Attachment 7

PATH Study Privacy Impact Assessments (PIA)

June 26, 2014

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:*

07/01/2012

**2. OPDIV Name:*

National Institute on Drug Abuse (NIDA)

**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:*

TBD

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

8954

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

PATH IMS – Ancillary Support Systems

**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	
Dr. Kevin Paul Conway NSC BG RM 5185 6001 EXECUTIVE BLVD ROCKVILLE MD 20852 (301) 402-1817 kevin.conway@nih.gov	

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

The PATH IMS includes several ancillary support applications that do not collect, store, or display any personally identifiable information (PII). The systems that will not contain personally identifiable information are a public information website, a SharePoint collaboration site, a tobacco product image repository using the Alchemy image management application, a SAS® collaboration environment, a biospecimen tracking tool called BEST, a technical support issue tracking tools called BMC Remedy Magic, a Learning Management System hosted by ComplianceWire, an anonymous incentive payment management application hosted by Payoneer, and an inventory tracking application called ITMS. The public website will be used to convey information about the study to the public. The SharePoint site will be used for the partners in the study to collaborate and share ideas about the research. Alchemy is an image management

system that will store images of tobacco products and ads. The SAS Collaboration Environment is an environment in which research partners can access restricted use files that have had all personally identifiable information redacted. BEST tracks the shipping and receipt of biospecimens collected from participants, but does not store any participant data, only sample ID's which cannot be linked to participants by an external party. The Remedy Magic technical support tool tracks system problem reports, but identifies staff only by their business contact information, thus falling into the "federal contact data" category. The ComplianceWire application tracks training and certification of staff, and also holds only federal contact information. The Payoneer application supports the payment of incentives to study participants anonymously (participants are known to the application only by their debit card account number, not by any PII). ITMS is an inventory management application that is used to track the consumption of forms and other supplies. ITMS carries no data about participants or staff. *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*
**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?*
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).
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.
Yes
**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):*
N/A
**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:*
N/A
**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.]):*
N/A
**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:*
N/A

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:*

7/1/2012

**2. OPDIV Name:*

National Institute on Drug Abuse (NIDA)

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

TBD

**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:*

TBD

5a. OMB Collection Approval Number Expiration Date:

TBD

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

Westat internal project ID 8954

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

PATH Ancillary Support Systems

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

System Location:	
OPDIV or contractor office building	Westat Inc. 1600 Research Blvd.
Room	

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	Dr. Kevin Paul Conway

The following information will not be made publicly available:

POC Title	
POC Organization	National Institute on Drug Abuse
POC Phone	(301) 402-1817
POC Email	Kevin.conway@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 PATH IMS includes several ancillary support applications that do not collect, store, or display any personally identifiable information (PII). The systems that will not contain personally identifiable information are a public information website, a SharePoint collaboration site, a tobacco product image repository using the Alchemy image management application, a SAS® collaboration environment, a biospecimen tracking tool called BEST, a technical support issue tracking tools called BMC Remedy Magic, a Learning Management System hosted by ComplianceWire, an anonymous incentive payment management application hosted by Payoneer, and an inventory tracking application called ITMS. The public website will be used to convey information about the study to the public. The SharePoint site will be used for the partners in the study to collaborate and share ideas about the research. Alchemy is an image management system that will store images of tobacco products and ads. The SAS Collaboration Environment is an environment in which research partners can access restricted use files that have had all personally identifiable information redacted. BEST tracks the shipping and receipt of biospecimens collected from participants, but does not store any participant data, only sample ID's which cannot be linked to participants by an external party. The Remedy Magic technical support tool tracks system problem reports, but identifies staff only by their business contact information, thus falling into the "federal contact data" category. The ComplianceWire application tracks training and certification of staff, and also holds only federal contact information. The Payoneer application supports the payment of incentives to study participants anonymously (participants are known to the application only by their debit card account number, not by any PII). ITMS is an inventory management application that is used to track the consumption of forms and other supplies. ITMS carries no data about participants or staff.

Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.

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)

No

12a. If no, identify the system operator:

Westat Inc.
1600 Research Blvd, Rockville, MD 20850

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

New

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

Acquisition/Development

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?*

No

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).

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the 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) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	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 Uniform Resource Locator(s) (URL)	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
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.

Yes

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

Categories:	Yes/No
Employees	No
Public Citizen	No

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

**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)	No
Date of Birth	No
SSN *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	No
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	No

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

N/A
**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.
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?

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 *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	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):*

NA

24. If the PII in the system is matched against PII in one or more other computer systems, are computer data matching agreement(s) in place?

No

25. Is there a process in place to notify organizations or systems that are dependent upon the PII contained in this system when major changes occur (i.e., revisions to PII, or when the system is replaced)?

No

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

N/A

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

N/A

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?

N/A

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

{notification text}

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?

NA

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

NA

29. Are there rules of conduct in place for access to PII on the system?

NA

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	NA	{purpose text}
Administrators	NA	
Developers	NA	
Contractors	NA	
Other	NA	{purpose text}

**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:*

N/A

**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.])*

{process text}

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	Public website: www.pathstudyinfo.gov SharePoint collaboration site: www.pathcollaboration.org
Intranet	Yes	
Both	Yes	

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?
(Note: A website privacy policy is required for Internet sites only.)

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)?
(Note: Privacy policy in machine-readable format is required for Internet sites only.)

Yes

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

36. Does the website employ tracking technologies?

Yes

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

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

No

37a. If yes, is there a unique privacy policy for the site, and does the unique privacy policy address the process for obtaining parental consent if any

information is collected?

38. Does the website collect PII from individuals?

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	No
Date of Birth	No
SSN *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	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: Employer Name, NIH commons ID, NIH account ID, Job specialty	No

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

N/A

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.

Yes

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 (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?

A C&A is in progress.

42. Is there a system security plan for this system?

Yes

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

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

Yes

47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?

Yes

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

Yes

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

Yes

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

User roles are defined and individuals are assigned to one or more roles. These roles ensure that access privileges are narrowly defined, and that only those staff members that need certain types of access are granted that access. In addition to limiting functions, physical access controls limit access to the system.

Accountability is assured through authentication and authorization and the use of audit logs for applications, systems and network infrastructure components.

**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):*

N/A

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

N/A

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)	Yes
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 Westat systems group is responsible for monitoring and responding to any security incident in collaboration with the project. The systems group employs various tools like network scanners and sniffers and regularly scheduled internal and external agency network vulnerability scans etc. to stay on top of any security threat. All privacy and/or security incidents, or suspected incidents, must be reported promptly by the project to the agency.

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	Yes
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:*

Information is secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly accredited information system, control of changes to the system, by appropriate planning and testing of configuration management and contingency processes, by ensuring that all users of the information system are properly identified and authorized for access and are aware of and acknowledge the system rules of behavior, by ensuring that any contingency or incident is handled expeditiously, properly maintaining the system and regulating the environment it operates in, by controlling media, by evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the confidentiality and integrity of the information system, and by adhering to the requirements established in the contract and statement of work.

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:		

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:*

07/01/2012

**2. OPDIV Name:*

National Institute on Drug Abuse (NIDA)

**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:*

TBD

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

8954

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

PATH IMS – Core Systems

**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	
Dr. Kevin Paul Conway NSC BG RM 5185 6001 EXECUTIVE BLVD ROCKVILLE MD 20852 (301) 402-1817 kevin.conway@nih.gov	

