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:*

15 July 2015

**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:*

Requested

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

N/A

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

NIH NCI Cancer Trials Support Unit (CTSU)

**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	Mike Montello

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

The Cancer Trials Support Unit (CTSU) is a service offered by the National Cancer Institute (NIH) to enhance and facilitate access to cancer clinical trials for clinical investigators in the United States and Canada. The CTSU maintains a broad menu of trials developed by the National Clinical Trials Network (NCTN) groups and other research consortia and works with these organizations to offer patient enrollment, data collection, and data quality management services to clinical sites entering patients in these trials. In addition, the CTSU offers a regulatory support service to all cancer clinical trials by collection of regulatory documents and maintenance of a national database of investigators and sites. The CTSU also provides education and training for clinical site staff and clinical trials promotion services to help increase enrollment in cancer trials. A large and complex information technology infrastructure has been developed to support CTSU operations and exchange data with other data centers involved in cancer research. Westat is the prime contractor on the project, utilizing subcontractors, and working with numerous other organizations.

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

Existing

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

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

Yes

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

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

Yes

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

Yes

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

CTSU shares NCI Investigator and NCI Associates data with CTEP-ESYS – an NCI sponsored project and other NCTN groups, to increase participation in NCI sponsored cancer related clinical trials.
With increased awareness and access to the trials information, CTEP intends to increase physician and patient participation in the NCI sponsored trials.
CTSU shares this information, which may contain PII, with lead research organizations for the purpose of assuring patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations.
CTSU also shares this information with the NCTN groups and with NCI Center for Biomedical Informatics and Information Technology's Clinical Data System (CBIIT-CDS). Some of this information is available to staff at NCTN group member sites on a limited basis.
Some of the information that CTSU shares with CTEP and CBIIT-CDS is also publicly available elsewhere.

**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:*

Legislation authority is the Public Health Service Act (42 U.S.C. 241, 242, 248, 282, 284, 285a-j, 285l-q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.).

The types of data used are scientific and health data about cancer clinical trials, including clinical and pre-clinical data with associated regulatory and administrative supporting information. Patient participation in CTEP clinical trials is voluntary and participants in CTEP clinical trials sign an informed consent. Types of information available in the CTSU Enterprise include protocols and protocol attributes, Investigator registration details, and non-PII patient accrual details. The information is used to assure patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations.

The CTSU collects and maintains various types of data.

- Investigator and treatment site staff information is obtained from the CTEP-ESYS and maintained in the CTSU. NCTN group staff use this data to maintain their membership rosters. This data is used as part of the credentialing requirements for patient enrollments.
- Protocol and regulatory information related to the member sites is collected and maintained in the CTSU Enterprise. This data is disseminated to NCTN groups to support patient enrollment and data collection processes.
- The CTSU also supports web application to collect demographic, eligibility criteria data, and other enrollment required data as part of patient enrollment process. This data is collected on behalf of and shared with the organization that is leading a study.
- For some studies, the CTSU performs the complete data management and collects/maintains the clinical data collected for a study and disseminates it to the organization leading the study.
- Patient participation in CTEP clinical trials is voluntary. Patient demographic data is provided by the participating sites.
- PII collected and maintained includes name, date of birth, social security number(SSN), mailing address, phone number, medical records number, medical notes, and email address.

**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.]):*

Users that access the systems must reregister on an annual basis and any changes would be communicated through that process.

NCI Investigators furnish their information to CTEP in a written application. PII related to the Regulatory Support System (RSS)/Financial Management System (FMS) [JM1] are supplied to the CTSU at the time of account request via a standard application.

Participating research organizations require trial participants to sign an authorization to use or disclose identifiable health information for research. A subject cannot enroll in a study without providing one of these release forms. They can withdraw the authorization at a later time, but then must leave the study. The link to the form is https://www.ctsu.org/HIPAA/

**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:*

CTSU data is maintained in a secure database.

