Data / Information Security Plan

This task order will complete a Security Assessment and Authorization (SA&A) process at the CDC. We will work closely with CDC to complete the SA&A, and will comply with all required standards and procedures throughout the life of the project. Elizabeth Gall at IMPAQ is the designated RSS team project coordinator for this process. Assisting her will be the IT specialists at IMPAQ and other Task Order team members.

The development and maintenance of all data management and storage systems for the RSS team will be the responsibility of IMPAQ International, since IMPAQ has pursued and achieved the level of data protection and security best suited for project requirements. Data collected in the field, both on paper and recordings, will be securely managed at RSS, IMPAQ, and Emory using conventions approved through the SA&A. To transcribe encrypted and password protected documents, RSS and Emory are prepared to use password protected computers and password protected networks or to use standalone computers not networked or connected to the Internet. Transcript data will be transmitted to IMPAQ by secure methods as agreed in the SA&A process. Options available include:

- Email of password protected transcripts that have been checked to ensure there is no PII.
- FTP uploads of password-protected transcripts that have been checked to ensure there is no PII.
- FedEx of batched password protected transcripts that have been checked to ensure there is no PII.

Coded and sorted analysis files will be sent to Emory and RSS as necessary, again following SA&A determined procedures. At Emory and RSS, those files will only be used on password-protected computers and password-protected networks or standalone computers not networked or connected to the Internet, depending on SA&A determination. Backup files will be encrypted and maintained on flash drives securely kept under lock and key.

Specific procedures on management of the information will be tailored to project needs, but the overall information system in which the information will be securely housed is described below in this plan.

IMPAQ is committed to ensuring the confidentiality, integrity and availability of all project data, as well as the privacy and confidentiality of any individuals represented in the data. The policies, procedures, and technologies IMPAQ employs to ensure the security and confidentiality of data are compliant with Federal Information Security Management Act of 2002 (FISMA) and Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. They have implemented a Security Program consistent with NIST SP 800-53. In addition, they will comply with all data security policies and

procedures referenced in the RFTOP at all times while working under this IDIQ contract and the procedures laid out in the SA&A.

IMPAQ has successfully and securely managed and stored sensitive research data for clients, including offices and agencies within DHHS, the Department of Labor, the Department of Education, and others. For the Centers for Medicare & Medicaid Services they have successfully stored and processed data sets consisting of tens of millions of individually identifiable healthcare claims records. IMPAQ has never had a data breach or other data-security incident.

All storage and processing of sensitive project data occurs on IMPAQ's FISMA-compliant enclave (The IMPAQ FISMA Enclave, or IFE). This network of servers is protected by a state-of-the-art router, firewall and intrusion detection and prevention system that is monitored. Formal configuration and change management procedures and tools are employed to ensure changes to IMPAQ's network systems are made in a controlled and documented manner and only after the security and performance implications of proposed changes have been carefully considered.

Based on guidance provided in NIST SP 800-37 rev.1, the Moderate security control baseline was selected for the development of IFE security controls. IMPAQ's systems log all PII-related access and extracts. IMPAQ information technology security personnel routinely review these logs for inappropriate activities and take corrective action. They will provide all pertinent security information to the NCHHSTP ISSO and Security Staff. CDC Certification and Accreditation documents will be sent to the CDC Chief Information Security Office (CISO) for review, approval and subsequent issuance of an Authority to Operate (ATO). IMPAQ will work with the NCHHSTP Information System Security Officer as a part of the Certification and Accreditation (SA&A) process on the initial determination of the overall security category. All SA&A documentation will be submitted to the CDC Chief Information System Officer.

IMPAQ has experience with accessing CMS's and other Federal agencies' information systems and, if required by CDC, they will ensure secure integration with CDC Network Infrastructure. If any PII or other sensitive project data is disclosed inadvertently or is at risk of disclosure due to a lost, missing, or intercepted transfer, IMPAQ will follow its Incident Handling and Privacy Policies to report to designated CDC staff immediately. Any and all breach events will be documented and provide follow-up reports to the COR. IMPAQ holds privacy notification insurance with the Chubb Insurance Group.

Below we describe IMPAQ's qualifications and compliance with the seven security areas listed in the RFTOP for this Task Order.

Position Sensitivity Designation. All prospective IMPAQ employees must pass a criminal background check as a condition of employment.

Privacy Compliance. IMPAQ, in conjunction with CDC Center ISSO, will conduct and maintain an initial Privacy Impact Assessment (PIA) as defined by Section 208 of E-Government Act of 2002. IMPAQ will also ensure that periodic reviews of the PIA, determining if a major change to the system has occurred and if an update is needed, will take place.

Offeror's Official responsible for Information Security. IMPAQ's Director of IT Operations & Support, David Denbow, will be responsible for all information security requirements.

Rules of Behavior. IMPAQ's information technology procedures are consistent with the HHS Information Technology General Rules of Behavior (HHS RoB). IMPAQ will ensure that all project staff comply with the HHS RoB (http://www.hhs.gov/ocio/policy/2008-0001.003s.html).

Information Security Training. IMPAQ personnel are trained in their applicable roles and duties. Training occurs annually or as significant changes to the system are implemented. All IMPAQ team employees and potentially subcontractors will complete the HHS Computer Security Awareness Training course, or any other course designated by CDC, before performing any work. Thereafter, all employees and subcontractors will complete an annual HHS-specified refresher course during the life of this contract. All IMPAQ executives and research personnel annually complete the FISMA-compliant, Federal information system security awareness training provided online by Department of Defense at http://iase.disa.mil/eta/iss_icv5/.

HSPD-12 Compliance. IMPAQ utilizes dual-factor authentication process for accessing its IMPAQ FISMA Enclave. All users need to provide two means of identification, one of which is username and password and the other of which is a security token. If directed by CDC, IMPAQ will include FIPS 201-compliant card readers with workstations, laptops and servers purchased for the project, and will comply with FAR Subpart 4.13, Personal Identify Verification.

Encryption. All data stored on IMPAQ's network are encrypted. Our encryption mechanisms comply with FIPS 140-2 requirements. For the transfer of project data to or from IMPAQ we utilize an internally managed secure file transfer server running a FIPS 140-2 compliant encryption module. All volumes containing PII data are encrypted at the drive level as well. This Task Order will not keep any PII electronically.

Secure Web Conferencing System for Remote Communication. IMPAQ utilizes Microsoft Lync, an enterprise communication platform that provides a single interface for business communication including Web conferencing, instant messaging (IM), VoIP (voice over IP), file transfer, and voice mail. It can be used for collaboration within a single organization, between multiple organizations, and with external individuals. It is supported on a wide variety of electronic devices including PCs, MACs, IPhones, IPADs, and android devices.

Microsoft Lync supports the creation and use conferences so that web meetings, voice calls and instant messaging can be established for the entire group at the touch of a single button. Lync

web conferencing enables participants located anywhere around the world to join a live meeting at a moment's notice via an internet connection.

Microsoft Lync web conferences or meetings are organized in a number of ways;

- For participants within the same organization, invites are sent by selecting participant names from the company's email address book. They have the option to connect using a web browser or Lync client.
- For external participants, invites are sent to their email addresses with a link to connect to the meeting. External user can connect using a browser or have Lync client installed (it is a free download for PCs, IOS and Android)

Lync communication is secured using SSL and 256-bit Advanced Encrypted Standard (AES). It also uses TLS over SIP traffic and SRTP for media such as audio, video and desktop sharing. This makes it very difficult for an attacker to intercept or interfere with information during the time of a conversation. IMPAQ International stores recorded information from a Lync meeting in a FISMA compliant network environment and data confidentiality is maintained according to HIPAA policies.

IMPAQ provides 24/7 IT support to employees and meeting participants to ensure remote user devices are quickly set up and configured for smooth and uninterrupted web meetings. Microsoft Lync is supported on several computing platforms including windows, Android and IOS.