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

The PATH IMS includes a set of core applications that collect and store research and study operations data, including study participants' PII as needed to identify, contact, and follow-up with participants. These applications include: the Home Office Management System (HMS), the Basic Field Operating Systems (BFOS/IMS and BFOS/SMS), the Multi-Mode Manager (M3), Blaise® survey instruments, the Blaise Editing System (BES), and the BMC Remedy Magic (Secure Instance). The HMS tracks overall information about the study sample, the status of field activities, and the status of study participants as the study protocol unfolds. The BFOS/IMS (**Interviewer** Management System) allows field interviewers to manage their cases, launch data collection instruments, record contacts and contact attempts, and record study activity completion statuses. The BFOS/SMS (**Supervisor** Management System) allows field supervisors to assign cases to

interviewers and track field activity in detail. The M3 is a data transport layer that allows flexible, secure communication between HMS, BFOS, and other applications that collect or generate study data in different modes. Blaise is a commercial survey instrumentation platform which Westat uses to develop and deploy the PATH data collection instruments. Blaise itself is a tool; it is the Blaise instruments that collect the data, which is stored in secure databases. The BES is a back-end system used to review and clean data collected by the Blaise instruments. The Magic application tracks questions, issues, and complaints reported by the public or by participants who call the PATH 800 number or request information via the PATH website.

Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.

**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?*

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).

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):*

N/A

**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:*

For PATH, Westat on behalf of NIDA will collect PII as necessary to identify, screen, enroll, and maintain contact with study participants and potential participants. The data include name, address, telephone, and other contact information as well as some information critical to informed consent and other PATH protocol procedures such as date of birth. PII will NOT be disseminated beyond the project in any form; it is only used to conduct study operations. Any data analyzed by PATH investigators or other authorized investigators will have PII removed and will have undergone appropriate non-disclosure review and modification. Any PII collected by PATH is strictly voluntary. Study participants may refuse to answer any question, and may withdraw from participation at any time.

**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.]):*

Before participants enroll in the study, they are given a detailed written explanation of the study's purpose, methods, and the uses to which any information collected will be put. At this time they are asked to sign a written general consent to participate in the study, and notified that they may withdraw at any time without penalty. Prior to specific study procedures, such as an in-home visit or a blood collection, study participants are informed of the purpose of the activity and asked for consent again.
Participants will be notified of any substantive change to the system that would have any impact on the original consent(s), and will be given an opportunity to withdraw their consent. If a participant withdraws from the study, he or she may request that all study data collected about them up to that time be destroyed, and PATH will comply with that request.

**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 following levels of security controls protect PII in the PATH IMS core systems:

1. Only PATH supplied tablet computers with NIST and FIPS-compliant security controls, including whole disk encryption, can be used to collect or access data in the field.
2. A valid PATH username and password is required to access any PATH core application.
3. Two-factor authentication is required to access central systems containing PII.
4. PII stored in the BFOS/SMS, M3, and HMS database is encrypted.
5. All PATH core applications generate audit logs that contain records for every access activity.
6. Access to the PATH data center is restricted by the Westat Corporate Officer for System Security.
7. A special keycard is required to open a cipher lock to gain access to the Data Center
8. There are video monitors that record activity in the data center.
9. Only authorized personnel who have passed the appropriate level of background investigation may access PII.
10. All PATH staff must take annual computer security awareness training, privacy awareness training, and human subjects protection training.

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:*

7/1/2012

**2. OPDIV Name:*

National Institute on Drug Abuse (NIDA)

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

TBD

**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:*

TBD

5a. OMB Collection Approval Number Expiration Date:

TBD

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

Westat internal project ID 8954

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

PATH IMS – Core Systems

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

System Location:	
OPDIV or contractor office building	Westat Inc. 1600 Research Blvd.
Room	
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	Dr. Kevin Paul Conway

The following information will not be made publicly available:

