



DEPARTMENT OF THE INTERIOR

Office of the Secretary

[DOI-2021-0011; 22XD4523WS, DWSN00000.000000, DS64800000, DP64803]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary, Interior.

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974, as amended, the Department of the Interior (DOI) is issuing a public notice of its intent to create a new Privacy Act system of records titled, “INTERIOR/DOI-92, Public Health Emergency Response Records.” This system of records notice (SORN) describes DOI’s collection, maintenance, and use of records on individuals associated with DOI efforts to respond to the Coronavirus Disease 2019 (COVID-19), a declared public health emergency, and protect the health and safety of its workforce and members of the public. This newly established system will be included in DOI’s inventory of record systems.

DATES: This new system will be effective upon publication. New routine uses will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: You may send comments identified by docket number [DOI-2021-0011] by any of the following methods:

- Federal eRulemaking Portal: <https://www.regulations.gov>. Follow the instructions for sending comments.
- Email: DOI_Privacy@ios.doi.gov. Include docket number [DOI-2021-0011] in the subject line of the message.
- U.S. mail or hand-delivery: Teri Barnett, Departmental Privacy Officer, U.S.

Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC

20240.

Instructions: All submissions received must include the agency name and docket number [DOI-2021-0011]. All comments received will be posted without change to <https://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <https://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: Teri Barnett, Departmental Privacy Officer, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, DOI_Privacy@ios.doi.gov or 202-208-1605.

SUPPLEMENTARY INFORMATION:

I. Background

The DOI Office of Occupational Safety and Health (OSH) is establishing a new Department-wide system of records, INTERIOR/DOI-92, Public Health Emergency Response Records. This system will help DOI manage records related to DOI's response to the COVID-19 public health emergency and future high consequence public health threats, support emergency or medically related decisions affecting DOI personnel, and ensure the health and safety of the various categories of personnel, contractors, grantees, detailees, volunteers, interns, long-term trainees, and visitors at DOI owned, operated, leased or managed facilities or properties.

This system supports DOI's COVID-19 vaccination and testing program as required by Executive Orders 14043 and 14042; Office of Management and Budget (OMB) Memorandums M-21-15 and M-21-25; COVID-19 Workplace Safety: Agency Model Safety Principles issued by the Federal Safer Federal Workforce Task Force; and other applicable law and policy. Federal labor, employment and workforce health and safety laws that govern the collection, dissemination, and retention of DOI employees'

medical information include the Americans with Disability Act (ADA), the Rehabilitation Act of 1973 (Rehab Act), and the Occupational Safety and Health Act of 1970. The Department of Health and Human Services (HHS) Secretary may, under section 319 of the Public Health Service (PHS) Act codified at 42 U.S.C 247d, declare that: (a) a disease or disorder presents a public health emergency; or (b) that a public health emergency, including significant outbreaks of infectious disease or bioterrorist attacks, otherwise exists.

The Occupational Safety and Health Act (OSHA) of 1970, Public Law 91-596, 29 U.S.C. 668, Section 19(a) requires the head of each Federal agency to establish and maintain an effective and comprehensive occupational safety and health program and safe and healthful places and conditions of employment, and to keep adequate records of all occupational accidents and illnesses for proper evaluation and necessary corrective action. OSHA also requires that Federal agencies maintain an injury and illness prevention program, which is a proactive process designed to reduce injuries, illnesses, and fatalities. State governors also have the authority to declare public health emergencies by executive order or other declaration. State declared public health emergencies could also involve a significant risk of substantial harm to DOI personnel or visitors at DOI buildings, facilities and events.

Executive Order 14043, *Requiring Coronavirus Disease 2019 Vaccination for Federal Employees*, signed September 9, 2021, establishes mandatory requirements for Federal executive agencies to implement a program to require COVID-19 vaccinations for Federal employees, with some exceptions as required by law. Additionally, Executive Order 14042, *Ensuring Adequate COVID Safety Protocols for Federal Contractors*, signed September 9, 2021, establishes requirements for Federal executive agencies to implement workplace safety protocols for contractors and subcontractors to protect the health and safety of the Federal workforce and members of the public. DOI is

implementing these requirements to ensure the safety of its workforce and visitors to its facilities and sponsored events.

