

SYSTEM NUMBER: 09-25-0223

SYSTEM NAME:

NIH Records Related to Research Misconduct Proceedings, HHS/NIH

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

This system of records will be located in National Institutes of Health (NIH) facilities and/or in the facilities of contractors and/or other affiliates working on behalf of NIH. Specific location:

Office of Intramural Research (OIR), National Institutes of Health (NIH), 9000 Rockville Pike, Bethesda, Maryland 20892.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system will contain records about individuals who are the subject of research misconduct allegations or proceedings, referred to as “respondents.” The Public Health Service (PHS) Policies on Research Misconduct (“PHS Policies on Research Misconduct”), 42 CFR Part 93 (“Part 93”), define the term “respondent” to mean “the person against whom an allegation of research misconduct is directed or who is the subject of a research misconduct proceeding.” 42 CFR 93.225. This definition has also been incorporated into the NIH Intramural Research Program Policies & Procedures for Research Misconduct Proceedings (“NIH Policy”). Other individuals who may be involved in research misconduct allegations or proceedings (e.g., complainants, witnesses) are not record subjects for purposes of this system.

Consistent with the NIH’s responsibilities under Part 93 and the NIH Policy, this system notice applies to alleged or actual research misconduct (fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results) involving research: (1) carried out in NIH facilities by any person; (2) funded by the NIH Intramural Research Program (IRP) in any location; or (3) undertaken by an NIH employee or trainee as part of his or her official NIH duties or NIH training activities, regardless of location. A person who, at the time of the alleged or actual research misconduct, was employed by, was an agent of, or was affiliated by contract, agreement, or other arrangement with NIH, is subject to the NIH Policy and covered by this system if, for example, he or she is involved in: (1) NIH- or PHS-supported biomedical or behavioral research; (2) NIH- or PHS-supported biomedical or behavioral research training programs; (3) NIH- or PHS-supported activities that are related to biomedical or behavioral research or research training, such as the operation of tissue and data banks and the dissemination of research information; (4) plagiarism of research records produced in the course of NIH- or PHS-supported research, research training or activities related to that research or research training; or (5) an application or proposal for NIH or PHS support for biomedical or behavioral research, research training or activities related to that research or research training, such as the operation of tissue and data banks and the dissemination of research information (regardless of whether it is approved or funded).

The term “research misconduct” is defined to mean “fabrication, falsification, or plagiarism in proposing, performing, or reviewing research, or in reporting research results.” “Fabrication” is defined to mean “making up data or results and recording or reporting them.” “Falsification” is “manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.” “Plagiarism” is “the appropriation of another person’s ideas, processes, results, or words without giving appropriate credit.” Research misconduct does not include honest error or differences of opinion. 42 CFR 93.103.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system contains records related to research misconduct proceedings. The term “research misconduct proceeding” is defined in Part 93 and the NIH Policy to mean “any actions related to alleged research misconduct,” including, but not limited to, allegation assessments, inquiries, investigations, oversight reviews by the Office of Research Integrity (ORI) of the U.S. Department of Health and Human Services (DHHS, HHS or Department), hearings, and administrative appeals.

The records include all information that NIH receives or generates in overseeing or conducting research misconduct proceedings, including the implementation of research misconduct findings, and all information that NIH submits to, or receives from, ORI or other institutions under Part 93. This information includes, but is not necessarily limited to information about respondents (this may include social security numbers), complainants, and witnesses; the nature of the allegations; the NIH or PHS funding involved, including grant numbers; the offices, Institutes, Centers, and officials responsible for conducting the actions that are part of the research misconduct proceeding; the documentation used in the assessment, inquiry, and investigation, including relevant research data and materials, applications, proposals and documentation related to review and award actions, reports, abstracts, manuscripts and publications by the respondent(s) and other relevant reports, abstracts, manuscripts and publications; correspondence; memoranda of telephone calls, summaries of interviews and transcripts or recordings of interviews; statistical, scientific, and forensic analyses; interim and final reports; and records of findings, administrative actions, and appeal proceedings, if any.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The legal authorities to operate and maintain this Privacy Act records system are Sections 301, 401, 402, and 405 of the Public Health Service Act (42 U.S.C. 241, 281, 282, and 284); 5 U.S.C. 301; 44 U.S.C. 3101; and 42 C.F.R. Part 93.