The following are in place as Management Controls:
- Rules of Behavior
- System Security Plan
- Configuration Management, Change Management Plans and Processes
- Disaster Recovery Plan
- Interconnection Security Agreement

The following are in place as Technical controls for CTSU:
- User ID and Passwords are required to login to CTSU applications
- The CTSU application is hosted within Westat Network boundaries and is protected by Westat provided Perimeter Firewall and Intrusion Detection Systems
- SSL Encryption is enabled to access web based interfaces of CTSU modules, where necessary
- Proactive Systems Monitoring and Alerts Management
- Anti-virus, security updates and patching procedures
- Periodic vulnerability scans for CTSU systems – both internal and external
- Incidence Response Procedures
- System and Database Audit Trails and Logs

The following are in place as Operational controls for CTSU:
- Personnel Security
- Security Training/Clearance Process for all personnel working on CTSU
- Westat Hiring and Termination Process
- Non Disclosure Agreements for all employees working on CTSU
- All employees take/review NIH CIT Security Awareness Training on an annual basis
- Physical and Environmental Protection
- Visitor Log Procedures
- Backup Procedures
- Offsite Storage for Tapes
- Video Surveillance of Data Center
- AC Maintenance Process
- Contingency /Disaster Recovery Plan – tested regularly (last test on 12/10/2012)
- Incidence Response Procedures
- Alerts and Scans
- Identification and Authentication
- User Account Management Process
- Role based user access to systems
- Password Change Policies (in sync with CTEP-ESYS)
- Procedures for handling lost/compromised passwords
- Audit Trails

The system falls under the Privacy Act System of Records Notice 09-25-0200

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 15 2015

**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:*

Requested

5a. OMB Collection Approval Number Expiration Date:

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

N/A

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

NIH NCI Cancer Trials Support Unit (CTSU)

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

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

The following information will not be made publicly available:

POC Title	Branch Chief Operations and Informatics Branch Cancer Therapy Evaluation Program Division of Cancer Treatment and Diagnosis
POC Organization	NIH/NCI
POC Phone	240-276-6080
POC Email	montellom@mail.nih.gov

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

The Cancer Trials Support Unit (CTSU) is a service offered by the National Cancer Institute (NIH) to enhance and facilitate access to cancer clinical trials for clinical investigators in the United States and Canada. The CTSU maintains a broad menu of trials developed by the National Clinical Trials Network (NCTN) groups and other research consortia and works with these organizations to offer patient enrollment, data collection, and data quality management services to clinical sites entering patients in these trials. In addition, the CTSU offers a regulatory support service to all cancer clinical trials by collection of regulatory documents and maintenance of a national database of investigators and sites. The CTSU also provides education and training for clinical site staff and clinical trials promotion services to help increase enrollment in cancer trials. A large and complex information technology infrastructure has been developed to support CTSU operations and exchange data with other data centers involved in cancer research. Westat is the prime contractor on the project, utilizing subcontractors, and working with numerous other organizations.

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

**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?

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	**Yes**
New Interagency Uses	**No**
Internal Flow or Collection	**Yes**
Alteration in Character of Data	**No**

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

Minor Application (child)

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

Yes

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

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
Social Security Number (SSN)	Yes
Photographic Identifiers	No
Driver's License	No

Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	Yes
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	Yes
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	

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

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

Categories:	Yes/No
Employees	Yes
Public Citizen	No
Patients	Yes
Business partners/contacts (Federal, state, local agencies)	Yes
Vendors/Suppliers/Contractors	Yes
Other	NCI Investigators, NCI Associates, NCI Stakeholders

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

Yes

Please indicate "Yes" or "No" for each PII category. If the applicable PII category is not listed, please use the Other field to identify the appropriate category of PII.

