the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," 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 4000–A–2, which allows records to be destroyed when no longer needed for administrative purposes. Refer to the NIH Manual Chapter for specific disposition instructions.

SYSTEM MANAGER(S) AND ADDRESS:

Chief, Information Systems Branch, Division of Research Grants, Westwood Building, 5333 Westbard Avenue, Bethesda, MD 20892 and

For chartered advisory committees of the National Institutes of Health:

NIH Committee Management Officer, Building 31, Room 3B–55, 9000 Rockville Pike, Bethesda, MD 20892.

NOTIFICATION PROCEDURE:

To determine if a record exists write to:

Privacy Act Coordinator, Division of Research Grants, Westwood Building, Room 449, 5333 Westbard Avenue, Bethesda, MD 20892

and

For information pertaining to the chartered advisory committees of the National Institutes of Health:

NIH Committee Management Officer, Building 31, Room 3B–55, 9000 Rockville Pike, Bethesda, MD 20892.

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.

RECORD ACCESS PROCEDURE:

Same as notification procedures. 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 PROCEDURE:

Contact the official under notification procedures above, and reasonably identify the record and specify the information to be contested, and state the corrective action sought and the reasons for the correction, with supporting justification. The right to contest records is limited to information which is incomplete, irrelevant, incorrect, or untimely (obsolete).

RECORD SOURCE CATEGORIES:

Individual, individual's educational institution and references.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.

09-25-0042

SYSTEM NAME:

Clinical Research: National Institute of Dental Research Patient Records, HHS/NIH/NIDR.

SECURITY CLASSIFICATION: None.

None.

SYSTEM LOCATION:

National Institutes of Health, Building 10, Room 1B01, 10 Center Drive MSC 1190, Bethesda, MD 20892–1190.

Write to system manager at the address below for the address of the Federal Records Center where records from this system may be stored.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Patients and other participants in current and past research projects of the National Institute of Dental Research (NIDR).

CATEGORIES OF RECORDS IN THE SYSTEM:

Medical and dental histories, dental pathologies and therapies.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Sections 301, 401, 405 and 453 of the Public Health Service Act (42 U.S.C. 241, 281, 284, 285h). These sections establish the National Institute of Dental Research and authorize the conduct and support of dental oral research and related activities.

PURPOSE(S):

 To record the diagnosis and treatment of patients with diseases of the mouth, tongue, teeth and surrounding tissues; (2) To record the normal condition of the mouth, tongue, teeth and surrounding tissues of individuals referred to the dental clinic;
To provide clinical data for research into the etiology, treatment and prevention of oral diseases; (4) For review and planning of the NIDR clinical program.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

1. Disclosure may be made to HHS contractors, grantees and collaborating researchers and their staff in order to accomplish the clinical and research purposes for which the records are collected. The recipients are required to maintain Privacy Act safeguards with respect to these records.

2. Certain diseases and conditions, including infectious diseases, may be reported to appropriate representatives of State or Federal Government as required by State or Federal law.

3. Information may be used to respond to congressional inquiries for constituents concerning admission to the NIH Clinical Center.

4. 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 in his or her individual capacity where the Justice Department has agreed to represent such employee, for example, when a claim is based upon an individual's mental or physical condition and is 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:

Records are stored in file folders.

RETRIEVABILITY:

Records are retrieved by name and hospital ID 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: