purpose of the research project, unless the recipient has presented adequate justification of a research or health nature for retaining such information, and (3) make no further use or disclosure of the record except (a) in emergency circumstances affecting the health or safety of any individual, (b) for use in another research project, under these same conditions, and with written authorization of the Department, (c) for disclosure to a properly identified person for the purpose of an audit related to the research project, if information that would enable research subjects to be identified is removed or destroyed at the earliest opportunity consistent with the audit, or (d) when required by law; (D) has secured a written statement attesting to the recipient's understanding of, and willingness to abide by these provisions.

- 4. The Department contemplates that it will contract with a private firm for the purpose of collating, analyzing, aggregating or otherwise refining records in this system. Relevant records will be disclosed to such a contractor. The contractor will be required to maintain Privacy Act safeguards with respect to records.
- 5. Disclosure may be made to a congressional office from the record to an individual in response to an inquiry from the congressional office made at the request of the individual.
- 6. In the event of litigation where the defendant is (a) the Department, any component of the Department, or any employee of the Department in his or her official capacity; (b) the United States where the Department determines that the claim, if successful, is likely to directly affect the operations of the Department or any of its components; or (c) any Department employee, for example, in defending against a claim based upon an individual's mental or physical condition and alleged to have arisen because of activities of the Public Health Service in connection with such individual, the Department may disclose such records as it deems desirable or necessary to the Department of Justice to enable that Department to present an effective defense, provided that such disclosure is compatible with the purpose for which the records were collected.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Data may be stored in file folders, magnetic tapes or disks, punched cards, or bound notebooks.

RETRIEVABILITY:

Information is retrieved by name and/or a participant identification number.

SAFEGUARDS:

Measures to prevent unauthorized disclosures are implemented as appropriate for each location and for the particular records maintained in each project. Each site implements personnel, physical and procedural safeguards such as the following:

- 1. Authorized users: Employees who maintain records in this system are instructed to grant regular access only to contractor personnel; consultants to the contractor; the NIDR project officer; and NIDR employees whose duties require the use of such information. Access to the data controlled by the Project Director, the NIDR Project Officer, and/or the System Manager.
- 2. Physical safeguards: Records are stored in locked files or secured areas. Computer terminals are in secured areas.
- 3. Procedural safeguards: Names and other identifying particulars are deleted when data from original records is encoded for analysis. Encoded data is indexed by code numbers. Tables linking these code numbers with actual identifiers are maintained separately. Code numbers and identifiers are linked only if there is a specific need. Data stored in computers is accessed through the use of keywords known only to the principal investigators or authorized personnel. These keywords are changed frequently.

The particular safeguards implemented in each project will be developed in accordance with Chapter 45–13, "Safeguarding Records Contained in Systems of Records," of the HHS General Administration Manual, supplementary Chapter PHS.hf: 45–13, and Part 6, "ADP Systems Security", of the HHS Information Resources Management Manual and the National Institute of Standards and Technology Federal Information Processing Standards (FIPS Pub. 41 and FIPS Pub. 31).

RETENTION AND DISPOSAL:

Records are retained and disposed of under the authority of the NIH Records Control Schedule contained in NIH Manual Chapter 1743, Appendix 1— "Keeping and Destroying Records" (HHS Records Management Manual, Appendix B–361), item 3000–G–3, which allows records to be kept as long as they are useful in scientific research. Refer to the NIH Manual Chapter for specific disposition instructions.

SYSTEM MANAGER AND ADDRESS:

Chief, Contract Management Section, Extramural Program, National Institute of Dental Research, Natcher Building, Room 4AN–44B, 45 Center Drive MSC 6402, Bethesda, MD 20892–6402

NOTIFICATION PROCEDURE:

Write to:

Privacy Act Coordinator, National Institute of Dental Research, 31 Center Drive MSC 2290, Building 31, Room 2C–35, Bethesda, MD 20892–2290 and provide the following information in writing:

- 1. Full name at time of participation in the study.
- 2. Name and description of the study. 3. Location and approximate dates of participation.

The requester must also verify his or her identity by providing either a notarization of the request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Act, subject to a five thousand dollar fine.

An individual who requests notification of, or access to, a medical or dental record shall, at the time the request is made, designate in writing a responsible representative who will be willing to review the record and inform the subject individual of its contents at the representative's discretion.

A parent or guardian who requests notification of, or access to, the medical record of a child or incompetent person shall designate a family physician or other health professional (other than a family member) to whom the records, if any, will be sent. The parent or guardian must verify relationship to the child or incompetent person as well as his or her own identity.

RECORD ACCESS PROCEDURES:

Same as notification. Requesters should also reasonably specify the record contents being sought. Individuals may also request listings of accountable disclosures that have been made of their records, if any.

CONTESTING RECORD PROCEDURES:

Contact the System Manager at the address above. The contestor must reasonably identify the record, specify in writing the information being contested, and state the corrective action sought, and the reason(s) for the corrective action, with supporting justification. The right to contest records is limited to information which is incomplete, irrelevant, incorrect, or untimely (obsolete).