§ 1182.14 Procedures for maintaining accounts of disclosures made by the Institute from its systems of records.

(a) The Office of the General Counsel shall maintain a log containing the date, nature, and purpose of each disclosure of a record to any person or to another agency. Such accounting also shall contain the name and address of the person or agency to whom each disclosure was made. This log need not include disclosures made to Institute employees in the course of their official duties, or pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 552).

(b) The Institute shall retain the accounting of each disclosure for at least five years after the accounting is made or for the life of the record that was disclosed, whichever is longer.

(c) The Institute shall make the accounting of disclosures of a record pertaining to you available to you at your request. Such a request should be made in accordance with the procedures set forth in §1182.8. This paragraph (c) does not apply to disclosures made for law enforcement purposes under 5 U.S.C. 552a(b)(7) and §1182.13(a)(7).

§ 1182.15 Institute responsibility for maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems.

The Chief Information Officer has the responsibility of maintaining adequate technical, physical, and security safeguards to prevent unauthorized disclosure or destruction of manual and automatic record systems. These security safeguards shall apply to all systems in which identifiable personal data are processed or maintained, including all reports and outputs from such systems that contain identifiable personal information. Such safeguards must be sufficient to prevent negligent, accidental, or unintentional disclosure, modification or destruction of any personal records or data, and must furthermore minimize, to the extent practicable, the risk that skilled technicians or knowledgeable persons could improperly obtain access to modify or destroy such records or data and shall further insure against such casual entry by unskilled persons without official reasons for access to such records or data.

(a) Manual systems. (1) Records contained in a system of records as defined in this part may be used, held, or
stored only where facilities are ade-
quately to prevent unauthorized access
by persons within or outside the Insti-
tute.

(2) All records, when not under the
personal control of the employees au-
thorized to use the records, must be
stored in a locked filing cabinet. Some
systems of records are not of such con-
fidential nature that their disclosure
would constitute a harm to an indi-
vidual who is the subject of such rec-
dand. However, records in this cate-
geory also shall be maintained in
locked filing cabinets or maintained in
a secured room with a locking door.

(3) Access to and use of a system of
records shall be permitted only to per-
sons whose duties require such access
within the Institute, for routine uses
as defined in §1182.1 as to any given
system, or for such other uses as may
be provided in this part.

(4) Other than for access within the
Institute to persons needing such
records in the performance of their of-
official duties or routine uses as defined
in §1182.1, or such other uses as pro-
vided in this part, access to records
within a system of records shall be per-
mitted only to the individual to whom
the record pertains or upon his or her
written request to the General Counsel.

(5) Access to areas where a system of
records is stored will be limited to
those persons whose duties require
work in such areas. There shall be an
accounting of the removal of any
records from such storage areas util-
izing a log, as directed by the Chief In-
formation Officer. The log shall be
maintained at all times.

(6) The Institute shall ensure that all
persons whose duties require access to
and use of records contained in a sys-
tem of records are adequately trained
to protect the security and privacy of
such records.

(7) The disposal and destruction of
records within a system of records
shall be in accordance with rules pro-
mulgated by the General Services Ad-
ministration.

(b) Automated systems. (1) Identifiable
personal information may be processed,
stored, or maintained by automated
data systems only where facilities or
conditions are adequate to prevent un-
authorized access to such systems in
any form. Whenever such data, whether
contained in punch cards, magnetic
tapes, or discs, are not under the per-
sonal control of an authorized person,
such information must be stored in a
locked or secured room, or in such
other facility having greater safe-
guards than those provided for in this
part.

(2) Access to and use of identifiable
personal data associated with auto-
mounted data systems shall be limited to
those persons whose duties require
such access. Proper control of personal
data in any form associated with auto-
mated data systems shall be main-
tained at all times, including mainte-
nance of accountability records show-
ing disposition of input and output doc-
ments.

(3) All persons whose duties require
access to processing and maintenance
of identifiable personal data and auto-
mated systems shall be adequately
trained in the security and privacy of
personal data.

(4) The disposal and disposition of
identifiable personal data and auto-
mated systems shall be done by shred-
ding, burning, or, in the case of tapes
or discs, degaussing, in accordance
with regulations of the General Serv-
ces Administration or other appro-
priate authority.

§1182.16 Procedures to ensure that In-
stitute employees involved with its
systems of records are familiar with
the requirements and of the Pri-

cacy Act.

(a) The Director shall ensure that all
persons involved in the design, develop-
ment, operation, or maintenance of
any Institute system are informed of
all requirements necessary to protect
the privacy of subject individuals. The
Director also shall ensure that all In-
stitute employees having access to
records receive adequate training in
their protection, and that records have
adequate and proper storage with suffi-
cient security to assure the privacy of
such records.

(b) All employees shall be informed
of the civil remedies provided under 5
U.S.C. 552a(g)(1) and other implications
of the Privacy Act, and the fact that
the Institute may be subject to civil
remedies for failure to comply with the