Attachment L:

Information Security Plan

NIOSH adheres to all Federal, HHS, and/or CDC IT security policies and procedures. CDC/IT security procedures implement the Federal Information Security Management Act of 2002 (P.L. 107-347) (FISMA) (http://csrc.nist.gov/policies/FISMA-final.pdf). These policies and procedures protect federal information and federal information systems in order to protect confidentiality, integrity, and availability of the study data and include the implementation of technical, administrative, and operational safeguards. Where:

- integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- and availability means ensuring timely and reliable access to and use of information.

The requirements described below apply to both NIOSH employees and potential contractors. The term “information technology (IT)”, as used in this document, includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Physical data security procedures:

Only staff whose services are required to complete the project are granted access to the data. All CDC researchers, staff and in-house contractors are required to complete information security awareness training before access is granted to CDC computers. An annual refresher is required in order to maintain access to CDC computers. The safekeeping of sensitive data and the Privacy Act are included in the training. Employees and contractors agree to the rules of behavior, including non-disclosure, following the training.

The project shall comply with the HSPD-12 requirements contained in “HHS-Controlled Facilities and Information Systems Security. “The building in which the data are housed is a limited access facility with guards, fences, and security cameras. Hardcopy output will be physically controlled while in use and securely stored when not in use. Data files are to be stored on the CDC network which has strict physical access controls. User access to the network is restricted to badged users with strong password or PIV enabled authentication. Any portable media on which data may be stored during transportation are encrypted with FIPS 140-2 compliant software. Non-record media are sanitized in accordance with federal standards and policies.

Personally identifiable data will be protected at NIOSH in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and the Privacy Act SORN 09-20-0147, "Occupational Health Epidemiologic Studies", http://www.cdc.gov/od/science/regs/privacy/systemNotices/09-20-0147.htm.

Access to study data is granted to CDC employees and contractors who are supporting the study, have passed background checks, have taken security training, and have signed non-disclosure agreements. Annual refresher training is required in order to maintain access to CDC computers. The safekeeping of sensitive data and the Privacy Act are included in the training. CDC facilities in which data are stored are limited access facilities, have 24 hour guard service, fences and security cameras. Electronic data are only accessible to approved users and are stored on a file server in a limited access room in a secured building. When data transfer is required for data collection activities, such as matching with cancer registry, the data transfer will be protected by encryption that meets Federal standard. All data reporting will be carefully reviewed for small cell size to avoid the risk of inadvertent data disclosure.

Analysis files will not include personal identifiers. Direct identifiers will not be published. Small cell size statistics will be reviewed to assess the potential for re-identification. Corrective actions such as further data collapse or data suppression will be taken as necessary.

Additionally, NIOSH shreds paper records prior to disposal in accordance with federal standards. PID records are destroyed using cross-cut shredders or shredders meeting a stricter standard. Media are sanitized prior to disposal or reuse including secure wiping, degaussing, or physical destruction as appropriate for the media.

Record retention policies:

It is our policy to keep the original data (NIOSH Master File) on which our studies are based for 75 years in the event that questions are raised about the original study or we decide to update the study at a later date. The 75-year retention period has been incorporated into section 2-79 (NIOSH Epidemiologic Studies) of the CDC records management policy. This policy ensures the creation and maintenance of complete and accurate records of its programs and activities and ensures the efficient and economical management of all records in compliance with 44 U.S.C. 2901. However, NIOSH electronic records are governed by section 4-53 of the CDC Records Management policy which requires permanent retention of "study data files", but only "90 days after all data from them (source files) has been entered onto a master file and verified, or when no longer needed to support the reconstruction of, or serve as the backup to, the master files, whichever is later". Additionally, NIOSH shreds paper records prior to disposal in accordance with federal standards. PID records are destroyed using cross-cut shredders or shredders meeting a stricter standard. Media are sanitized prior to disposal or reuse including secure wiping, degaussing, or physical destruction as appropriate for the media.