PURPOSE(S):

NIH personnel and any contractors assisting them will use information from this system, on a need-to-know basis, for the following purposes:

1. To enable NIH and its Institutes and Centers (“ICs”) to protect the health and safety of the public, to promote the integrity of NIH- or PHS-supported research, and to conserve public funds;
2. To enable NIH to discharge effectively its responsibilities in managing the NIH intramural research program and in the award and administration of research and training grants, cooperative agreements, and contracts;
3. To ensure that research misconduct proceedings are carried out in accordance with the NIH Policy, 42 CFR Part 93, and other applicable Federal statutes and regulations;
4. To enable NIH to inform other IC, NIH, ORI, PHS, and other HHS agency officials who have a need for the records in the performance of their duties, of the status and results of research misconduct proceedings; and
5. To enable NIH to notify, consult with, and provide assistance to other Federal, State, local, or Tribal governmental agencies to permit them to take action to protect the health and safety of the public, to promote the integrity of NIH- and PHS-supported research, to conserve public funds, or to pursue potential violations of civil and criminal statutes.

ROUTINE USES DISCLOSURES MADE OUTSIDE OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS OR DEPARTMENT) OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

A “routine use” is defined in 45 CFR 5b.1(j) to mean “the disclosure of a record outside the Department, without the consent of the subject individual, for a purpose which is compatible with the purpose for which the record was collected.” The routine uses for which NIH will disclose information from this system of records are as follows:

1. Disclosure may be made to any person able to obtain information or provide information or assistance in a research misconduct proceeding or related proceeding. Recipients of disclosures under this routine use may include: experts asked to perform statistical, forensic or other analyses or otherwise to provide assistance; institutions with which the respondent(s) was previously or is currently affiliated; Federal, State, local, and Tribal governmental agencies; the respondent(s); the complainant(s); witnesses; and organizations or individuals acting on behalf of those institutions, agencies, and individuals; provided, however, in each case NIH determines whether limited disclosures, confidentiality statements, contractual commitments to comply with the requirements of the Privacy Act of 1974, or similar measures are needed to protect the privacy of respondent(s), complainant(s), witnesses, research subjects, or others who may be identified in the records to be disclosed.
2. Disclosure may be made to NIH/DHHS guest researchers, special government employees (SGEs), trainees, volunteers, former employees, contractors, and other persons engaged to perform a service in support of NIH/DHHS related to this system of records, if such persons need access to the records to perform their assigned task; provided, however, in each case NIH/DHHS determines whether limited disclosures, confidentiality statements, contractual commitments to comply with the requirements of the Privacy Act of 1974, or similar measures are needed to protect the privacy of respondent(s), complainant(s), witnesses, research subjects, or others who may be identified in the records to be disclosed; and NIH/DHHS determines that the disclosure is for a purpose compatible with the purpose for which the agency collected the records.
3. Disclosure may be made to other Federal, State, local, or Tribal governmental agencies and offices, if NIH has reason to believe that a research misconduct proceeding may involve that agency or office.
4. When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, disclosure may be made to the appropriate governmental agency, whether Federal, State, local or Tribal, or other public authority responsible for enforcing, investigating or prosecuting such violation, if the information disclosed is relevant to the responsibilities of the agency or public authority.
5. Disclosure may be made to Institutional Review Boards, research-sponsoring institutions, and individual research subjects, regarding information obtained or developed through a research misconduct proceeding that, in NIH's judgment, may have implications for individuals' health or for their participation in a research study.
6. After NIH makes a finding of research misconduct and has informed ORI of the finding, disclosure may be made to responsible officials of NIH- or PHS-supported institutions or organizations, when in connection with a research misconduct proceeding concerning an individual previously or currently employed by, or affiliated with the institution or organization, or when NIH, ORI, or HHS makes a finding or takes an action potentially affecting the institution or organization or its NIH or PHS support for research, research training, or related activities.
7. A record from this system may be disclosed to a Federal, State, local, or Tribal governmental agency maintaining civil, criminal, or other relevant enforcement records, or other pertinent records, or to another public authority or professional organization, if necessary to obtain information relevant to an investigation concerning the employment, clearance, suitability, eligibility or retention of an employee or other personnel action, the retention of a security clearance, the letting of a contract, issuance of a benefit or qualification decision made by HHS or NIH. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another Federal agency for criminal, civil, administrative, personnel, or regulatory action. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No information will be released that would reveal a confidential source.
8. After NIH makes a finding of research misconduct and has informed ORI of the finding, disclosure may be made to research collaborators of the respondent, professional journals, other publications, news media, professional societies, other individuals and entities, and the public concerning research misconduct findings and the need to correct or retract research results or reports that have been affected by research misconduct, unless NIH determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal

privacy. No information will be released that would reveal a confidential source.

9. After NIH makes a finding of research misconduct and has informed ORI of the finding, disclosure may be made to a State or other professional licensing board, certifying body, or other similar entity authorized to conduct a review of the respondent, to aid the entity in meeting its responsibility to protect the health of the population in its jurisdiction or the integrity of the profession.

10. After NIH concludes a research misconduct proceeding without a finding of research misconduct or a settlement, disclosure may be made to the respondent, the complainant, witnesses, or other persons involved in or aware of the research misconduct proceeding; provided, however, in each case NIH determines whether limited disclosures, confidentiality statements, contractual commitments to comply with the requirements of the Privacy Act of 1974, or similar measures are needed to protect the privacy of respondent(s), complainant(s), witnesses, research subjects, or others who may be identified in the records to be disclosed.

11. Disclosure may be made to the Department of Justice (DOJ), a court, or other tribunal, when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where the DOJ has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation and, by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by the DOJ, a court, or other tribunal is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.

12. A record may be disclosed to appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, if the information disclosed is relevant and necessary for that assistance.

13. Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made pursuant to the written request of the individual and if disclosure does not compromise the law enforcement activities of the Office of Research Integrity or other government agency.

14. NIH may disclose information to the National Archives and Records Administration (NARA), General Services Administration (GSA), or other Federal government agencies pursuant to records management inspections conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

15. Records may become accessible to U.S. Department of Homeland Security (DHS) cyber security personnel, if captured in an intrusion detection system used by HHS and DHS pursuant to the Einstein 2 program. Under Einstein 2, DHS uses intrusion detection systems to monitor Internet traffic to and from federal computer networks to prevent malicious computer code from reaching the networks. According to DHS' Privacy Impact Assessment for Einstein 2 (available on the DHS Cybersecurity privacy website, http://www.dhs.gov/files/publications/editorial_0514.shtm#4), only personally identifiable information (PII) that is directly related to a malicious code security incident is captured by and accessible to DHS, and DHS does not access PII unless the PII is part of the malicious code.

NIH may also disclose information from this system as authorized directly in the Privacy Act at 5 U.S.C. 552a(b).

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

STORAGE:

Records will be stored in various electronic media and paper form, and maintained under secure conditions in limited access areas or with controlled access. Only authorized users whose official duties require the use of this information will have regular access to the records in this system.

In accordance with established NIH, HHS and other Federal security policies and controls, records may also be located, maintained and accessed from secure servers whenever feasible or located on portable/mobile devices including, but not limited to: laptops, PDAs, USB drives, portable hard drives, Blackberrys, iPods, CDs, DVDs, electronic readers, and/or other portable/mobile storage devices. Records are maintained on portable/mobile storage devices only for valid, business purposes, with prior approval, and in accordance with all applicable NIH, HHS and Federal security requirements, policies and controls.

