

06.1 HHS Privacy Impact Assessment (Form) / NIH CC Rehabilitation-Social Security Administration Data Sharing System (Item)

Primavera
ProSight

Form Report, printed by: Martin, Susan, **Aug 29, 2012**

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 23, 2012

*2. OPDIV Name:

NIH

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

09-25-0200

*5. OMB Information Collection Approval Number:

Not Applicable

*6. Other Identifying Number(s):

None

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

CC: Rehabilitation Medicine Dept - Social Security Administration Data Sharing 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	Sue Martin

*10. Provide an overview of the system:

The Clinical Center Rehabilitation Medicine Department (CC-RMD) at the National Institutes of Health (NIH) has agreed to assist the Social Security Administration (SSA) to explore innovative methods for augmenting and improving the current disability evaluation process. The first major line of work requires analysis of data from longitudinal research files maintained by the Social Security Administration and assessing the feasibility of developing Computer Adaptive Testing (CAT) instruments that can be integrated into the SSA data collection and determination processes.

*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
<i>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.</i>
No
<i>*19. Are records on the system retrieved by 1 or more PII data elements?</i>
Yes
<i>*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)</i>
Yes
<i>*23. If the system shares or discloses PII, please specify with whom and for what purpose(s):</i>
The research data set is only shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information.
<i>*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:</i>
Analysis of data from longitudinal research files maintained by the Social Security Administration Office of Disability Program Information and Studies (ODPIS). These files house extensive administrative data, including application data and decisional data. Each record represents one disability claim. Past efforts to improve the quality and utility of the files were challenged by resource constraints. Users of the data files will need to creatively problem-solve and formulate solutions to data-related issues as they arise. The data includes limited personal identifiers including a pseudo social security number, medical notes, and birth month and year. Data is submitted as part of an application for a disability determination. The submission of data by applicants is required as part of the process when applying for benefits. Sharing of the data with the RMD is entirely voluntary on the part of the SSA.
<i>*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.]):</i>
All individuals are notified of use at the time of disability filing and consent is written and maintained by SSA. Major changes will be communicated by the CC CIO to the SSA Project Director. A limited data set, aka, research data is shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information. In the event a change to the CC system would include a new use or disclosure, the SSA Project Director would make a determination to notify individuals whose data is contained in the CC system.
<i>*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)</i>
No
<i>*37. Does the website have any information or pages directed at children under the age of thirteen?</i>
Not Applicable
<i>*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)</i>
Yes
<i>*54. Briefly describe in detail how the PII will be secured on the system using administrative, technical, and physical controls:</i>
A limited data set, aka, research data is shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information. Access is password protected and role based security is also used. All data resides on a server and SAN solely dedicated to that purpose and is located within the secure CC Data Center which uses state of the art backup and physical security measures. Individual files include a scrambled social security number (aka pseudo SSN). The key to unscramble the pseudo SSN is stored at the SSA to ensure protection of sensitive PII.

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 23, 2012

*2. OPDIV Name:

NIH

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

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

09-25-0200

*5. OMB Information Collection Approval Number:

Not Applicable

5a. OMB Collection Approval Number Expiration Date:

*6. Other Identifying Number(s):

None

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

CC: Rehabilitation Medicine Dept - Social Security Administration Data Sharing System

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

System Location:	
OPDIV or contractor office building	NIH:CC:DCRI Bldg 10-CRC
Room	Room B25750
City	Bethesda
State	Maryland

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

Point of Contact Information	
POC Name	Sue Martin

The following information will not be made publicly available:

POC Title	CC Privacy Officer
POC Organization	NIH/CC/Department of Clinical Research Informatics
POC Phone	(301) 496-4240
POC Email	smartin@cc.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 Clinical Center Rehabilitation Medicine Department (CC-RMD) at the National Institutes of Health (NIH) has agreed to assist the Social Security Administration (SSA) to explore innovative methods for augmenting and improving the current disability evaluation process. The first major line of work requires analysis of data from longitudinal research files maintained by the Social Security Administration and assessing the feasibility of developing Computer Adaptive Testing (CAT) instruments that can be integrated into the SSA data collection and determination processes.

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:

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)?

Major Application

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

Yes

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)	No
Date of Birth	No
Social Security Number (SSN)	No
Photographic Identifiers	No

Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	Yes
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	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Birth Month and Year, Death Month and Year, pseudo SSN

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	No

*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)	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	Yes
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	Birth Month and Year, Death Month and Year

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

Yes

*21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)

Yes

21a. If yes but a SORN has not been created, please provide an explanation.

