ATTACHMENT 12: PRIVACY AND DATA SECURITY

Privacy and Data Security: Point of Sale Intervention for Tobacco Evaluation (POSITEv)

Implementation of data security systems and processes will occur as part of the survey data collection. Data security provisions for the mail screeners, field screener, and in-person and online evaluation questionnaires will involve the following:

- All data collection activities will be conducted in full compliance with Federal regulations to maintain the privacy of data obtained on private persons and to protect the rights and welfare of human research subjects as contained in their regulations. Respondents will receive information about privacy protections as part of the informed consent process.

- All data collectors will be trained on privacy procedures and be prepared to describe them in full detail, if necessary, or to answer any related questions raised by respondents. Training will include procedures for safeguarding participant information in the field, including securing hardcopy case materials and tablets/laptops in the field, while traveling, and in respondent homes, and protecting the identity of participants.

- All project employees will sign a confidentiality agreement with RTI that emphasizes the importance of privacy and describes their obligations.

- Access to the file linking respondents' sample identification numbers and data with their contact information will be limited to project staff who have signed confidentiality agreements with RTI.

- Hard copies of mail screeners will be will be receipted and stored within RTI's Research Operation Center (ROC). The ROC facility has various controlled access measures including electronic doors locks that operate on either a pin or card access, controlled visitations policy and RTI onsite security officers during normal business hours. The camera systems are monitored directly by RTI's security console and alarm systems that are directly linked to the local police and fire stations. Discarded mail screeners will be securely shredded.

- All field staff laptops will be equipped with encryption software so that only the laptop user or RTI administrators can access any data on the hard drive even if the hard drive is removed and linked to another computer.

- Laptops will use the Microsoft Windows operating system and require a valid login ID and password in order to access any applications or data.

- The tablets will use the Android operating system and require a password/PIN to access any application or data.

- All data transferred to RTI servers from field staff laptops will be encrypted and transferred via a secure (SSL) broadband connection. Data will be passed through a firewall at RTI, then collected and stored on a protected network share on the RTI network. Only authorized RTI project staff members will have access to the data on the secure network share.

Following receipt from the field, PII will be stored only on RTI password protected, secured servers. All PII stored at RTI will be stored separately from questionnaire responses. In

addition, before it is transmitted from the field to RTI, PII will be stored separately from questionnaire responses on all laptops. Only authorized project members will have access to PII for research sample members.

Data security provisions for the optional smartphone app/geotracking portion of the study will include:

- The smartphone-based portion of the study will be a completely optional part of the evaluation. Participants can participate in the evaluation even if they do not have a smartphone or decline to participate in the app-based portion. The consent form for the app-based portion of the study clearly communicates the optional nature of the smartphone portion of the evaluation.

- Participants who choose to participate in the smartphone app-based portion of the study will first receive and be read a separate consent form that outlines the privacy and security procedures for this portion of the evaluation. Those who choose to participate will provide verbal consent.

- The subcontractor, Question Pro, who has developed the app underwent a data security and privacy review with RTI's Privacy Officer.

- The app developer will not have access to participants' identifying information.

- RTI will administer the incentives ($5 electronic gift card) for the app-based survey to participants so that the RTI, but not the app vendor, will have access to participants' e-mail addresses.

- Data obtained from the app-based component will be stored on a cloud server that meets federal requirements for data security and is managed by the app developer. Only the authorized app developer staff will have access to this data in the cloud.
- Data obtained from the app will be transferred from the app developer's cloud server to RTI's network server by a nightly process that executes at QuestionPro via the Secure File Transfer Protocol (SFTP), which encrypts the data in transit. Access to this folder is limited to QuestionPro and select RTI project members.

- We will collect contact information for respondents, including their mobile phone number and/or e-mail address if they consent to receive reminders to complete the app-based questionnaire via text and/or e-mail. Phone numbers will be stored on RTI's network server and only accessible to authorized staff. Once securely transmitted from the field to RTI, this information will be stored separately from data collected from the app and from the 4 waves of evaluation questionnaires. In addition, identifying information will be stored separately from questionnaire response on all laptops used for field data collection.

- The app vendor will only have access to an RTI-assigned case identification number to identify participants. Only RTI will have access to the file that links the case ID to participants' identifying information, and RTI project staff will only have access to this file as necessary.

- Data obtained by the app will be encrypted in while at rest on the tablet and while in transit to the QuestionPro (app vendor) cloud and the RTI SFTP folder.

- The app vendor will delete the data after RTI has confirmed that they have received their copy of the data and before the end of their subcontract with RTI.