RETRIEVABILITY:

Records will be retrieved by manual or computer search using a unique case number or the name of the respondent(s) (i.e., the individual or individuals who are the subject of an allegation of research misconduct or of a research misconduct proceeding).

SAFEGUARDS:

Measures to prevent unauthorized disclosures are implemented as appropriate for each location or form of storage and for the types of records maintained. Site(s) implement personnel and procedural safeguards such as the following:

Authorized Users:

Access is strictly limited to ensure least privilege by authorized personnel whose duties require such access (i.e., valid, business need-to-know). Records from this system are available to the System Manager, to the Director, NIH, and to other appropriate NIH staff when they have a need for the records in the performance of their duties. Records are also available to the Director, ORI, and to other appropriate HHS officials, including attorneys in the Office of the General Counsel, when there is a need to know in the performance of their duties. All authorized users are informed that the records are confidential and are not to be further disclosed.

Physical Safeguards:

Controls to secure the data and protect paper and electronic records, buildings, and related infrastructure against threats associated with their physical environment include, but are not limited to the use of the HHS Employee ID and/or badge number and NIH key cards and security guards. Paper records are secured in locked file cabinets, offices and facilities. Electronic media are kept on secure servers or computer systems. Data on computer files is accessed by a password known only to authorized users who have a need for the data in the performance of their duties as determined by the System Manager. During regular business hours, rooms in this restricted area are unlocked but entry is controlled by on-site personnel. Security guards perform random checks on the physical security of the storage locations after duty hours, including weekends and holidays. The NIH main campus in Bethesda, Maryland is protected by perimeter barriers and limited points of access, security personnel, and intrusion alarms. Electronic access to computer files is strictly limited through passwords and user-invisible encryption. Special measures commensurate with the sensitivity of the record are taken to prevent unauthorized copying or disclosure of the records. Individually identifiable records are kept in locked file cabinets or in rooms under the direct control of the System Manager. Contractor interaction with records covered by this system will occur on-site and no physical records (paper or electronic) will be allowed to be removed from the NIH Office of Intramural Research unless authorized. All authorized users of personal information in connection with the performance of their jobs protect information from public view and from unauthorized personnel entering an unsupervised area/office.

Administrative Safeguards:

Controls to ensure proper protection of information and information technology systems include, but are not limited to the completion of a Certification and Accreditation (C&A) package and a Privacy Impact Assessment (PIA) for associated information technology systems, a system security plan, a contingency or back-up plan, user manuals, and mandatory completion of annual NIH Information Security and Privacy Awareness training. All authorized 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 area/office. When the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the applicable Privacy Act Federal Acquisition Regulation (FAR) clauses are inserted in solicitations and contracts.

Technical Safeguards:

Controls are generally executed by the computer system and are employed to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. They include, but are not limited to user identification, password protection, firewalls, virtual private network, encryption, intrusion detection system, common access cards, smart cards, biometrics and public key infrastructure.

Implementation Guidelines: This Privacy Act System of Records Notice conforms to and complies with Office of

Management and Budget (OMB) Circular A-130 – Appendix I “Federal Agency Responsibilities for Maintaining Records about Individuals” <http://www.whitehouse.gov/omb/assets/omb/circulars/a130/a130trans4.pdf>, standards outlined in the Health and Human Services (HHS) General Administration Manual (GAM), HHS Chapter 45-10 “Privacy Act – Basic Requirements and Relationships” <http://www.hhs.gov/hhsmanuals/gam/chapters/45-10.pdf>, HHS Chapter 45-12 “Creation, Alteration, and Termination of Privacy Act Systems of Records and Associated Documentation” (available in paper copy only), HHS Chapter 45-13, “Safeguarding Records Contained in Systems of Records” <http://www.hhs.gov/hhsmanuals/gam/chapters/45-13.pdf>, and HHS Information Security and Privacy Program Policy.