DOI will collect and maintain information within the scope of this system of records when it is determined that it is authorized and necessary to meet Federal requirements and respond to a declared public health emergency. To make this determination, DOI will evaluate the privacy risks for the collection of information, who the information pertains to, how the information is used and shared, the actions needed to protect individuals and respond to the public health emergency, and the laws that may apply, including the U.S. Constitution, Executive orders, Federal privacy laws, Federal labor and employment laws, and Federal workforce health and safety laws.

DOI will only collect the minimum information necessary to respond to COVID-19, or future high consequence public health threat, and comply with Federal workforce safety requirements, when DOI determines that a significant risk of substantial harm exists to individuals working at or visiting a DOI controlled facility, or attending a DOI sponsored event in a non-DOI controlled facility. These circumstances may include mitigation response activities in response to: (1) an Executive order or mandate or health related declaration of a national emergency by the President; (2) a declared public health emergency by the HHS Secretary; (3) when designated Federal or state officials make a declaration or official determination that a public health emergency exists; or (4) when DOI determines that a significant risk of substantial harm exists to the health of DOI personnel or visitors and it is necessary to ensure their health and safety in accordance with the Centers for Disease Control and Prevention (CDC) and other Federal and local guidance on communicable disease.

DOI's responsibilities for ensuring a safe workforce and secure buildings and workspaces depend on the nature and circumstances of the public health emergency. In order to meet requirements for workforce safety and the Federal government-wide

COVID-19 response, DOI must collect information on its workforce related to the COVID-19 disease to protect its workforce and customers. DOI will make all efforts to minimize the collection of information to the greatest extent possible to protect individual privacy and will only share information when authorized by the subject individuals or when authorized or required by law. Records may include personally identifiable information of individuals who have: (1) contracted or may have been exposed to a suspected or confirmed disease or illness that is the subject of a declared public health emergency; (2) attested to their vaccination status or are required to participate in a vaccination program; or (3) are required to participate in a testing program or have undergone testing for a disease or illness that is the subject of a declared public health emergency or a Federal, state, or local public health order. Records on individuals may include circumstances and dates of suspected exposure; symptoms, referrals and results of screening or treatments; health status information; and related medical information such as vaccination records and results of testing for disease or illness. DOI may also collect location and dates of potential exposure, information related to employee requests for reasonable accommodation, and other information that may be relevant or required for DOI to comply with Federal guidelines and prevent or slow the spread of the COVID-19 disease and mitigate health impacts to DOI personnel, visitors, and other individuals at DOI controlled facilities and sponsored events.

DOI is establishing a screening testing program for SARS-CoV-2, the virus that causes COVID-19, in limited circumstances to test personnel who work onsite and who are not fully vaccinated and have requested a legal exception under the law for reasonable accommodations due to medical reasons or religious belief. The purpose of the testing is to identify asymptomatic or presymptomatic infected individuals who may have been exposed to the SARS-CoV-2 virus to protect the health and safety of individuals in DOI buildings, facilities, and events. Employees who are fully vaccinated generally do not

need to participate in the testing program. An employee's failure to comply with vaccination or testing requirements may result in disciplinary action, including an adverse action. However, records of proposed disciplinary actions are maintained in other employee personnel records under a separate SORN and will not be maintained in this system of records.

Federal civilian employee medical records are covered by a government-wide Privacy Act SORN published by the Office of Personnel Management (OPM), OPM/GOVT-10, Employee Medical File System Records (75 FR 35099, June 21, 2010; modification published at 80 FR 74815, November 30, 2015). These Federal employee confidential medical records are managed in accordance with OPM regulations at 5 CFR part 293, the OPM/GOVT-10 SORN, and its published routine uses. The OPM/GOVT-10 SORN covers Federal civilians that are identified under Title 5 U.S.C. chapter 21. The majority of DOI Federal employees fall under Title 5 and their medical records are covered by the OPM/GOVT-10 SORN and must be managed in accordance with that SORN and applicable OPM regulations.

