Privacy Impact Assessment (PIA): FDA - ExPECT II - QTR3 - 2022 - FDA2061510

Date Signed: 7/13/2022

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1460096
PIA Name:	FDA - ExPECT II - QTR3 - 2022 - FDA2061510	**Title:**	FDA - CTP RTI International
OpDiv:	FDA		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Operations and Maintenance
PTA - 1B:	Is this a FISMA-Reportable system?	No
PTA - 2:	Does the system include a website or online application?	No
PTA - 3:	Is the system or electronic collection, agency or contractor operated?	Agency
PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	7/21/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	On behalf of the Food and Drug Administration's (FDA) Center for Tobacco Products (CTP), RTI

International (RTI) will implement the Monthly Monitoring Study (MMS) – an electronic information collection subject to the Paperwork Reduction Act (PRA). The term study is used in this assessment instead of system. The purpose of MMS is to inform specified recommendations around FDA's public education programs' impact and effectiveness in reducing tobacco-related death and disease. MMS is needed to understand the trends in brand and device choices so that FDA can develop new media campaign messages related to tobacco products that resonate with youth and young adults ages 15 to 24 years old in the United States. MMS will collect primary data to monitor youth and young adult perceptions and emerging trends in brand and device use for Electronic Nicotine Delivery Systems (ENDS), little cigars and cigarillos (LCCs), and other tobacco products.

The study will be conducted using web-based cross-sectional surveys that are self-administered on personal computers or web enabled mobile devices. It will use online surveys to collect data from up to 27,000 youth and young adults ages 15 to 24 years to monitor perceptions about ENDS and other emerging tobacco products. The study will include questions about marijuana use to allow the study team to differentiate between use of current and emerging tobacco products and marijuana, which can be used in tobacco products such as ENDS and LCCs. The survey will take approximately 15 minutes to complete per participant. This survey will ask participants to provide feedback on tobacco use and quitting behavior, as well as brand and device preferences, tobacco information sources, peer influence and perceptions, and marijuana use. Respondents will receive a $5 incentive after completing the online survey.

To adhere to the Children's Online Privacy Protection Act (COPPA), RTI has a privacy policy that addresses the

collecting of data from minors under 13 as well as procedures to collect and store parental consent for the minor's personal information. The Institutional Review Board overseeing the study has waived parental permission for those ages 15 to 17 (or 15 to 18 in Alabama and Nebraska as required by state law). We ask youth respondents to provide assent of their own accord.

PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	Data collection for MMS will consist of an online screener and online cross-sectional survey. The following

personally identifiable information (PII) and potential PII about survey respondents will be collected by RTI (but will not be shared with FDA): (a) date of birth; (b) state; (c) zip code; (d) email address; (e) Facebook unique ID; (f) IP address; and (g) assigned unique study ID. Email addresses will be shared with the incentive provider, Creative Group, so that they can distribute incentives.

MMS will also collect the following non-PII data: (a) gender; (b) race/ethnicity; (c) sexual orientation; (d) marijuana and tobacco use; and (e) knowledge and attitudes about tobacco use.

The screener and surveys will collect PII and non-PII from respondents via their personal computer or mobile device. Respondents will click on an advertisement for the study in Facebook or Instagram (or other similar social media platform) to access the screener programmed and maintained by Qualtrics, LLC (a subcontractor to RTI) in their secure network server. All data stored on Qualtrics servers are encrypted at rest. RTI will download data from Qualtrics to an RTI server using an SSL (Secure Sockets Layer) connection.

All PII collected using the Qualtrics survey platform will be stored in the RTI server as one file in a share drive specific to the study that contains only PII including an RTI-assigned unique study ID. RTI will use the study ID to connect screener data and survey data and to determine if participants have completed the survey. Study IDs will not be shared with the participants but will be included in the survey data on the project share drive and the PII data that will be stored on RTI's secure server. The Facebook unique ID is assigned by Facebook to identify each account. Some Facebook users do not have an email address, but every Facebook user has a Facebook unique ID associated with their account. The Facebook

unique ID is necessary to identify potential duplicate respondents. IP address will be stored by Qualtrics and RTI in a second file that contains only IP address, the study ID, and the participant responses to the screener. Responses to the body of the survey will be stored as a third separate file. IP address and e-mail address will not be stored in this third separate file.

PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	MMS is a monthly cross-sectional study being conducted to inform specified recommendations around FDA's public education programs' impact and

effectiveness in reducing tobacco-related death and disease. MMS is needed to understand the trends in brand and device choices so that FDA can develop new media campaign messages related to tobacco products, such as ENDS and LCCs, that resonate with youth and young adults ages 15 to 24 years old in the United States. MMS will collect primary data to monitor youth and young adult perceptions and emerging trends in brand and device use for ENDS, LCCs, and other tobacco products.