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

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

Yes

Please indicate “Yes” or “No” for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	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	Yes
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	Birth Month and Year, Death Month and Year

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

The research data set is only shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information.

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?

Yes

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

Individuals are notified at the time a disability claim is filed with the Social Security Administration that data provided in their claim will be reviewed for more effective management of the program.

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?

Not Applicable

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

Not Applicable

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.

All data files are subjected to a thorough review by CC personnel before loading onto dedicated servers. Periodic reviews are also completed to compare working data with that created by sophisticated SAS analysis. Original data is never removed from the dedicated server and SAN.

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	Perform statistical analyses
Administrators	Yes	Data loading and systems administration
Developers	No	
Contractors	Yes	Perform statistical analyses
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:

Analysis of data from longitudinal research files maintained by the Social Security Administration Office of Disability Program Information and Studies (ODPIS). These files house extensive administrative data, including application data and decisional data. Each record represents one disability claim. Past efforts to improve the quality and utility of the files were challenged by resource constraints. Users of the data files will need to creatively problem-solve and formulate solutions to data-related issues as they arise. The data includes limited personal identifiers including a pseudo social security number, medical notes, and birth month and year. Data is submitted as part of an application for a disability determination. The submission of data by applicants is required as part of the process when applying for benefits. Sharing of the data with the RMD is entirely voluntary on the part of the SSA.

*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.]

All individuals are notified of use at the time of disability filing and consent is written and maintained by SSA. Major changes will be communicated by the CC CIO to the SSA Project Director. A limited data set, aka, research data is shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information. In the event a change to the CC system would include a new use or disclosure, the SSA Project Director would make a determination to notify individuals whose data is contained in the CC 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)

No

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	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?

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?

Not Applicable

Please indicate "Yes", "No", or "N/A" for each type of cookie below:	Yes/No/N/A
Web Bugs	Not Applicable
Web Beacons	Not Applicable
Session Cookies	Not Applicable
Persistent Cookies	Not Applicable
Other	Not Applicable

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

Not Applicable

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?

Not Applicable

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?

Not Applicable

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)?

No

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

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?

No

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

No

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

No

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):

Each contractor agrees to maintain confidentiality of all data and is granted access solely on a need to know basis. They are also required to take Computer Security & Privacy Awareness Training. Their access is restricted by role and is monitored.

*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:

All data provided by the SSA is required to be returned to them upon request for disposal as per requirements under the Privacy Act.

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)	No
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:

The CC Data Center Manager provides immediate notification as per NIH SOP to CC CIO, CIT and CC Privacy Officer. Also conducts investigation and provides report of specific circumstances and resolution.

PHYSICAL ACCESS

1 Physical Access

53. Are physical access controls in place?

Yes

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

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

A limited data set, aka, research data is shared between the SSA and the specific RMD staff authorized to perform statistical and other related analyses of the information. Access is password protected and role based security is also used. All data resides on a server and SAN solely dedicated to that purpose and is located within the secure CC Data Center which uses state of the art backup and physical security measures. Individual files include a scrambled social security number (aka pseudo SSN). The key to unscramble the pseudo SSN is stored at the SSA to ensure protection of sensitive PII.

APPROVAL/DEMOTION

1 System Information

System Name: CC: Rehabilitation Medicine Dept - Social Security Administration Data Sharing System

2 PIA Reviewer Approval/Promotion or Demotion

Promotion/Demotion: Promote

Comments: Review conducted with Diane Brandt, RMD Protocol Manager on July 23, 2012. Response to question 1 was modified. Data transfer from SSA to RMD was a one-time manual transfer via encrypted hard drive. Annual reports include aggregated data sent to SSA via SFTP. It is followed by submission of a hard copy of the report and a copy on CD shipped to SSA via FedEx.

Approval/Demotion Point of Contact: Sue Martin , CC Privacy Officer

Date: Jul 23, 2012

3 Senior Official for Privacy Approval/Promotion or Demotion

Promotion/Demotion: Promote

Comments:

4 OPDIV Senior Official for Privacy or Designee Approval

Please print the PIA and obtain the endorsement of the reviewing official below. Once the signature has been collected, retain a hard copy for the OPDIV's records. Submitting the PIA will indicate the reviewing official has endorsed it

This PIA has been reviewed and endorsed by the OPDIV Senior Official for Privacy or Designee (Name and Date):

Name: _____ **Date:** _____

Name:	Karen Plá
Date:	Sep 14, 2011

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:	
----------------------------	--