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No
SSN	No
Photographic Identifiers	No

Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	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	

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

Yes

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

Yes

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

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

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

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	Yes
SSN	Yes
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	Yes
Medical Notes	Yes
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	

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

CTSU shares NCI Investigator and NCI Associates data with CTEP-ESYS – a NCI sponsored project and other NCTN groups, to increase participation in NCI sponsored cancer related clinical trials.
With increased awareness and access to the trials information, CTEP intends to increase physician and patient participation in the NCI sponsored trials.
CTSU shares this information, which may contain PII, with lead research organizations for the purpose of assuring patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations.
CTSU also shares information on patients, investigators and associates with the NCTN groups and with NCI Center for Biomedical Informatics and Information Technology's Clinical Data System (CBIIT-CDS). Some of this information is available to staff at NCTN group member sites on a limited basis.
Some of the information that CTSU shares with CTEP and CBIIT-CDS is also publicly available elsewhere.

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?

Yes

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

Yes

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

Yes

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

CTSU obtains PII related to NCI Investigators and Associates who are aware of the intended purpose and usage of the information. NCI Investigators furnish their information to CTEP in a written application. PII related to the Regulatory Support System (RSS) are supplied to the CTSU at the time of account request via a standard application.

Participating research organizations require trial participants (patients) to sign an authorization to use or disclose identifiable health information for research. A subject cannot enroll in a study without providing one of these release forms. They can withdraw the authorization at a later time, but then must leave the study. The link to the form is https://www.ctsu.org/HIPAA/

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.

Individuals can contact the CTSU Help Desk to make an incident report for release of PII or for correction of PII. A procedure document will be posted on the CTSU public web site.

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 NCI Investigator and Associate data are synchronized with the CTEP system. Data in that system are maintained through a yearly reregistration process that is required for both NCI Investigators and Associates.

The CTSU member sites and the NCTN groups are contacted periodically for corrections to the PII (e.g. name/email/phone) for their members who use the CTSU applications.

The process and forms for maintaining patient related data are available as part of the protocols and can be submitted by the participating sites. Quality assurance and audit procedures are used to ensure accuracy of the data collected.

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	CTSU staff and NCTN groups: a) Maintain regulatory, membership, and protocol logistics data; b) Manage patient enrollment and clinical research data.
Administrators	Yes	Privileged CTSU staff: a) Manage system and provide support.
Developers	Yes	View/Update/Report Manage regulatory data.
Contractors	Yes	View/Update/Report Manage regulatory data.
Other		

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

Legislation authority is the Public Health Service Act (42 U.S.C. 241, 242, 248, 282, 284, 285a-j, 285l-q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.).

The types of data used are scientific and health data about cancer clinical trials, including clinical and pre-clinical data with associated regulatory and administrative supporting information. Patient participation in CTEP clinical trials is voluntary and participants in CTEP clinical trials sign an informed consent. Types of information available in the CTSU Enterprise include protocols and protocol attributes,

Investigator registration details, and non-PII patient accrual details. The information is used to assure patient safety, for scientific decision making, drug distribution, regulatory oversight (i.e., investigator registration; trial audits) and to facilitate administrative operations.

The CTSU collects and maintains various types of data.

- Investigator and treatment site staff information is obtained from the CTEP-ESYS and maintained in the CTSU. NCTN group staff use this data to maintain their membership rosters. This data is used as part of the credentialing requirements for patient enrollments.
- Protocol and regulatory information related to the member sites is collected and maintained in the CTSU Enterprise. This data is disseminated to NCTN groups to support patient enrollment and data collection processes.
- The CTSU also supports web application to collect demographic, eligibility criteria data, and other enrollment required data as part of patient enrollment process. This data is collected on behalf of and shared with the organization that is leading a study.
- For some studies, the CTSU performs the complete data management and collects/maintains the clinical data collected for a study and disseminates it to the organization leading the study.
- Patient participation in CTEP clinical trials is voluntary. Patient demographic data is provided by the participating sites.
- PII collected and maintained includes name, date of birth, social security number(SSN), mailing address, phone number, medical records number, medical notes, and email address.

**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.])*

Users that access the systems must reregister on an annual basis and any changes would be communicated through that process.

NCI Investigators furnish their information to CTEP in a written application. PII related to the Regulatory Support System (RSS) are supplied to the CTSU at the time of account request via a standard application.

