06.1 HHS Privacy Impact Assessment (Form) / NIH NCI Smokefree QuitTXT Evaluation Study (Survey) (Item)

Primavera ProSight

Form Report, printed by: Milliard, Suzanne, **Dec 18, 2012**

PIA SUMMARY

1

The following required questions with an asterisk (*) represent the information necessary to complete the PIA Summary for transmission to the Office of Management and Budget (OMB) and public posting in accordance with OMB Memorandum (M) 03-22.

Note: If a question or its response is not applicable, please answer "N/A" to that question where possible. If the system hosts a website, the Website Hosting Practices section is required to be completed regardless of the presence of personally identifiable information (PII). If no PII is contained in the system, please answer questions in the PIA Summary Tab and then promote the PIA to the Senior Official for Privacy who will authorize the PIA. If this system contains PII, all remaining questions on the PIA Form Tabs must be completed prior to signature and promotion.

2 Summary of PIA Required Questions

**Is this a new PIA?*

Yes

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

**1. Date of this Submission:*

Nov 13, 2012

**2. OPDIV Name:*

NIH

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

09-25-0156

**5. OMB Information Collection Approval Number:*

N/A

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

N/A

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

NIH NCI Smokefree QuitTXT Evaluation Study (Survey)

**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. Linda Squiers

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

RTI International has been contracted by the NCI to develop a web based survey application that collects effectiveness of QuitTXT program, a text message intervention designed for young adult smokers age 18-29. The survey study will operate for a limited period of approximately 2 years, beginning in early 2013 and ending around the end of 2014. RTI is an independent, nonprofit institute that provides research, development, and technical services to government and commercial clients worldwide. Their mission is to improve the human condition by turning knowledge into practice. RTI has a history of scientific achievement in the areas of health and pharmaceuticals, education and training, surveys and statistics, advanced technology, international development, economic and social policy, energy and the environment, and laboratory testing and chemical analysis.

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

New

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

TIP: If the answer to Question 17 is "No" (indicating the system does not contain PII), only the remaining PIA Summary tab questions need to be completed and submitted. If the system does contain PII, the full PIA must be completed and submitted. (Although note that "Employee systems," – i.e., systems that

collect PII "permitting the physical or online contacting of a specific individual … employed [by] the Federal Government – only need to complete the PIA Summary tab.)

Yes

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

No

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

Yes

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

Yes

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

Participants' cell phone numbers are shared with Mobile Commons, the text messaging vendor, because they need to know when an individual has enrolled in the study in order to send them the appropriate set of text messages. Thus, we will share only the cell phone numbers of those who have completed enrollment.

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

1. The survey follows up with users who participate in the Smokefree Quit.TXT program, where they have consented to send/receive messages that will help them follow through with smoking cessation. Users who consent to participate in this evaluation study via the online web based survey are asked to provide email mobile phone number, address, ethnicity, race, and gender. Data are NOT collected only from federal contacts, but are collected from private citizens who are participating in the Quit.TXT program.
2. Data collected are used to describe the respondents as an aggregate, as well as to explore the relationships between demographic variables and the uptake and outcomes of the study. Taking the survey is voluntary as is answering any of the survey questions (e.g., respondents are not required to respond to questions on ethnicity, race, and/or gender).
3. Data collected does contain PII.
4. Participation in the study is completely voluntary. However, for those who do participate, collection of the user's email address and mobile phone number are mandatory, but other demographic PII are not required.

**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.]):*

1. Because major changes to the system are prohibited once OMB and IRB approvals are obtained, there are no plans in place to notify and obtain consent from individuals.

2. Consent to participate in the study is obtained from an individual when he/she clicks on the link (URL) for the web survey and enters his/her randomly generated user ID and password. Individuals will see that there are survey questions on ethnicity, race, and gender and can choose to skip those (and any other) survey questions.

3. Data from the survey will be reported in aggregate format only and will be shared only with appropriate NIH staff.

**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:*

RTI will observe high standards of information technology (IT) security to protect the confidentiality, integrity and availability of all computer-based systems and the data they contain. RTI IT security policies and procedures are designed to protect information systems and data from a wide range of risks and to educate our staff to be aware of their responsibilities for ensuring information security and to comply with these policies. RTI also participates with agencies to ensure that our policies conform to agency information security requirements and applicable laws and regulations as required by contract.