POC Title	Deputy Director
POC Organization	National Institute on Drug Abuse
POC Phone	(301) 402-1817
POC Email	Kevin.conway@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 PATH IMS includes a set of core applications that collect and store research and study operations data, including study participants' PII as needed to identify, contact, and follow-up with participants. These applications include: the Home Office Management System (HMS), the Basic Field Operating Systems (BFOS/IMS and BFOS/SMS), the Multi-Mode Manager (M3), Blaise® survey instruments, the Blaise Editing System (BES), and the BMC Remedy Magic (Secure Instance). The HMS tracks overall information about the study sample, the status of field activities, and the status of study participants as the study protocol unfolds. The BFOS/IMS (**Interviewer** Management System) allows field interviewers to manage their cases, launch data collection instruments, record contacts and contact attempts, and record study activity completion statuses. The BFOS/SMS (**Supervisor** Management System) allows field supervisors to assign cases to interviewers and track field activity in detail. The M3 is a data transport layer that allows flexible, secure communication between HMS, BFOS, and other applications that collect or generate study data in different modes. Blaise is a commercial survey instrumentation platform which Westat uses to develop and deploy the PATH data collection instruments. Blaise itself is a tool; it is the Blaise instruments that collect the data, which is stored in secure databases. The BES is a back-end system used to review and clean data collected by the Blaise instruments. The Magic application tracks questions, issues, and complaints reported by the public or by participants who call the PATH 800 number or request information via the PATH website.

Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.

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)

No

12a. If no, identify the system operator:

Westat Inc.
1600 Research Blvd, Rockville, MD 20850

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

New

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

Acquisition/Development

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

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).

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the 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) *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web Uniform Resource Locator(s) (URL)	No
Personal Email Address	Yes
Education Records	No
Military Status	Yes
Employment Status	No
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	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)	Yes
Date of Birth	No
SSN *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	No

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

Yes
**21. Is the system subject to the Privacy Act? (If the response to Q.19 is Yes, the response to Q.21 must be Yes and a SORN number is required for Q.4)*
Yes
21a. If yes but a SORN has not been created, please provide an explanation.
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?

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 *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	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

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

N/A

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?

N/A

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)?

N/A

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.

Before participants enroll in the study, they are given a detailed written explanation of the study's purpose, methods, and the uses to which any information collected will be put. At this time they are asked to sign a written general consent to participate in the study, and notified that they may withdraw at any time without penalty. Prior to specific study procedures, such as an in-home visit or a blood collection, study participants are informed of the purpose of the activity and asked for consent again.
Participants will be notified of any substantive change to the system that would have any impact on the original consent(s), and will be given an opportunity to withdraw their consent. If a participant withdraws from the study, he or she may request that all study data collected about them up to that time be destroyed, and PATH will comply with that request.

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.

Participants may at any time contact PATH using a toll-free telephone number, which is staffed by a dedicated Support Desk staff. Complaints received from and issues reported by participants are escalated from the Support Desk to PATH study management and to NIDA, depending on the nature of the report. Participants may also contact NIDA directly; this information is available on the PATH website www.pathstudyinfo.gov.

At the NIH level, the Incident Response Team in OD CIO is responsible for the NIH-wide incident response capability. The IRT receives incident reports from its intrusion detection server and from individuals. The IRT informs the appropriate technical staff in the affected Institute or Center who take follow-up actions to investigate and respond to the incident.

28. Are there processes in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy?

No

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

No data have yet been collected; the system is still in development and testing.

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	Users with specific roles, such as Data Collector or Field Supervisor, have access to PII as needed for study operations (e.g., scheduling an appointment with a study participant)
Administrators	Yes	Administrators, because of their role in system operations, security, and network administration, have privileges that would allow them to access servers storing PII. These individuals have all passed background investigations, taken security training over and beyond regular users, and by policy may not use their access privileges to examine any data other than system operational data (e.g., error logs and audit logs) necessary to perform thir duties.