Alleged or Confirmed Security Incidents: NIH will report and take action to remediate security incidents involving the disclosure of personally identifiable information according to law, regulations, OMB guidance, HHS and NIH policies.

RETENTION AND DISPOSAL:

Records will be maintained for 7 years in accordance with 42 CFR Part 93 and retained and disposed of under the authority of the NIH Records Control Schedule contained in Manual Chapter 1743, "Keeping and Destroying Records", Appendix 1, item 1700-A-3. Refer to the NIH Manual Chapter for specific retention and disposition instructions: <http://www1.od.nih.gov/oma/manualchapters/management/1743>

SYSTEM MANAGER AND ADDRESS:

The agency official responsible for the system policies and practices outlined above is:

NIH Agency Intramural Research Integrity Officer (AIRIO), Office of Intramural Research (OIR), National Institutes of Health (NIH), 9000 Rockville Pike, Bethesda, Maryland 20892.

NOTIFICATION PROCEDURE:

This system will be exempt from the Privacy Act provision requiring procedures for notifying an individual, upon his or her request, if the system contains a record about him or her. However, consideration will be given to requests addressed to the System Manager listed above. Any individual who wishes to know if this system contains a record about him or her may make a written request to the System Manager.

RECORD ACCESS PROCEDURE:

This system will be exempt from access. However, because the access exemption is limited and discretionary, consideration will be given to access requests addressed to the System Manager. The requester must verify his or her identity by providing either a notarization of the request or a written certification that he or she is who he or she claims to be and understands that the knowing and willful request of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act, subject to a fine of up to five thousand dollars. If records are requested on behalf of a minor or legally incapacitated person, a statement of guardianship/conservatorship must be included. Requesters should also reasonably specify the record contents being sought. Requests should include a) full name, b) address, c) the approximate date(s) the information was collected, d) the types of information collected, and e) the office or official responsible for the collection of information, etc. Individuals may also request an accounting of disclosures that have been made of their records, if any, if the System Manager determines that disclosure would not compromise the law enforcement activities of the NIH Office of Intramural Research. (These access procedures are in accordance with Department regulation (45 CFR 5b.5(a)(2)).

CONTESTING RECORD PROCEDURE (REDRESS):

This system will be exempt from redress. However, records that contain factually incorrect information may be amended. To contest such information, 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 reason(s) for

requesting the correction, along with supporting information. The right to contest records is limited to information which is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

RECORD SOURCE CATEGORIES:

Information in this system is received or obtained from many sources, including: (1) directly from the complainant or respondent or his/her representative; (2) derived from materials supplied by the complainant or respondent or his/her representative; (3) from information supplied by institutions, witnesses, scientific publications or other nongovernmental sources; (4) from observation and analysis made by NIH staff, guest researchers, SGEs, trainees, volunteers, former employees, contractors, and other persons engaged to perform a service in support of NIH; (5) departmental and other Federal, State, local, and Tribal government records; (6) from hearings and other administrative proceedings; and (7) from any other relevant source.

EXEMPTIONS CLAIMED FOR THIS SYSTEM:

Pursuant to 5 U.S.C. 552a (k)(2) and (k)(5) of the Privacy Act, the system will be exempted from the Privacy Act requirements pertaining to providing an accounting of disclosures, access and amendment, notification, and agency procedures and rules (5 U.S.C. 552a (c)(3), (d)(1)–(4), (e)(4)(G)-(H), and (f)). NIH believes that these exemptions are necessary to maintain the integrity of the research misconduct proceedings and to ensure that the NIH's efforts to obtain accurate and objective information will not be hindered. However, any individual who has been denied any right, privilege, or benefit to which he or she otherwise would have been entitled as a result of the maintenance of such material will be given access to the material, unless disclosure of the material would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality.