Privacy Act Checklist

Develop a brief narrative answering the following questions:

- Does the data collection involve collecting sensitive and/or personally identifiable information?

Yes. The data collected contains personally identifiable information.

- Describe how personal information will be maintained (i.e., locked file cabinet, on computer, etc.) and who will have access to it (employees only, contractors, etc.).

Authorized Users

A database software security package is utilized to control access to the system. Access is granted to only a limited number of scientists and designated support staff and contractors, as authorized by the system manager to accomplish the stated purposes for which the data in this system have been collected.

Physical Safeguards

Hard copy records are kept in locked cabinets in locked rooms (or equivalent safeguarding). Guard service in buildings provides screening of visitors. Computer work stations and automated records are located in secured areas.

Procedural Safeguards

Data sets are password protected and/or encrypted. Protection for computerized records includes programmed verification of valid user identification codes and passwords prior to login to the system, mandatory password changes, limited log-ins, virus protection, and user rights/file attribute restrictions. Password protection imposes user name and password log-in requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures and Vault Management System for secure off-site storage is available for backup tapes. Additional safeguards may be built into the program by the system analyst as warranted by the sensitivity of the data.

- State how long the sensitive and/or personal information will be maintained. This information is crucial. If sensitive information is maintained for even one day, the Privacy Act will apply and we will have to provide language in the clearance package.

Program records are transferred to the Federal Records Center 15 years after the case file becomes inactive and are destroyed after 75 years. Paper files that have been scanned to create electronic copies are disposed of after the copies are verified. Disposal methods include erasing computer tapes and burning or shredding paper materials.

- For Extensions and Reinstatements only: Data management procedures have not changed since previous approval and the instruments have not been through extensive revisions.

This is a request for an extension of an existing approved information collection activity. Data management procedures and data collection instruments have not been changed significantly since the previous approval.

- Ensure that the consent documents/advisements contain the following information: authority for collecting the data; purpose of collecting the data; with whom the identifiable information will be shared; voluntary nature of the information collected; effect upon respondent for not participating.

The system notice for system 09-20-0147, "Occupational Health Epidemiological Studies, EEOICPA Program Records and WTC Health Program Records, HHS/CDC/NIOSH." describes routine uses for the data collected under this program. The advisement information is found on the second page of each telephone interview questionnaire in Attachment C.