09-25-0014 **SYSTEMS LISTING**

SYSTEM NAME:

Clinical Research: Student Records, HHS/NIH/CC/OD/OCRTME

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Office of Clinical Research Training and Medical Education, Office of the Director (OD), NIH Clinical Center, Building 10, B1L403, 10 Center Drive, Bethesda, MD 20892-1158.

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Clinical fellows, medical and dental students, and other students in NIH clinically-related training programs.

CATEGORIES OF RECORDS IN THE SYSTEM:

Application form, transcripts, references, evaluations.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. 241.

PURPOSE(S):

1. To review materials submitted by applicants for entry into NIH training programs.
2. To identify participants in clinical research training programs, clinical elective rotations, and other clinical research training positions.
3. To maintain a record of those individuals who have received clinical research training at the NIH for historical and reference uses.

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

1. Information may be used to respond to congressional inquiries regarding constituents who have applied for training programs.
2. Information may be used to respond to inquiries from hospitals and other healthcare institutions seeking information regarding the nature or duration of clinical research

training or education of medical students, dental students, or physicians enrolled in NIH programs referenced above.

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

STORAGE:

Hard copy records are stored in file folders. Electronic records are stored on computer databases and other media, primarily compact disks.

RETRIEVABILITY:

Records are retrieved by name and year, program or training type.

SAFEGUARDS:

Measures to prevent the unauthorized disclosure of information covered under the Privacy Act are implemented for each training program administered through the Office of Education.

1. Authorized Users: Staff in the NIH Clinical Center's Office of Clinical Research Training and Medical Education are required to take Computer Security and Privacy Awareness Training, and are instructed to disclose information only to authorized NIH personnel who are involved in the evaluation and selection of candidates for intramural training programs.
2. Physical Safeguards: Paper files and disks are stored in locked cabinets in locked rooms within the Office of Clinical Research Training and Medical Education. Electronic databases are accessible only with individual passwords and are further protected by role-based security to limit access.
3. Procedural Safeguards: Access to the paper files is strictly controlled by the Office of Clinical Research Training and Medical Education staff. Files may be removed only with the approval of the system manager or other authorized official(s).

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), items 2300-320-1-13, which allows records to be kept up to a maximum period of seven years following the completion of training. Refer to the NIH Manual Chapter for specific disposition instructions.

SYSTEM MANAGER(S) AND ADDRESS(ES):

Director, Office of Clinical Research Training and Medical Education, NIH Clinical Center, Building 10/CRC, Room B1 L403, Bethesda, Maryland 20892-1352

NOTIFICATION PROCEDURE:

Write to the System manager to determine if a record exists. 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 s/he 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:

To obtain access to a record, contact the System Manager at the above address and provide the information described under notification procedures above. 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:

Write to the System Manager at the address specified above, and reasonably identify the record and specify the information to be contested, 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:

Applicants, universities and teachers.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

None.