Developers	Yes	Certain developers may require access to production data, including PII, in order to diagnose and fix a problem that cannot be reproduced in Test mode. These developers are all cleared to see PII if necessary, and have taken required security and human subjects protection training. By policy, these developers may only access production systems when requested by operations staff, and access to production is only granted temporarily for the duration of the diagnosis/fix/test cycle.
Contractors	Yes	One subcontractor to Westat, Hooper Holmes, has limited access to participant contact information for the purpose of scheduling biospecimen collection visits. These staff operate under the same clearance, training, authorization, and policy constraints that apply to Westat staff.
Other	NA	

**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:*

For PATH, Westat on behalf of NIDA will collect PII as necessary to identify, screen, enroll, and maintain contact with study participants and potential participants. The data include name, address, telephone, and other contact information as well as some information critical to informed consent and other PATH protocol procedures such as date of birth. PII will NOT be disseminated beyond the project in any form; it is only used to conduct study operations. Any data analyzed by PATH investigators or other authorized investigators will have PII removed and will have undergone appropriate non-disclosure review and modification. Any PII collected by PATH is strictly voluntary. Study participants may refuse to answer any question, and may withdraw from participation at any time.

**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.])*

Before participants enroll in the study, they are given a detailed written explanation of the study's purpose, methods, and the uses to which any information collected will be put. At this time they are asked to sign a written general consent to participate in the study, and notified that they may withdraw at any time without penalty. They are given a copy of the consent brochure and the consent signature page(s) indicating specifically what they have agreed to. Prior to specific study procedures, such as an in-home visit or a blood collection, study participants are informed of the purpose of the activity and asked for consent again.
Participants will be notified of any substantive change to the system that would have any impact on the original consent(s), and will be given an opportunity to withdraw their consent. If a participant withdraws from the study, he or she may request that all study data collected about them up to that time be destroyed, and PATH will comply with that request.

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	Yes	

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?
(Note: A website privacy policy is required for Internet sites only.)

N/A

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)?
(Note: Privacy policy in machine-readable format is required for Internet sites only.)

N/A

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?

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 *Note: According to OMB 07-16M, All agencies MUST participate in government-wide effort to eliminate unnecessary use of and explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs.*	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	No
Medical Notes	No
Financial Account Information	No
Certificates	No
Legal Documents	No
Device Identifiers	No
Web URLs	No
Personal Email Address	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other: Employer Name, NIH commons ID, NIH account ID, Job specialty	No

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?

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.

Yes

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 (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?

C&A is in progress.

42. Is there a system security plan for this system?

Yes

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

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

Yes

47. Have personnel (system owners, managers, operators, contractors and/or program managers) using the system been trained and made aware of their responsibilities for protecting the information being collected and maintained?

Yes

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

Yes

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

Yes

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

User roles are defined and individuals are assigned to one or more roles. These roles ensure that access privileges are narrowly defined, and that only those staff members that need certain types of access are granted that access. In addition to limiting functions, physical access controls limit access to the system.

Accountability is assured through authentication and authorization and the use of audit logs for applications, systems and network infrastructure components.

**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:

PII is never released to the general public or research community at large. If a study participant decides to leave the study, he or she can request that all his/her data be destroyed, including PII, and the NCS must comply with that request. All PII is encrypted so that even on backup media, it cannot be accessed directly. Specific policies have not yet been formulated regarding the destruction of PII from the PATH systems at the end of the study, but it is certain that those policies and procedures will comply with the Privacy Act, and with HHS and NIH guidelines, and with IRB guidelines.

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)	Yes
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 Westat systems group is responsible for monitoring and responding to any security incident in collaboration with the project. The systems group employs various tools like network scanners and sniffers and regularly scheduled internal and external agency network vulnerability scans etc. to stay on top of any security threat. All privacy and/or security incidents, or suspected incidents, must be reported promptly by the project to the agency.

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	Yes
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:*

Information is secured on the system through access controls, personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly accredited information system, control of changes to the system, by appropriate planning and testing of configuration management and contingency processes, by ensuring that all users of the information system are properly identified and authorized for access and are aware of and acknowledge the system rules of behavior, by ensuring that any contingency or incident is handled expeditiously, properly maintaining the system and regulating the environment it operates in, by controlling media, by evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the confidentiality and integrity of the information system, and by adhering to the requirements established in the contract and statement of work.

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:		