



DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Privacy Act of 1974; System of Records

AGENCY: National Institutes of Health (NIH), Department of Health and Human Services (HHS).

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS) is publishing notice of modifications to a system of records maintained by the National Institutes of Health (NIH), “Clinical Research: Patient Medical Records, HHS/NIH/CC,” no. 09-25-0099. The modifications affect most sections of the System of Records Notice (SORN) and are fully explained in the “Supplementary Information” section of this notice.

DATES: The modified system of records is [INSERT DATE 30 DAYS AFTER OF PUBLICATION IN THE *FEDERAL REGISTER*], subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may submit comments, identified by the Privacy Act SORN no. 09-25-0099, by any of the following methods: Email: privacy@mail.nih.gov. Telephone: (301) 402-6201. Fax: (301) 402-0169. Mail or hand-delivery: NIH Privacy Act Officer, Office of Management Assessment, National Institutes of Health, 6011 Executive Blvd., Ste. 601, MSC 7669, Rockville, MD 20892. Comments received will be available for public inspection at this same address from 9:00 a.m. to 3:00 p.m., Monday through Friday, except federal holidays. Please call (301) 496-4606 for an appointment.

FOR FURTHER INFORMATION CONTACT: General questions about the system of records may be submitted to Celeste Dade-Vinson, NIH Privacy Act Officer, Office of

Management Assessment (OMA), Office of the Director (OD), National Institutes of Health (NIH), 6011 Executive Blvd., Ste. 601, MSC 7669, Rockville, MD 20892, or telephone (301) 402-6201.

SUPPLEMENTARY INFORMATION:

Explanation of Revisions to System No. 09-25-0099

The revised SORN published in this notice for system no. 09-25-0099 is in accordance with 5 U.S.C. 552a(e)(4) and (11), and includes the following significant changes, in addition to minor wording changes throughout:

- Purposes section. Three new purpose descriptions (a, c, d,) have been added, and the one existing purpose description (b, formerly 1 and 2) has been revised. The changes reflect additional purposes for which records will be used within the agency due to a system upgrade or other developments intended to serve patient needs, or provide improved descriptions of existing uses within the agency. For example:
 - The patient medical records system was upgraded to provide the basic functions of a hospital electronic health record. As a result, the system is now able to support the electronic registration of new patients, electronic authorization of patient travel for participation in research protocols conducted at the NIH Clinical Center, and the creation of reports for the patient and any physician authorized by the patient to receive a summary of the patient's care.
- Categories of Individuals section. This section has been updated to include only registered NIH Clinical Center patients (non-registered patients have been excluded).
- Routine Uses section. Certain routine uses have been deleted, revised, or added, and a note has been added to the introductory paragraph to indicate that other federal laws may place additional requirements on the use and disclosure of the information contained in this system. Specifically:

- The routine use formerly numbered as 1, which authorized disclosures to congressional offices to assist them in responding to constituent inquiries, has been deleted as unnecessary. NIH can respond to a congressional inquiry by explaining that NIH will provide requested records directly to the named constituent or with the prior written consent of the named constituent.
- The routine use formerly numbered as 2, which authorized disclosures by the Social Work Department to community agencies to assist patients or their families, has been deleted as unnecessary. Such disclosures are provided pursuant to written authorization by the patient.
- Routine uses 1 through 8 are existing routine uses; routine uses 2 through 8 have been revised as follows:
 - The last sentence in routine use 2 (formerly 4), which stated that the disclosure recipients (research organizations, experts, or consultants outside HHS) are required to maintain Privacy Act safeguards with respect to the records, has been omitted because those recipients are not agency contractors, so are not required to be subject to the federal Privacy Act.
 - Routine use 3 (formerly 5) has been broadened to refer to “authorized accrediting agencies or organizations” “conducting established accreditation activities,” instead of referring to one particular accrediting agency and one activity (e.g., onsite inspections).
 - Routine use 4 (formerly 6) has been revised to include “other reportable events” and reporting to “local or tribal” (not just state and federal) government authorities as disclosure recipients.
 - Routine use 5 (formerly 7) has been revised to remove unnecessary wording (i.e., “may be disclosed in identifiable form”).

- Routine use 6 (formerly 8), which previously authorized disclosures to “private firms” (meaning, contractors and others functioning akin to HHS employees) for limited purposes (i.e., “transcribing updating, copying or otherwise refining records in the system”), has been revised to include more of the same type of disclosure recipient (i.e., “other federal agencies, HHS contractors, or HHS volunteers”) and to describe broader purposes for which they might be engaged to assist HHS and require access to records in this system (i.e., to assist HHS in accomplishing an HHS function relating to the purposes of the system of records).
 - Routine use 7 (formerly 9), which authorizes disclosures for litigation purposes, has been revised to include courts and tribunals (not just the Department of Justice) as disclosure recipients; to reorganize the description of “defendant” into subparts a through d (instead of a through c); and to omit a condition that followed the reference to the United States (i.e., that any claim against the United States must be likely to directly affect agency operations if successful).
 - Routine use 8 (formerly 10), which authorizes disclosure of information concerning exposure to HIV, has been revised to state that such information may be disclosed “consistent with applicable laws, policies, and procedures.”
- Routine use 9 is new. Routine use 9 has been added to authorize disclosures to “designated organ procurement organizations/agencies that recover organs, eyes or tissue for transplantation or donation” in order “to facilitate donor and recipient matching involving patients participating in clinical research.”
- Routine uses 10 is also new; it authorizes disclosures for records management purposes.