RTI's Information Technology Service supports approximately 400 Windows, Linux, and high-performance cluster computing (HPCC) servers. Data storage capacity is in excess of 50 terabytes (TB). RAID disk arrays and Storage Area Network (SAN) technologies are used for performance and redundancy in the event of a disk failure. Microsoft Exchange servers are used for electronic messaging and scheduling. Microsoft SQL and Oracle servers are provided for database applications.

Web content delivery is provided using multiple highly available FIPS 140-2 compliant hardware load-balancers. Web server farms running Microsoft Internet Information Server, Oracle Application Server, Adobe ColdFusion, and Apache Tomcat are currently supported and in use. Significant levels of redundancy are achieved through the geographical separation of redundant servers and services. Additionally, third-party applications, such as NSI's Double-Take, are utilized to minimize service disruption.

RTI maintains several fully switched and routed Ethernet-based local area networks (LANs) in support of both corporate and project initiatives. RTI wide area networks (WANs) employ technologies which include site-to-site VPN, Metro Ethernet, MPLS, VSAT, Voice over IP (VoIP), and WAN Acceleration appliances.

RTI maintains two links to the Internet: a primary 1 Gb fiber link and a secondary 100 Mb/sec microwave link. RTI's Internet service provider links are path-diverse and terminate in separate data centers on RTI's main campus. Both links are maintained in an active state and configured for automated, unattended failover.

Remote access to RTI's data networks is provided through the use of client-computer-installed VPN software, a clientless SSL/VPN portal, and direct dial-in connections. Access from the Internet is available to authorized staff only and is controlled by RTI's Internet firewalls. The use of RSA SecurID two-factor authentication for remote access is supported.

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:*

Nov 13, 2012

**2. OPDIV Name:*

NIH

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

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

09-25-0156

**5. OMB Information Collection Approval Number:*

N/A

5a. OMB Collection Approval Number Expiration Date:

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

N/A

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

NIH NCI Smokefree QuitTXT Evaluation Study (Survey)

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

System Location:	
OPDIV or contractor office building	RTI Haynes Bldg. (Bldg 08) at RTI Headquarters; 3040 Cornwallis Rd.
Room	Ragland Data Center
City	Research Triangle Park
State	NC

**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. Linda Squiers

The following information will not be made publicly available:

POC Title	Project Director
POC Organization	RTI
POC Phone	919-597-5128
POC Email	lsquiers@rti.org

**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)*

RTI International has been contracted by the NCI to develop a web based survey application that collects effectiveness of QuitTXT program, a text message intervention designed for young adult smokers age 18-29. The survey study will operate for a limited period of approximately 2 years, beginning in early 2013 and ending around the end of 2014. RTI is an independent, nonprofit institute that provides research, development, and technical services to government and commercial clients worldwide. Their mission is to improve the human condition by turning knowledge into practice. RTI has a history of scientific achievement in the areas of health and pharmaceuticals, education and training, surveys and statistics, advanced technology, international development, economic and social policy, energy and the environment, and laboratory testing and chemical analysis.

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:

RTI

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

New

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

Development/Acquisition

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

No

Please indicate "Yes" or "No" for each category below:	Yes/No
Conversions	No
Anonymous to Non-Anonymous	No
Significant System Management Changes	No
Significant Merging	No
New Public Access	No
Commercial Sources	No
New Interagency Uses	No
Internal Flow or Collection	No
Alteration in Character of Data	No

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

Minor Application (stand-alone)

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

Yes

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

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

Categories:	Yes/No
Name (for purposes other than contacting federal employees)	Yes
Date of Birth	No
Social Security Number (SSN)	No

Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	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	No
Employment Status	No
Foreign Activities	No
Other	Race, Ethnicity, Gender (all are voluntarily provided)

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	None

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

Yes

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

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

SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	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.

INFORMATION SHARING PRACTICES

1 Information Sharing Practices

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

Yes

Please indicate "Yes" or "No" for each category below:	Yes/No
Name (for purposes other than contacting federal employees)	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	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	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	None

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

Participants' cell phone numbers are shared with Mobile Commons, the text messaging vendor, because they need to know when an individual has enrolled in the study in order to send them the appropriate set of text messages. Thus, we will share only the cell phone numbers of those who have completed enrollment.

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.

Individuals can choose not to respond to the survey, and may skip any questions they do not wish to answer. For example, they may

choose not to provide their gender and ethnicity or name. They do need to provide their cell phone number and email address to participate in the study, however, as they are essential for delivering the program and surveys. Individuals who choose to enroll in the study are formally consented through an informed consent process approved by RTI's IRB. Once they have consented to participate, they are contacted through email and asked to take the surveys. The purpose of the surveys is described in the informed consent procedures. In addition, RTI will post the privacy policies on the web site. We ask for a name so we can personalize invitation letters and for following up with non-responders, however it is optional.

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.

RTI plans to provide an electronic mailbox and a toll free number that survey respondents can use to ask questions, make comments, or report technical difficulties. NIH will also provide a phone number for survey participants to call with questions or comments related to this study.

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.

As a standard operating procedure RTI periodically reviews all PII information contained in information systems to ensure the confidentiality, integrity, availability and accuracy of the information is properly maintained and safeguarded. For this particular system the PII information will be used in sample stratification and it will be used to personalize survey invitations and follow-up email reminders that are sent to non-respondents. In addition, the PII information collected by the survey instruments (race and ethnicity) will be used during the analysis and reporting phase of the project to produce aggregated results.

During data collection RTI will periodically extract the data from the system to review survey response data provided by the respondent for completeness and accuracy. Following data collection RTI will use SAS or SPSS to perform quality control checks on the data to ensure its accuracy and completeness.

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	Survey participants (users) must provide certain PII in order to participate in the evaluation including their mobile phone number and, optionallly, other PII fields as noted on the registration site.
Administrators	Yes	Admins require access to the phone number and the unique Identifier that is created internally to link survey participants to their survey data.
Developers	Yes	Developers require access to create linkages between survey data and data from Mobile Commons
Contractors	Yes	Mobile Commons staff will only need phone number but no other identifiable information.
Other	No	

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

1. The survey follows up with users who participate in the Smokefree Quit.TXT program, where they have consented to send/receive messages that will help them follow through with smoking cessation. Users who consent to participate in this evaluation study via the online web based survey are asked to provide email mobile phone number, address, ethnicity, race, and gender. Data are NOT collected only from federal contacts, but are collected from private citizens who are participating in the Quit.TXT program.
2. Data collected are used to describe the respondents as an aggregate, as well as to explore the relationships between demographic variables and the uptake and outcomes of the study. Taking the survey is voluntary as is answering any of the survey questions (e.g., respondents are not required to respond to questions on ethnicity, race, and/or gender).

3. Data collected does contain PII.
4. Participation in the study is completely voluntary. However, for those who do participate, collection of the user's email address and mobile phone number are mandatory, but other demographic PII are not required.

**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.])*

1. Because major changes to the system are prohibited once OMB and IRB approvals are obtained, there are no plans in place to notify and obtain consent from individuals.

2. Consent to participate in the study is obtained from an individual when he/she clicks on the link (URL) for the web survey and enters his/her randomly generated user ID and password. Individuals will see that there are survey questions on ethnicity, race, and gender and can choose to skip those (and any other) survey questions.

3. Data from the survey will be reported in aggregate format only and will be shared only with appropriate NIH staff.

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://QuitTXT.rti.org
Intranet	No	
Both	No	

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

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

Yes

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

Yes

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

Yes

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

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	N/A

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

No

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

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)	No
Date of Birth	No
SSN	No
Photographic Identifiers	No
Driver's License	No
Biometric Identifiers	No
Mother's Maiden Name	No
Vehicle Identifiers	No
Personal Mailing Address	No
Personal Phone Numbers	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	No
Education Records	No
Military Status	No
Employment Status	No
Foreign Activities	No
Other	Yes; age, race/ethnicity, education, sex, income, employment status all voluntarily provided.

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

Not Applicable

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

No

40a. If yes, note whether the system provides a disclaimer notice for users that follow external links to websites not owned or operated by HHS.

ADMINISTRATIVE CONTROLS

1	Administrative Controls

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

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

No

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

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

Not Applicable

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

Yes

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

Yes

44. Are files backed up regularly?

Yes

45. Are backup files stored offsite?

Yes

46. Are there user manuals for the system?

No

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

Yes

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

Yes

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

Yes

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

Access to the data collected by the system will be limited to only RTI project staff who are designated to work on this project. Role Based Access Controls are the primary means of restricting access by user based on need to access and job or study role.

**50. Are there policies or guidelines in place with regard to the retention and destruction of PII? (Refer to the C&A package and/or the Records Retention and Destruction section in SORN):*

Yes

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

Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1 - "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B-361), item 1100-C-2. Refer to the NIH Manual Chapter for specific disposition instructions.

TECHNICAL CONTROLS

1 Technical Controls

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

Yes

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

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

Yes

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

In the event of a security incident, the employee experiencing the incident is to report to RTI's Information Security Officer (ISO), who will notify the RTI System Manager and Project Director of the nature of the incident, date and time of the incident. The RTI System Manager will work with the System Administrator and System Developer to remediate the issue. The RTI Project Director will notify the NCI Project Director of the event, date and time of occurrence and the plan for remediation and when the issue is resolved. All incidents are documented in an incident tracking system.

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:*

RTI will observe high standards of information technology (IT) security to protect the confidentiality, integrity and availability of all computer-based systems and the data they contain. RTI IT security policies and procedures are designed to protect information systems and data from a wide range of risks and to educate our staff to be aware of their responsibilities for ensuring information security and to comply with these policies. RTI also participates with agencies to ensure that our policies conform to agency information security requirements and applicable laws and regulations as required by contract.

RTI's Information Technology Service supports approximately 400 Windows, Linux, and high-performance cluster computing (HPCC) servers. Data storage capacity is in excess of 50 terabytes (TB). RAID disk arrays and Storage Area Network (SAN) technologies are used for performance and redundancy in the event of a disk failure. Microsoft Exchange servers are used for electronic messaging and scheduling. Microsoft SQL and Oracle servers are provided for database applications.

Web content delivery is provided using multiple highly available FIPS 140-2 compliant hardware load-balancers. Web server farms running Microsoft Internet Information Server, Oracle Application Server, Adobe ColdFusion, and Apache Tomcat are currently supported and in use. Significant levels of redundancy are achieved through the geographical separation of redundant servers and services. Additionally, third-party applications, such as NSI's Double-Take, are utilized to minimize service disruption.

RTI maintains several fully switched and routed Ethernet-based local area networks (LANs) in support of both corporate and project initiatives. RTI wide area networks (WANs) employ technologies which include site-to-site VPN, Metro Ethernet, MPLS, VSAT, Voice over IP (VoIP), and WAN Acceleration appliances.

RTI maintains two links to the Internet: a primary 1 Gb fiber link and a secondary 100 Mb/sec microwave link. RTI's Internet service provider links are path-diverse and terminate in separate data centers on RTI's main campus. Both links are maintained in an active state and configured for automated, unattended failover.

Remote access to RTI's data networks is provided through the use of client-computer-installed VPN software, a clientless SSL/VPN portal, and direct dial-in connections. Access from the Internet is available to authorized staff only and is controlled by RTI's Internet firewalls. The use of RSA SecurID two-factor authentication for remote access is supported.

APPROVAL/DEMOTION

1	System Information
System Name:	NIH NCI Smokefree QuitTXT Evaluation Study (Survey)

2	PIA Reviewer Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	This is a temporary survey and externally-hosted, so does not require a C&A according to NCI security office.
Approval/Demotion Point of Contact:	Suzy Milliard
Date:	Nov 13, 2012

3	Senior Official for Privacy Approval/Promotion or Demotion
Promotion/Demotion:	Promote
Comments:	

4	OPDIV Senior Official for Privacy or Designee Approval

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

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

Name: _____ **Date:** _____

Name:	Karen Plá
Date:	Dec 12, 2012

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

PIA % COMPLETE

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