SOCIAL DYNAMICS
Bringing Complex Issues Into Focus

Social Dynamics, LLC
481 North Frederick Ave., Suite 410
Gaithersburg, MD 20877
Phone: (301) 990-1105
www.socialdynamicsllc.com

There are five components of the DEI Evaluation data security protocol. Sections 1 through 3 of this memorandum summarize each component and the responsibilities of each organizational partner in maintaining, updating and implementing data security procedures. Section 4 and 5 summarize the DEI Rounds 5-6 administrative data elements that are required for each LWIA treatment site.

1.0 Secure Network

Altarum Institute maintains the Altarum Secure Network (ASN), which is used to upload and store DEI data. Altarum Institute is located in Ann Arbor, MI and has been responsible for DEI data security since 2010. The ASN has been assessed to be within 98 percent compliance of the National Institute for Standards and Technology (NIST) Special Publication 800-53 Revision 3 guidelines, and has been qualified for storage of such data. The ASN-supported DEI Data System provides the administrative processes to store, protect, and access Personally Identifiable Information (PII) in a controlled manner that complies with all privacy act and HIPPA regulations.

On a quarterly basis, each DEI state transmits workforce data to the ASN by secure file transfer protocol (SFTP). Data files are submitted via SFTP as an encrypted, compressed, delimited text file that includes headers. Altarum works with each state to establish user accounts for the ASN by sending the information necessary via encrypted email, to establish user accounts on the ASN. Authorized state personnel have access only to the data upload system. Data cannot be downloaded from the SFTP at any time. At the conclusion of the DEI evaluation, all data will be destroyed or returned according to each state's Data Sharing Agreement requirements.

2.0 Team Member Access to PII

Altarum Institute is the *only* organizational team member that has access to workforce (e.g. WIASRD and Wagner-Peyser) data PII. DEI workforce data files containing PII are processed by Altarum on a quarterly basis. In 2020, at the conclusion of Round 5, Altarum will submit the PII that is included in the DEI state quarterly extracts to the United States Social Security Administration (SSA). SSA will facilitate a match of the DEI PII to the SSA disability program database. Once the SSNs are matched to the SSA database, all PII will be removed by Altarum so that Social Dynamics and Abt Associates can complete the final analysis of program impact and implementation. At *no time* will Social Dynamics or Abt Associates hold workforce data PII.

2.1 Data Security at Abt SRBI

Abt SRBI is tasked with conducting the survey of disability categories and activities of daily living for comparison group individuals and treatment group individuals that have not completed this information in their hardcopy form profile. To do this, Abt SRBI will have access to first and last names and telephone numbers of individuals that will be asked to participate in the survey. Social Dynamics, Abt Associates, and Altarum Institute will not have access to this information. As with Altarum Institute, Abt SRBI has a stellar reputation for data security.

Abt SRBI collects data for Federal, state and local governments, universities, and commercial and non-profit organizations and maintains strict data security and confidentiality procedures to protect the personal information of all sample members. Abt SRBI frequently handles PII including social security numbers, birthdates, and health information for federal clients including the Centers for Medicare and Medicaid, Veterans Administration, Internal Revenue Service, and Social Security Administration, to name a few. Abt SRBI systems are designed to maintain data security throughout the entire data collection process. All Abt SRBI data collection servers are housed in co-location in an AT&T Datacenter in Secaucus, New Jersey. The co-location has redundant power, expandable bandwidth and a high level of physical security. All data collection servers are virtualized using VMware virtualization platform, and all data is processed and stored on a FIPS 142 encrypted Storage Area Network (SAN). The co-location is a hardened facility with many levels of security for protection of hardware and data. The facility is monitored 24 hours, 7 days a week by on-site professional security guards and monitored over continuous closed circuit video surveillance from a command center via both stationary and 360° cameras located both outside and inside the facility.

2.2 Data Security Training

Abt SRBI staff are trained in data security and confidentiality issues. Project management staff regularly complete data security and ethics and compliance training, and receive a certificate for successful completion. Interviewers are briefed on confidentiality and security issues as part of their basic training, and those working on sensitive projects like CHS are also trained on data security features of the servers that house the CATI project files. CHS project management staff and interviewers also sign a confidentiality pledge. Abt SRBI adheres to the privacy and confidentiality policies of the Association of American Public Opinion Researchers (www.AAPOR.org) and the Council of Survey Research Organizations (www.CASRO.org). Both of the organizations have a code of professional ethics and practices to which we adhere.[1] We also include our confidentiality statement on our Website.[2]

3.0 Destruction or Return of Data to Each DEI State

Upon completion of the DEI evaluation in 2021, Social Dynamics will use the de-identified data set that was used for the analysis of program impact to create a public use data file. Altarum will then destroy or return the original extract files submitted by DEI states and submit a certification of such action to each state principle agency for the DEI grant. Destruction of the extract files and submission of the certification will be made according to each state's DSA and point of contact. The written certification shall attest to the destruction of the dataset and all copies thereof, not including the de-identified analysis file, and shall be accomplished within 180 days of completion of the evaluation as determined by DOL's acceptance of the final report.

---

[1] http://www.aapor.org/AAPORKentico/Standards-Ethics/AAPOR-Code-of-Ethics.aspx;
http://www.casro.org/?page=thecasrocode
[2] http://www.srbi.com/Contact-Us/About-Surveys/Survey-Confidentiality.aspx