- Two breach response-related routine uses which were added February 14, 2018 (see 83 FR 6591) are now numbered as 11 and 12.

Date: January 21, 2021.

Alfred C. Johnson,
Deputy Director for Management,
National Institutes of Health.

SYSTEM NAME AND NUMBER:

Clinical Research: Patient Medical Records, HHS/NIH/CC, 09-25-0099.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for the system of records is: Health Information Management Department, Clinical Center, Bldg. 10, Rm. 1N208, 10 Center Dr., Bethesda, MD 20892-1192.

SYSTEM MANAGER(S):

Director, Health Information Management Department, Clinical Center (CC), Bldg. 10, Rm. 1N208, 10 Center Dr., Bethesda, MD 20892-1192, (301) 496-2292.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

42 U.S.C. secs. 241, 248, 282 and 284. Collection of SSN is impliedly authorized by 42 U.S.C. sec. 282(b)(19) which authorizes the NIH Director to admit and treat individuals for purposes of study (this requires using an enumerator to differentiate between individuals for patient tracking

and patient safety), and by E. O. 9397 (8 FR 16,094, Nov. 30, 1943), as amended by E. O. 13478 (73 FR 70,239, Nov. 20, 2008), which permits SSN to be used as the enumerator.

PURPOSE(S) OF THE SYSTEM:

Records are used within the agency for these purposes:

- a. To facilitate clinical care, clinical research studies, discharge planning, and reporting of information (i.e., medical and research findings) to patients and their treating and/or referring physicians.
- b. To document clinical care and research and provide a continuous history of the medical and clinical research services afforded to registered Clinical Center patients.
- c. To create reports and compile information to provide to recipients authorized by the Privacy Act and this SORN, e.g., designated organ procurement organizations, consultants for expert medical opinions, and authorized outside physicians for continuing patient care.
- d. To allow Institute/Center research team members to register patients.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records pertain to registered NIH Clinical Center patients.

CATEGORIES OF RECORDS IN THE SYSTEM:

This system consists of medical and clinical records, containing patient name, demographics, contact information, physician name and work address, principal investigator name, names of clinicians and other health care staff involved in the care of the patient or management of research activities associated with the protocol, clinical research data and records related to screening, diagnosis, observation and/or treatment at the NIH Clinical Center, social security number (SSN), diagnosis and medication, protocol number, medical record number, lab tests

results, genomic data, radiologic images, imaging studies, blood product utilization, type of sample and storage location, social work encounter, medical and ethical consults, and surgery and other related clinical interactions.

RECORD SOURCE CATEGORIES:

Information contained within this system of records is obtained from the subject individuals; patient interviews; referring physicians; diagnostic, therapeutic, and research results; multi-disciplinary care teams; other medical facilities; relatives of patients; and others authorized by patients to provide information.

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

Under the Privacy Act of 1974, as amended, NIH may disclose information about an individual from this system of records to parties outside HHS, without the individual's prior written consent, pursuant to the following routine uses. Note, however, that other federal laws may apply to the information contained in this system that place additional requirements on the use and disclosure of that information, beyond those found in the Privacy Act of 1974, as amended, or what is mentioned in this system of records notice.

1. To referring physicians for continuing patient care after discharge, unless otherwise notified by patient.
2. To appropriate medical or research organizations, experts, or consultants outside HHS, to obtain expert opinions regarding diagnostic problems, or cases having unusual scientific value in connection with the treatment of patients, or in order to accomplish the research purposes of this system.
3. To representatives of authorized accrediting agencies or organizations conducting established accreditation activities.

4. To report certain diseases, conditions, or other reportable events to federal, state, local or tribal government authorities that are authorized by law to receive such information, or as may be required to comply with applicable laws, provided that such reporting is also consistent with applicable agency policies.
5. To tumor registries for maintenance of health statistics or use in epidemiologic studies.
6. To other federal agencies, HHS contractors, or HHS volunteers who are engaged to work directly for HHS but are not within the definition of HHS employees and who require access to the records in order to assist HHS in accomplishing an HHS function related to the purposes of this system of records. These recipients are required to comply with the requirements of the Privacy Act of 1974, as amended.
7. To the Department of Justice (DOJ) or to a court or other tribunal when: (a) HHS, or any component thereof; (b) any HHS employee in his/her official capacity; (c) any HHS employee in his/her individual capacity where the DOJ (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has a direct and substantial interest in the litigation and, by careful review, HHS determines that the record is both relevant and necessary to the litigation
8. Information concerning exposure to HIV may be disclosed consistent with applicable laws, policies, and procedures to the sexual and/or needle-sharing partner(s) of a subject individual who is infected with HIV under the following circumstances: (a) The information has been obtained in the course of clinical activities at NIH facilities; (b) NIH has made reasonable efforts to counsel and encourage the subject individual to provide information to the individual's sexual or needle-sharing partner(s); (c) NIH determines that the subject individual is unlikely to provide the information to the sexual or needle-sharing partner(s) or that the provision of such information cannot

