ATTACHMENT 9: PRIVACY AND DATA SECURITY

Privacy and Data Security Issues related to the Evaluation of the Public Education Campaign on Teen Tobacco (ExPECTT)

Implementation of data security systems and processes will occur as part of the survey data collection. Data security provisions for the field test 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 sample member information in the field, including securing hardcopy case materials and laptops in the field, while traveling, and in respondent homes, and protecting the identity of sample members.

- All project employees will sign a privacy pledge that emphasizes the importance of privacy and describes their obligations.

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

- Hardcopy documents containing personally identifying information (PII) will be stored in locked files and cabinets. Discarded material containing PII 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.

- All data transferred to RTI servers from field staff laptops will be encrypted and transferred via a secure (SSL) broadband connection or optionally a secure telephone (land) line. Similarly, all data entered via the web-based survey system will be encrypted as the responses will be on a web site with an SSL certificate applied. 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.

  Web survey respondents will be given a unique user ID and password to access their survey, and in the event of a break-off, to resume the survey at a later date.

- Following receipt from the field, PII will be stored only on RTI password protected, secured servers. Only authorized project members will have access to PII for research sample members.

- CARI files recorded on the field tablets will be encrypted using AES-256 with cipher block chaining and PKCS5 padding (AES/CBC/PKCS5Padding) and our key. We use a 128-bit (max size) initialization vector (“IV”) that is filled with a hashed (via SHA-256) secure random. The random hashed IV allows us to encrypt the same string multiple times but produce a different cipher text for each occurrence. The encrypted audio files will be zipped up along with the survey response data and transferred to the project share on the internal network at RTI. They will then be decrypted using the private key for review by RTI quality monitors. Only authorized project staff will be able to access the CARI files.

- Audio files recorded during telephone interviews will be stored on a dedicated internal share. Only authorized project staff will be able to access and review the files.

- Data collected through telephone interviews (CATI) and the World Wide Web will be stored on secure RTI servers. Only authorized project staff will have access to the data, which will require passwords and the enabling of user access by RTI IT security personnel. The data will be stored in SQL Server databases which require an additional layer of security to access.