affect directly the operations of the Department or any of its components; or (c) any Department employee in his or her individual capacity where the Department of Justice has agreed to represent such employee, for example, in defending a claim against the Public Health Service, 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 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.

3. NIH may disclose records to Department contractors and subcontractors for the purpose of collecting, compiling, aggregating, analyzing, or refining records in the system. Contractors maintain, and are also required to ensure that subcontractors maintain, Privacy Act safeguards with respect to such records.

A record may be disclosed for a research purpose, when the Department: (A) Has determined that the use or disclosure does not violate legal or policy limitations under which the record was provided, collected, or obtained; (B) has determined that the research purpose (1) cannot be reasonably accomplished unless the record is provided in individually identifiable form, and (2) warrants the risk to the privacy of the individual that additional exposure of the record might bring; (C) has required the recipient to (1) establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of the record, (2) remove or destroy the information that identifies the individual at the earliest time at which removal or destruction can be accomplished consistent with the 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 purpose of 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.

5. Information from this system may be disclosed to Federal agencies, State agencies (including the Motor Vehicle Administration and State vital statistics offices, private agencies, and other third parties (such as current or prior employers, acquaintances, relatives), in order to obtain information on morbidity and mortality experiences and to locate individuals for the followup studies. Social Security numbers may be disclosed: (1) To the National Center for Health Statistics to ascertain vital status through the National Death Index; (2) to the Health Care Financing Agency to ascertain morbidities; and (3) to the Social Security Administration to ascertain disabilities and/or location of participants. Social Security numbers may also be given to other Federal agencies, and State and local agencies for purposes of locating individuals for participation in follow-up studies.

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

STORAGE:

Records may be stored in file folders and computer types and diskettes, microfiche, and file cards.

RETRIEVABILITY:

Records are retrieved by name, Social Security number, or other identifying numbers, keywords, and parameters of individual patient health or medical record data.

SAFEGUARDS:

1. Authorized users: Data on computer files is accessed by keyword known only to authorized users who are NIH or contractor employees who have a need for the data in performance of their duties as determined by the system manager. Researchers authorized to conduct research on biologic specimens will have access to the system through the use of encrypted identifiers sufficient to link individuals with records in such a manner that does not compromise confidentiality of the individual. Access to information is thus limited to those with a need to know

2. *Physical safeguards:* Records and data tapes are stored in locked files in secured areas with restricted access. During regular business hours rooms are unlocked but are controlled by on-site personnel. Terminal access is controlled by user ID and keywords; off-site data backup is maintained in a separate building; fire protection is maintained

by an on-site fire extinguisher system and fire alarm system present in the computer room.

3. Procedural and technical safeguards: Names and other identifying particulars are deleted when data from original records are encoded for analysis. Data stored in computers is accessed through the use of keywords known only to authorized users. A password is required to access the terminal and a data set name controls the release of data to only authorized users. All users of personal information in connection with the performance of their jobs (see Authorized Users, above) protect information from public view and from unauthorized personnel entering an unsupervised office. Contractors and subcontractors who maintain records in this system are instructed to make no further disclosure of the records except as authorized by the System manager and permitted by the Privacy Act. Privacy Act requirements are specifically included in contracts and in agreements with grantees or collaborators participating in research activities supported by the system. HHS project directors, contract officers, and project officers oversee compliance with these requirements.

These practices are in compliance with the standards of Chapter 45–13 of the HHS General Administration Manual, "Safeguarding Records Contained in Systems of Records," supplementary Chapter PHS hf: 45–13, and the Department's Automated Information System Security Program Handbook, 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(b), 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, Diabetes Research Section, DPB, DDEM, National Institutes of Diabetes and Digestive and Kidney Diseases, National Institutes of Health, Westood Building, Room 622, 5333 Westbard Avenue, Bethesda, MD 20892.

NOTIFICATION PROCEDURES:

To determine if a record exists, write to the System Manager listed above. The