workstations and the Windows systems have the ability to track resources as small as a single file. File usage logging will be done for files specified by the HHS organization. Audit records and server logs will be reviewed daily for anomalies. Windows servers log user access and resource usage. An automated reporting tool will be used to analyze the server logs to look for abnormal activity. Automated audit trails also play an important part in governing the access granted to users outside the Contractor's Local Area Network (LAN). A firewall is in place that logs all incoming and outgoing connections to the LAN. This includes connections to the UNIX/Linux workstations and the Windows servers. This log will be maintain and checked for evidence of attempted unauthorized access to the Contractor's LAN.

Information Breach Policy
Procedures are in place to ensure the safety and integrity of all data and programs within IMS' control. These procedures include virus prevention, hardware and software configuration management, disaster recovery, and incident response.

The SOP for Computer Virus Prevention details steps both administrators and users must take to prevent viruses within the company. It details the responsibilities of the network administrators with regard to virus definition management and server virus scanning. It also outlines the steps users should take to prevent viruses on their own computers.

IMS network administrators follow a Configuration Management Plan for Computer Resources to ensure that all computers are maintained in a similar manner. The plan details the responsibilities for patch management; backup, restore and archiving; and computer retirement. If a disaster causes computer resources to be unavailable, the Disaster Recovery Plan will be followed to guide the recovery effort.

In the event of a computer break-in, network intrusion, or data theft, the SOP for Network/Computer Incident Response establishes procedures to follow. Decisions will be made regarding the level of response required and the appropriate actions necessary to preserve evidence of the intrusion while restoring service to the affected entities.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Yes

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

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

The IMS computer center consists of two co-location facilities. One is located in Baltimore MD and the other is located 60 miles away in Sterling VA. Both of these facilities are SAS-70 type II certified facilities which provide 24x7 security and monitoring for physical entry and environmental hazards. The internal IMS network is protected at all entry points by firewalls and intrusion detection devices.

IMS has Standard Operating Procedures (SOPs) governing the storage and transmission of all data types including PII. Transmission of data outside of the data center is secured using standard SSL or HTTPS based protocols. IMS has developed a data transfer facility utilizing the HTTPS protocol that allows for secure transfer data between the client and IMS. The storage of data that is deemed sensitive must be commensurate with the level of Confidentiality, Availability and Integrity required as specified in a PIA or other assessment document. Physical controls such as user/group authorization, encryption of data at rest, and weekly security/virus scans are employed in the data center to ensure continued data security while at IMS. All IMS employees are required to read, agree to, and sign a confidentiality agreement at the time of employment. They must also complete yearly security trainings. Additionally, employees that act as gate keepers to the data center such as network and database administrators are required to have security clearances while performing their job.

IMS continually monitors all of its systems for anomalies which could indicate a security breach or other issue with the systems. SOPs and a disaster recovery plan are in place that detail actions system administrators and other responsible parties must take in the event of a security incident, unplanned downtime or disaster. Also, IMS does weekly system scans with a vulnerability scanner to ensure all systems are patched to an acceptable level.

APPROVAL/DEMOTION

1 System Information

System Name:	NIH NCI Division of Cancer Prevention (DCP) Cancer Prevention Fellowship Program (CPFP) Application System

2 PIA Reviewer Approval/Promotion or Demotion

Promotion/Demotion:	Promote
Comments:	
Approval/Demotion Point of Contact:	Suzy Milliard
Date:	Feb 4, 2013

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:	Feb 22, 2013

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

PIA Completion	
PIA Percentage Complete:	100.00
PIA Missing Fields:	