February 2010

Children's Environmental Health Network

RECORD RETENTION AND DOCUMENT DESTRUCTION POLICY

The Children's Environmental Health Network ("CEHN") acknowledges its responsibility to preserve information relating to litigation, audits and investigations. The Sarbanes-Oxley Act of July 30, 2002 (18 U.S.C. Section 1519), makes it a crime to alter, cover up, falsify, or destroy any document to prevent its use in an official proceeding. Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against CEHN and its employees and possible disciplinary action against responsible individuals (up to and including termination of employment).

CEHN shall retain records for the period of their immediate or current use, unless longer retention is necessary for historical reference or to comply with contractual or legal requirements. Records and documents outlined in this policy include paper, electronic files (including e-mail) and voicemail records regardless of where the document is stored, including network servers, desktop or laptop computers and handheld computers and other wireless devices with text messaging capabilities.

CEHN shall not knowingly destroy a document with the intent to obstruct or influence an "investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States . . . or in relation to or contemplation of such matter or case." If an official investigation is underway or even suspected, document purging must stop in order to avoid criminal obstruction.

In order to eliminate accidental or innocent destruction, CEHN has the following document retention policy:

Type of Document	**Retention Period**
Accounts receivable and payable ledgers and schedules	7 years
Annual audited financial statements, audit reports, general ledgers, internal audit reports, trial balance journals	Permanently
Articles of Incorporation, Charter, Bylaws, minutes and other incorporation records	Permanently
Bank Reconciliation	3 years
Bank Statements, deposit records, electronic fund transfer documents, and cancelled checks	3 years
Chart of Accounts	Permanently
Contracts, mortgages, notes and leases (still in effect)	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Correspondence (general)	3 years

Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Depreciation schedules	Permanently
Employment applications	3 years from making the record or taking the personnel action
Garnishments	7 years
Insurance policies, records, current accident reports, claims (still in effect)	Permanently
Insurance policies, records, accident reports, claims (expired)	3 years
Inventory records	7 years
Invoices (to customers, from vendors)	7 years
Loan documents and notes	Permanently
Personnel files (employee demographic information and compensation records)	7 years
Personnel files (I-9's)	7 years after date of hire or 1 year after termination
Personnel files (payroll records and summaries including records related to employee's leave)	7 years
Personnel files (terminated employees)	7 years after termination

Retirement and pension records including Summary Plan Descriptions (ERISA)	Permanently
Tax Returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Workers Compensation documentation	10 years after 1st closure

APPENDIX A

Children's Environmental Health Network
Scientific Data Management, Storage, Retention, and Disposal Policy

Data Collection: Data are collected in a format appropriate for the task assignment. Most data are collected on paper forms in the field or the office. For certain tasks or subtasks, data may be collected directly in an electronic format. Project Managers are responsible for maintaining a written protocol for the collection and chain of custody for the data for each task within a project and for managing the data collection process.

Each data collection form includes a personal identifier and a study identifier. If the primary object for a task is a housing unit, the personal identifier is the street address for the unit, and the study identifier is a separate, unique alphanumeric code. If the primary object for a task is a person, the personal identifier is the person's name, and the study identifier is a separate, unique alphanumeric code. Signed informed consent forms are obtained before participants or subjects provide personal data needed for non-exempt research purposes. Project Managers are responsible for ensuring that all staff and contractors adhere to confidentiality agreements specific to the project.

Data Entry: Data that are collected using paper records are data-entered onto an electronic format compatible with the client's requirements. Project managers are responsible for ensuring that quality control activities are developed and implemented so that all necessary paper records are accurately transferred into an electronic format. When applicable, data collected in an electronic format are transferred to another electronic device (e.g., from PDA to computer network) for temporary and long-term storage.

Temporary Electronic Storage: Electronic records are stored on a computer network or personal computer that is password-protected. Records are backed up daily and are maintained in an offsite location. Records are also routinely backed up on a magnetic tape or disc and kept in a secure onsite location. Computers are maintained in secure areas, with access limited to authorized personnel. Electronic files are maintained on the computer network or personal computer until all task assignments are completed for a particular project/task order.

Temporary Paper/Materials Storage: Paper records and project-related materials include hardcopies of hand-completed data collection forms, project photos, personal communication records (e.g., memos, copies of e-mails), site visit records, training records, etc. Such materials are to be maintained by the Project Manager/Task Leader in locking file cabinets, with study data records kept in cabinets separate from non-data project documentation. For most projects, study data records are filed and retrieved by study code (e.g., a building ID), although for some projects, records are filed and retrieved by street address or participant name. During the data collection period, one or two filing systems may be maintained: one by the contractor or partner organization in the field and, as needed, and second by the Project Manager. The second filing system is especially needed when the CEHN office is responsible for data entry. At the conclusion of the data collection period, paper records in the field are generally shipped to CEHN or

destroyed. For some projects, a partnering organization (e.g., a local HUD grant recipient may have an ongoing need for the records) and may sign a written agreement to retain some or all of them. When records will be maintained by the partnering organization, CEHN will document the procedures in the confidentiality agreement for the task. Filing cabinets are all maintained in secure areas, with access limited to personnel authorized by the Project Manager. Files may be maintained in specified temporary location during the project, and for one year after the project is completed, unless the project contract provides for a different time period.

Record Access Procedures: For each project with personally identifiable information, a confidentiality agreement is established near the start of the project, delineating who is permitted access to the data containing personally identifiable information. In general, access to such records is limited to the study participant, research staff/contractors, and data collection personnel. In some cases, certain data may need to be publicly available due to legal mandates. Partnering organizations may also require that they maintain full access to all data. Under certain contracts, the client may require that they have access to the personally identifiable data.

A public use dataset may be a deliverable for a project. The creation of such a dataset includes the removal of personal identifiers and other data (e.g., phone numbers) that would allow a user to identify participants. A data dictionary that describes the variables and variable names as well as full documentation describing the data collection methodology accompanies the dataset. Datasets are most commonly prepared in SAS.

Notification Procedures: For studies or evaluations, participants are notified of their personal results in writing in a timely manner following verification and quality control and quality assurance procedures. If the results suggest that a participant is at immediate substantial risk, the Project Manager shall ensure that the participant is notified as quickly as possible, following verification, and advised on where to go for assistance, such as a local health department. Participants are also notified that they can receive a copy of the full research report upon request. Hardcopies of notification letters are maintained in the project file.

Final Retention and Disposal: The Project Manager confers with the client about specific regulatory/contractual requirements concerning the minimum or maximum length of data retention, the format of data storage, and the location of data storage. In the absence of such requirements, the following procedures are to be used:

- Long-Term paper storage: After a project is complete, and all deliverables have been provided to the client, all data collection instruments and forms are indexed by file, boxed, and transferred to a secure location either on- or offsite. If offsite, the location must be managed by a contractor specializing in document storage. Records are retained at the secure location for seven years from the date of the last data collected, unless a different time period is specified in the contract or grant agreement. For some studies, a research oversight committee or Institutional Review Board may require the personal identifiers are redacted prior to long-term storage. At any time while the data are in long-term storage, the client may request that the data (redacted or unredacted,

depending on the client's authorization as described in the confidentiality agreement) be transferred. Seven years after the anniversary date of the end of the project, the Project Manager has the discretion to dispose of the files at any time. If the files are unredacted, the documents are disposed of in a manner that assures confidentiality is maintained, e.g., files with personal identifiers can be shredded.

- Long-term electronic storage: After the project is complete and all deliverables have been provided and approved by the client, the electronic files (including personal identifiers) are retained onsite on magnetic tape or disc with the paper records in a locked filing cabinet in a secure area. A copy of the electronic file is provided to the Project Manager, who must keep the second copy in a secure locked location. All electronic files on the computer network or personal computer are removed. If the client is authorized to maintain the personally identifiable data, the client may request a copy of the data for up to seven years after the closeout of a project. After seven years, the Project Manager has the discretion to destroy the electronic files at any time. The electronic link between data and personal identifiers shall be destroyed. (Note: The public use dataset is a public record and will not be destroyed.)