Appendix C

Access Controls

Technical Controls

- User Identification
- Passwords
- Firewall
- Encryption
- Smart Cards

Physical Controls

- Guards
- Identification Badges
- Key Cards

Administrative Controls

1. What is the system security plan (or will there be a security plan) for this information collection?

The Katrina-Rita Pilot Registry files will be maintained as two separate files—one with and one without personal identifiers. All data collected by the contractor will be returned to the Surveillance and Registries Branch (SRB), Division of Health Studies (DHS), ATSDR (Atlanta).

ATSDR staff members are trained in the proper procedures to ensure strict confidentiality. Staff members who have access to the registry data files are required to complete and submit the appropriate forms in accordance with published U.S. Department of Health and Human Services (DHHS) regulations. Summary data and data without personal identifiers will be released for public use. No data with personal identifiers are released except for the releases permitted by the written consent of registrants for the express purpose stated in the signed consent form.

Creation and Maintenance of Files

Quality control procedures will be executed to ensure compliance with file definitions and specifications. If additions are being made to an existing file, the record is matched to the master registry listing to determine the status of the record (that is, whether it is a new or an existing record); if an existing record is located, both records are reviewed to assess any additions, changes or deletions. When the registry file is updated by additions, changes, or deletions to an existing file, copies of all such actions are kept as an audit trail for the file.

Access to the data will be closely controlled and restricted to authorized users--only designated SRB staff located at ATSDR, using password-protected, network-connected personal computers, will have the capability to retrieve all of the information contained on the files.

There will be a written data security policy and procedures that will be enforced by the registry's principal investigator. These policies and procedures will apply to such things as controlling data access (through restriction to authorized users with valid accounts and passwords) and procedures for deletion or purging of registrants who opt not to participate in the registry after the enrollment phase.

All personnel, including contractors, dealing with contact [identifying] information about registrants will be required to sign a confidentiality agreement that will specify penalties for unauthorized use or release of data from the registry.

2. What is the contingency (or backup) plan for this information?
Strict enforcement of the original plan.

3. How frequently will the files be backed up?
Daily (every 24 hours).

4. Where will the backup files be stored? Onsite? Offsite?
File Transfer Protocol (FTP) will be used to transfer files between the contractor and SRB staff. The objectives of FTP system are to share files (computer programs and/or data) electronically and as a way to promote consistency and uniformity in file storage. The backup files will be stored on the FTP server and accessible both on and offsite.

5. Will there be user manuals for this information collection?
Yes. Interviewer Manual, Supervisor Manual, Data Procedures Manual

6. How will personnel (principal investigator, managers, operators, contractors and/or program staff) using the system be trained and made aware of their responsibilities for protecting the information being collected and maintained?
Prior to data collection, all staff and contractors will be trained on security and confidentiality policies and procedures.

7. If contractors operate or use the system, will the contracts include clauses ensuing adherence to privacy provisions and practices?
Yes

8. Will methods be in place to ensure least privilege (e.g., access is "role based" on a "need to know" basis and is there accountability? Specify other method(s).
Access to the data will be closely controlled and restricted to authorized users (staff working on the registry only) with valid accounts and passwords. There will be a written data security policy and procedures that will be enforced by the registry's principal investigator.

9. Are there policies or guidelines in place with regard to the retention and destruction of IIF? Provide some detail about the policies/practices applicable to this specific data collection, and add at the conclusion:

The data will be collected by a contractor and maintained in-house. Access to the data will be closely controlled and restricted to authorized users (staff working on the registry only) with valid accounts and passwords only. One of the linked tables within the database will hold all unique person identifiers, demographics, employer, occupation, and relevant occupational history.

This information will be maintained for a finite number of years and will be destroyed in accordance with specific termination rationales. The criteria for termination are:
(1) The hazardous substance of interest is no longer used or manufactured or no longer found at dump sites, and all registrants are deceased; an exception may be made when the contaminant is thought to have the potential for causing multigenerational effects; and
(2) The hazardous substance is determined through further study to cause no adverse health outcomes. If either of these conditions is met, the registry will be considered for termination. Before a decision to terminate a registry is made, ATSDR will discuss this action with the appropriate state and local health authorities, the registrants, and other appropriate parties at all phases of the decision-making process. When the registry is terminated, surviving registrants are notified of the termination, the rationale for the termination, and the implications for them.

Records will be retained and destroyed in accordance with the applicable CDC Records Control Schedule. http://aops-mas-iis.od.cdc.gov/Policy/Doc/policy449.htm