Appendix G – Baseline Security Requirements

To ensure the quality, reproducibility, and appropriateness of our data management and analyses, Abt programmers and analysts follow standard industry practices. This includes guidelines surrounding data security, reproducibility, documentation, code review, and coding style. We also create project-specific data management guidelines that address any security or human subjects concerns pointed out by the client or Abt's IRB.

Abt will ensure this project has a data security plan with adequate provisions to protect the privacy of subjects and the confidentiality of their information. Abt has a highly visible, coordinated Information Risk Management (IRM) program to ensure project teams have the training, knowledge, tools, and resources required to protect sensitive data, including data subject to data use agreements. Abt's IRM includes representatives from Contracts Operations, Abt's Client Cybersecurity Center, and IRB. In reviewing confidentiality protections in the data security plan, Abt's IRM will consider the nature, probability, and magnitude of harms that would be likely to result from a disclosure of collected information outside of authorized recipients. The Director of Abt's Client Cybersecurity Center ensures that technical safeguards (e.g., data transfer, encryption, access controls, and destruction methods) are compliant with requirements of regulations, the contract, and any data agreements.

Incident Response

Abt has developed Information System Security Plans (ISSP) and completed the Security Assessment and Authorization (SA&A) process with multiple federal agencies, including HRSA, to receive authorization to operate in their respective enterprise environments. In addition, Abt has received authorizations to operate (ATO) "low-" to "moderate-" risk category information systems in other environments and has recently received an ATO for two HRSA projects, IM-COIIN for the Maternal and Child Health Bureau (low), and the Ryan White Chart Abstraction project for the HIV/AIDS Bureau (moderate). With our understanding of HRSA and the project's security needs, Abt can decrease the time from contract award to accreditation. This also reduces the security cost and leaves more funding for innovative research solutions.

To develop the ISSP and core of Abt's information security program, we have used the following key federal guidelines, standards, and publications, and supporting policies and procedures:

- OMB Circular A-130 and specifically Appendix III;
- OMB Memorandum M-06-16 – Protection of Sensitive Agency Information
- FIPS 199—Standards for Security Categorization of Federal Information and Information Systems;
- FIPS 200—Minimum Security Requirements for Federal Information and Information Systems;
- NIST SP800-18—Guide to Developing Security Plans for Federal Information Systems;
- NIST SP800-37—Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP800-53 (rev.4)—Recommended Security Controls for Federal Information Systems and Organizations;
- NIST SP800-60—Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations;
- NIST SP800-88 – Guidelines for Media Sanitation;
- NIST SP800-61—Computer Security Incident Handling Guide; and
- NIST SP800-63—Electronic Authentication Guideline.

Abt has integrated multiple security approaches to securing client data. First, we focus on the network where we block Personally Identifiable Information (PII) received through email, a major source of incidents

for many companies. Abt is very aware of the reporting timelines for incidents as defined by the contract and the US Computer Emergency Readiness Team (USCERT). Our incident response capability is designed to meet these requirements and we will collaborate closely with AHRQ during any incident.

## Secure Data Storage

Abt is extremely conscious of the need to protect the confidentiality, integrity and availability of sensitive data and is well aware of government laws and regulations such as Federal Information Security Management Act (FISMA) of 2002 and the Privacy Act of 1974. For over four decades, we have conducted numerous projects involving sensitive information; through this experience we have developed the facilities and procedures to maintain the confidentiality of data entrusted to us. Abt has a documented incident response plan developed in accordance with NIST SP800- 61, a system security plan in accordance with NIST SP800-37 and SP800-53, and a risk management strategy in accordance with NIST SP800-30. For any cloud services that store or transmit Federal data, Abt uses services that have completed the FedRAMP process; e.g. AWS.

Access to sensitive areas is controlled. Project Directors are required to formally authorize access rights to sensitive data based on a person's job requirements. Data integrity and confidentiality are enforced by procedures based on authorization, authentication, and least-privilege access to prevent unauthorized changes or access to data files. Project directories and databases are protected by assigned group memberships, passwords and other techniques which prohibit access by unauthorized users. All employees and contractors working on this effort will be required to understand and follow these guidelines. In addition to the issue of protection of privacy, data security includes backup procedures and other file management techniques to ensure that files are not inadvertently lost or damaged. Project data files are backed up to enterprise tape libraries. The full backups are sent off-site for storage at industry leading storage facilities. The procedures currently utilized at Abt Associates ensure the privacy and security of Abt Associates' research databases, project documents and notes, and all data collection activities. Laptops have full drive encryption and data transfers occur using a secure file transfer server that uses a FIPS 140-2 certified module.

## Compliance with HHS and Federal IT Policies

As outlined above, the Abt Team will align all work with current HHS and AHRQ policies, as we have throughout our long history of supporting AHRQ and its programs. We will also ensure that all materials to be posted online are 508 compliant. Our team has worked closely with AHRQ IT and Security teams on the ATO process for several projects. Scheduling is critical to obtain approvals for strategy, architecture, and hosting environment. Abt also complies with the Privacy Act of 1974, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the EGovernment Act of 2002, including Title III: Federal Information Security Management Act (FISMA), which covers site security, security control documentation, access control, change management, incident response, and risk management. Abt uses the publications in the NIST Special Publication 800 series (including SP800-53 and SP800-37) as a blueprint for our policies and procedures, as well as the Information System Security Plan (ISSP), and Plan of Action and Milestones. Abt has also successfully complied with client requirements for a System of Records Notice (SORN) and a Privacy Impact Assessment (PIA).