Participating research organizations require trial participants (patient) to sign an authorization to use or disclose identifiable health information for research. A subject cannot enroll in a study without providing one of these release forms. They can withdraw the authorization at a later time, but then must leave the study. The link to the form is https://www.ctsu.org/HIPAA/

WEBSITE HOSTING PRACTICES

1 Website Hosting Practices

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

Yes

Please indicate "Yes" or "No" for each type of site below. If the system hosts both Internet and Intranet sites, indicate "Yes" for "Both" only.	Yes/ No	If the system hosts an Internet site, please enter the site URL. Do not enter any URL(s) for Intranet sites.
Internet	Yes	https://www.ctsu.org; https://open.ctsu.org https://rss.ctsu.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?

Yes

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

Yes

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

36. Does the website employ tracking technologies?

Yes

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

**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	Yes
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	Yes
Personal Phone Numbers	Yes
Medical Records Numbers	Yes
Medical Notes	Yes
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	

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.

ADMINISTRATIVE CONTROLS

1	Administrative Controls

Note: This PIA uses the terms ''Administrative,'' ''Technical'' and ''Physical'' to refer to security control questions—terms that are used in several Federal laws when referencing security requirements.

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

Yes

41a. If yes, please indicate when the C&A was completed (Note: The C&A date is populated in the System Inventory form via the responsible Security personnel):

11/22/2013

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

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

Yes

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

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

Yes

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

Yes

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

Yes

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

Yes

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

There are user roles defined for CTSU Enterprise application access. These roles assure that those access privileges are very narrowly defined and that only the staff that perform these roles are granted that access. In addition to limiting functions, the user's membership at sites also constrain the type of data that can be viewed.

Accountability is assured through strict authentication and authorization and the use of audit logs that exist 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 data stored in the CTSU is not purged or deleted and is retained to support CTSU'S business mission.

The system falls under the Privacy Act System of Records Notice 09-25-0200

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:

Westat Systems Group is responsible for monitoring and responding to any security incident in collaboration with the CTSU project group. The Systems Group employs various tools such as Snort and regularly scheduled internal and external agency network vulnerability scans, etc., to stay on top of any security threat.

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:*

CTSU data is maintained in a secure database.

The following are in place as Management Controls:
- Rules of Behavior
- System Security Plan
- Configuration Management, Change Management Plans and Processes
- Disaster Recovery Plan
- Interconnection Security Agreement

The following are in place as Technical controls for CTSU:
- User ID and Passwords are required to login to CTSU applications
- The CTSU application is hosted within Westat Network boundaries and is protected by Westat provided Perimeter Firewall and Intrusion Detection Systems
- SSL Encryption is enabled to access web based interfaces of CTSU modules, where necessary
- Proactive Systems Monitoring and Alerts Management
- Anti-virus, security updates and patching procedures
- Periodic vulnerability scans for CTSU systems – both internal and external
- Incidence Response Procedures
- System and Database Audit Trails and Logs

The following are in place as Operational controls for CTSU:
- Personnel Security
- Security Training/Clearance Process for all personnel working on CTSU
- Westat Hiring and Termination Process
- Non Disclosure Agreements for all employees working on CTSU
- All employees take/review NIH CIT Security Awareness Training on an annual basis
- Physical and Environmental Protection
- Visitor Log Procedures
- Backup Procedures
- Offsite Storage for Tapes
- Video Surveillance of Data Center
- AC Maintenance Process
- Contingency /Disaster Recovery Plan – tested regularly (last test on 11/2/08)
- Incidence Response Procedures
- Alerts and Scans
- Identification and Authentication
- User Account Management Process
- Role based user access to systems
- Password Change Policies (in sync with CTEP-ESYS)
- Procedures for handling lost/compromised passwords
- Audit Trails

The system falls under the Privacy Act System of Records Notice 09-25-0200

APPROVAL/DEMOTION

1	System Information
System Name:	NIH NCI Cancer Trials Support Unit (CTSU)

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	
Comments:	
Approval/Demotion Point of Contact:	Suzy Milliard

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	No
Date Published:	
Publicly posted PIA URL or no PIA URL explanation:	

PIA % COMPLETE

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