- reasonably be verified; and (d) The notification of the partner(s) is made, whenever possible, by the subject individual's physician or by a professional counselor and shall follow standard counseling practices.
9. To designated organ procurement organizations/agencies that recover organs, eyes or tissue for transplantation or donation and to facilitate donor and recipient matching involving patients participating in clinical research. These recipients are required to apply reasonable safeguards to prevent unauthorized use or disclosure of the records.
 10. To the National Archives and Records Administration (NARA), General Services Administration (GSA), or other relevant federal agencies pursuant to records management inspections conducted under the authority of 44 U.S.C. secs. 2904 and 2906.
 11. To appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records; (2) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
 12. To another federal agency or federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

NIH may also disclose information about an individual from this system of records to parties outside HHS, without the individual's prior written consent, for any of the purposes authorized directly in the Privacy Act at 5 U.S.C. secs. 552a(b)(2) and (b)(4)-(11).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in various electronic media and paper form, and maintained under secure conditions in areas with limited and/or controlled access. In accordance with established NIH, HHS and other applicable federal security requirements, policies and controls, records may also be stored and accessed from secure servers whenever feasible or stored on approved portable/mobile devices designed to hold any kind of digital data including, but not limited to laptops, tablets, PDAs, USB drives, media cards, portable hard drives, blackberrys, smartphones, CDs, DVDs, and/or other mobile storage devices.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by a patient's name or other unique identifier such as date of birth or medical record number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are retained and disposed of under the authority of the NIH Intramural Retention Schedule, which currently includes these disposition authorities:

- Clinical Care Services Records, DAA-0443-2012-0007-0006, are temporary records that can be destroyed seven years after cutoff.
- Patient Medical Records, DAA-0443-2012-0007-0010, are temporary records that can be destroyed when no longer needed for scientific reference.

- Radiology and Imaging Records, DAA-0443-2012-0007-0007, are temporary records that can be destroyed 60 years after inactivity. (This retention period is being re-examined, and may in the future be significantly shortened.)

Refer to the schedule for complete descriptions of each type of record and for complete disposition instructions: https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-health-and-human-services/rg-0443/daa-0443-2012-0007_sf115.pdf

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Measures to prevent unauthorized disclosures are implemented as appropriate for each location or form of storage and for the types of records maintained. Safeguards conform to the HHS Information Security and Privacy Program, <https://www.hhs.gov/ocio/securityprivacy/index.html>. Site(s) implement personnel and procedural safeguards such as the following:

Authorized Users: Access to the records in this system is strictly limited to authorized users whose official duties require the use of information in the system.

Administrative Safeguards: Controls to ensure proper protection of information and information technology systems include, but are not limited to the completion of a security assessment and authorization (SA&A) package and a privacy impact assessment (PIA) and mandatory completion of annual NIH information security and privacy awareness training. The SA&A package consists of a security categorization, e-authentication risk assessment, system security plan, evidence of security control testing, plan of action and milestones, contingency plan, and evidence of contingency plan testing. 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.

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, security guards, cipher locks, biometrics and closed-circuit TV. Paper records are secured in locked file cabinets, offices and facilities. Electronic media are kept on secure servers or computer systems. Records are stored on portable/mobile devices only for valid business purposes and with prior approval.

Technical Safeguards: Controls that 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.

RECORD ACCESS PROCEDURES:

An individual who wishes to access a record about him or her in this system of records must make an access request, in writing, to the System Manager at the address specified above. For purposes of verifying the requester's identity, the request should provide 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 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 the request is made on behalf of a minor or incapacitated person, evidence of parent or guardian relationship must be included. Requests should include a) full name, b)

address, c) the approximate date(s) the information was collected, d) the type(s) of information collected, and e) the office(s) or official(s) responsible for the collection of information, if known. Individuals may also request an accounting of disclosures that have been made of their records, if any.

CONTESTING RECORD PROCEDURES:

An individual who wishes to contest or amend records about him or her in this system of records must write to the System Manager at the address specified above and provide the information described under “Record Access Procedure.” In addition, the request must reasonably identify the record and specify the information being contested, the corrective action sought, and the reason(s) for requesting the correction, and include any supporting documentation. The right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

NOTIFICATION PROCEDURES:

An individual who wishes to know whether this system of records contains a record about him or her may make a notification request. The request must be made in writing to the System Manager at the address specified above and provide the information described under “Record Access Procedure.”

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

67 FR 60742 at 60755 (Sept. 26, 2002), 83 FR 6591 (Feb. 14, 2018).