Qualtrics is FedRAMP (Federal Risk and Authorization Management Program) approved as a software as a system (SaaS), as a Government Community Cloud deployment model. Qualtrics software is a standard survey builder tool. The software is owned and externally hosted by Qualtrics and provides users with the ability to generate and manage secure web-based surveys.

E-mail addresses and birth date will each be collected separately in the Qualtrics survey platform and stored in separate isolated files that will contain an RTI-assigned unique ID along with either the email address or birthdate. IP address will be collected in the survey platform in an isolated survey that contains IP address, RTI-assigned unique ID, and screener responses. Responses to the body of the survey will be collected in the Qualtrics survey platform and stored in an isolated survey. IP address, zip code, e-mail address, and birthdate will not be collected in the same file.

All four survey data files (IP address, e-mail, birthdate, and survey responses) will be downloaded separately from Qualtrics (which requires a password). The four files will be downloaded to the secure RTI study share drive and stored on the study share drive for no more than 24 hours after download. After 24 hours, the data are moved and stored on the FIPS 199 moderate network. RTI study staff will be given as-needed access to the data files on the share

during that 24-hour period to conduct fraud detection procedures, at which point data from the individual will be combined to check for fraudulent responses.

All information collected will be securely maintained on RTI's network servers for the duration of the study. RTI implements security and privacy protections in alignment with the NIST SP 800-53 Rev. 5
Security and Privacy Controls for Information Systems and Organizations controls to secure the network.

PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	E-Mail Address Date of Birth Mailing Address Others - Facebook unique ID, IP address, RTI-assigned unique study ID
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Public Citizens
PIA - 4:	For what primary purpose is the PII used?	The primary purpose for use of the collected PII is to effectively administer the survey: confirm study eligibility, ensure data validity, and track survey completion. Date of birth is used to confirm that respondents are eligible to participate in the study. State and zip code are used to confirm that respondents are eligible to participate in the study. Email address is used to prevent multiple responses from a respondent and to deliver incentives. Facebook unique ID is used as an additional measure to prevent multiple responses from a respondent and prevent fraudulent responses from bots (automated computer programs designed to complete the survey multiple times to earn incentives). IP address is used to block responses from outside the United States (that are typically from bots), prevent duplicate responses, and block responses from bots within the United States. Study ID is used to connect screener data and survey data, and to determine if participants have completed the survey.
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	The 2009 Family Smoking Prevention and Tobacco Control Act (Tobacco

		Control Act) (Pub. L. 111-31) amends the Federal Food, Drug, and Cosmetic Act (the FD&C Act) to grant FDA authority to regulate the manufacture, marketing, and distribution of tobacco products to protect public health and to reduce tobacco use. Section 1003(d)(2)(D) of the FD&C Act (21 U.S.C. 393(d)(2)(D)) supports the development and implementation of FDA public education campaigns related to tobacco use. Accordingly, FDA is currently developing and implementing youth-targeted public education campaigns to help prevent tobacco use among youth ages 11-18. FDA will use data collected from MMS to understand trends in tobacco product use and brand and device choices to inform development of public education efforts related to tobacco products that resonate with youth and young adults.
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Non-Government Sources Members of the Public
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	FDA is in the process of submitting the necessary documents for OMB review and approval. We will provide the OMB control number and expiration date once OMB issues a Notice of Action.
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 10A:	Identify with whom the PII is shared or disclosed and for what purpose	Private Sector
PIA - 10A	Explain why (and the purpose) PII is shared with each entity or individual.	The incentive provider, Creative Group, is provided email addresses to deliver

(Justification):		incentives to respondents who complete the surveys.
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Before answering screening questions, respondents will be informed that they will be asked questions to determine their eligibility. After completing the screener, respondents will read the youth assent or adult consent, depending on their age and state of residence. It will be displayed on their personal computer or mobile device informing them that personal information will be collected as part of the study. At the end of the assent or consent process, the respondent will click a radio button indicating they understand and agree or do not agree to participate.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	Participation in MMS is entirely voluntary. Respondents may choose to not take the survey, and are free to withdraw at any time, including while responding to the survey questions.
PIA - 14:	Describe the process to 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 original collection). Alternatively, describe why they cannot be notified or have their consent obtained	No such changes are anticipated. If FDA changes its practices regarding the collection or handling of PII related to this study, RTI will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. Because this study consists of cross-sectional surveys, past respondents' PII will not be included in any revised use of their data, and therefore RTI will not contact those respondents.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not	Individuals can use a variety of avenues to seek assistance with concerns about their PII. The consent and assent forms include a phone number which will allow them to reach

		the RTI project director. The screener introduction includes an email address to reach a helpdesk maintained by RTI. Requests received via the helpdesk will be routed to the appropriate member of RTI's data collection management team. RTI also monitors comments on the social media recruitment ads and can respond directly to concerns about PII by giving the commenter the appropriate contact information for the study. The consent and assent forms provide the mailing address, phone number, and email address for the Institutional Review Board which oversees protection of human subjects who participate in this research study. Individuals may also contact FDA's Privacy Office via contact information provided on FDA.gov.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	Respondent PII will be provided voluntarily by the individual. The individual will be responsible for providing accurate information. Accuracy will be ensured by individual review at the time of data review at the end of each wave of data collection. Respondent PII is relevant and necessary to participate in the survey. Access to PII by RTI staff and subcontractors will be granted and restricted at the individual level as appropriate to the individual's duties (role-based access). Integrity and availability will be protected by privacy and security controls selected and implemented in the course of providing the system with an authority to operate (ATO). Controls will be selected based on National Institute of Standards and Technology's (NIST's) guidance concerning the ATO process, appropriate to the system's level of risk as determined using the NIST's Federal Information Processing Standards (FIPS) 199.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Contractors Others
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA -17	

	Contractors: RTI requires access to prevent duplicate and fraudulent responses. RTI creates the unique study ID to connect screener and survey data and determine if participants have completed the survey. **Others:** Creative Group will receive email addresses of participants to distribute incentives.	
PIA - 17B:	Select the type of contractor	Third-Party Contractor (Contractors other than HHS Direct Contractors)
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	System roles are reviewed and authorized by project management and granted by the appropriate administrator. Role-based access controls are applied for all PII. Contractor system administrators for the project have role-based access to PII and utilize only the PII necessary to perform job duties identified with their role. Other RTI employees (i.e., project director, data collection task leader, programming task leader, programming team, data collection managers, data collection supervisors, data collectors, analysts) are provided with access to the secure project share to access PII or survey data to perform role-based programming, data management, data collection, analysis, and/or reporting job duties. Role-based access control is employed so that users only have "need-to-know" access to the data necessary to perform their job duties.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	The data collection system employs data access through the use of controls advised by NIST Special Publication

		800-53 that are deployed in RTI's network to ensure that access to any data is restricted by role. Unaffiliated with the project team, RTI Global Technology Solutions (GTS) maintains all role-based access controls independently from project staff. Inclusion of project staff users in role groups must be formally requested to RTI GTS and specifically approved by the RTI project director or project manager for any user to obtain access to systems or data. Membership in specific role groups allows specific access to specific data and/or systems. Role-based access to PII is limited to the information needed to perform specific tasks. Role-based access controls are in place and authorized only for individuals who are or were involved in processing and managing data collection production, and for contacting study participants for incentive distribution.
PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	RTI requires all personnel to complete company-wide, Information Security and GTS cyber awareness training before obtaining authorization to access RTI's information system. RTI conducts this training upon employment and a refresher course at least annually thereafter. Additionally, RTI provides company-wide Privacy Training that cover the same core components as the FDA privacy awareness training. Additional project-specific training on protecting the information being collected and maintained will be provided to the RTI project team. These staff members are also required to complete the Commitment to Protect Non-Public Information Employee Agreement (FORM FDA 3398 (10/10)).
PIA - 21:	Describe training system users receive (above and beyond general security and privacy awareness training).	Staff are required to sign a pledge regarding data security practices they are expected to follow while working remotely.
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	PII will not be collected or store by FDA. In accordance with Federal Acquisition Regulation (FAR) Subpart 4.7, RTI will

		retain all documents and data for at least three years after final payment of the contract, unless a shorter period is specified. For electronic data and materials, file deletion is the only practical method of destroying records stored on hard drives or share drives that will remain in service following destruction of the information. Any hard drive that previously contained sensitive information will be reformatted and then physically destroyed when it is taken out of service. Sensitive records will be kept in a secure location described in question 13 until destruction occurs. Appropriate measures will be taken to ensure the security and confidentiality of recorded information during all phases of the destruction process, including pickup and transport of records from RTI's locations to the destruction site. PII will be stored at RTI for 5 years after the project has ended unless FDA requests it be retained for a longer period. De-identified data will be stored on RTI servers and delivered to FDA at the end of each wave of data collection. No PII will be sent to, or accessible by, FDA at any time.
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	Administrative safeguards include user training; system documentation that advises on proper use; implementation

of Need to Know and Minimum Necessary principles when awarding access, and others.

Technical Safeguards include use of multi-factor access authentication, firewalls, and network monitoring and intrusion detection tools.

Physical controls include all system servers located in facilities protected by guards, locked facility doors, and climate controls.

Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199.