This DOI-92 notice covers DOI employees and individuals that do not fall under Title 5 and OPM's personnel recordkeeping authority and thus are not covered by the OPM/GOVT-10 SORN. This includes DOI workers, such as Title 25 Indian education personnel and any other DOI workers, to the extent they are not Federal employees as defined under 5 U.S.C. 2105 or are not subject to OPM regulations. This system may also include information collected or maintained on DOI personnel, contractors, partners, detailees, volunteers, interns, long-term trainees, and visitors at or on facilities, buildings, grounds, and properties that are owned, operated, leased, managed or used by DOI, or DOI sponsored meetings and events. The information collected is required to conduct health screening for COVID-19 or other high consequence public health threat, and will be used to prevent the spread of disease and reduce the risk of individuals with symptoms

of a communicable disease entering a DOI building, facility, or DOI hosted event. As part of health screening efforts, DOI may be required to monitor symptoms to identify persons who may have been exposed to communicable disease, or identify and notify personnel or visitors who were present in a DOI building, facility or event that may have had physical contact with or come into close proximity with individuals who were infected or had symptoms of infection with a communicable disease.

Information in this system may be shared with other DOI bureaus and offices that have a need to know to carry out their mission-essential functions, when it is determined that the sharing is authorized under applicable laws and DOI policy and it is necessary to allow DOI to manage a vaccination and testing program and respond to a declared public health emergency. To the extent permitted by law, DOI may also share information with appropriate Federal, state, local, tribal, territorial, foreign, or international government agencies when authorized and compatible with the purpose of this system, or when proper and necessary, consistent with the routine uses set forth in this system of records notice.

II. Privacy Act

The Privacy Act of 1974, as amended, embodies fair information practice principles in a statutory framework governing the means by which Federal agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to records about individuals that are maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines an individual as a United States citizen or lawful permanent resident. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DOI by complying with DOI Privacy Act regulations at 43 CFR part 2,

subpart K, and following the procedures outlined in the Records Access, Contesting Record, and Notification Procedures sections of this notice.

The Privacy Act requires each agency to publish in the *Federal Register* a description denoting the existence and character of each system of records that the agency maintains and the routine uses of each system. The INTERIOR/DOI-92, Public Health Emergency Response Records, SORN is published in its entirety below. In accordance with 5 U.S.C. 552a(r), DOI has provided a report of this system of records to the Office of Management and Budget and to Congress.

III. Public Participation

You should be aware your entire comment including your personally identifiable information, such as your address, phone number, email address, or any other personal information in your comment, may be made publicly available at any time. While you may request to withhold your personally identifiable information from public review, we cannot guarantee we will be able to do so.

SYSTEM NAME AND NUMBER:

INTERIOR/DOI-92, Public Health Emergency Response Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Records are maintained by the Office of Occupational Safety and Health, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240; all DOI bureaus and offices in Washington, DC, and in field locations; and DOI contractor facilities.

SYSTEM MANAGER(S):

Director, Office of Occupational Safety and Health, U.S. Department of the Interior, 1849 C Street NW, Office 4316, Mail Stop 4310, Washington, DC 20240.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 301; Section 319 of the Public Health Service (PHS) Act (42 U.S.C. 247d); 40 U.S.C. 1315; Coronavirus Aid, Relief, and Economic Security (CARES) Act, Public Law 116-136, Div. B., Title VIII, sec. 18115, 134 Stat. 574 (codified in 42 U.S.C. 274d note); Americans with Disabilities Act, 42 U.S.C. 12112, 29 CFR 1602.14, 1630.14; the Rehabilitation Act of 1973 (Rehab Act), 29 U.S.C. 701 et seq.; Medical Examinations for Fitness for Duty Requirements, including 5 CFR part 339; the Occupational Safety and Health Act of 1970, 29 U.S.C. Chapter 15, 29 CFR part 1904, 29 CFR 1910.1020, and 29 CFR 1960.66; Executive Order 13991; Executive Order 13994; Executive Order 14042; Executive Order 14043; Executive Order 12196; 5 U.S.C. 7902; 25 U.S.C. 2012, Indian Education Personnel; 25 CFR chapter I, subchapter E, Education; Section 2 of the Reorganization Plan No. 3 of 1950 (64 Stat. 1262).

PURPOSE(S) OF THE SYSTEM:

The purpose of this system is to maintain records related to DOI's response to the COVID-19 public health emergency or other high-consequence public health threat, to manage a workplace health screening and vaccination program, and document results of screening and diagnostic testing to protect the Federal workforce and stop or reduce the spread of infectious disease or illness. This system will be used to:

- (1) Comply with Executive orders, Federal Government and OSHA requirements;
- (2) Manage records as part of the COVID-19 vaccination requirement including confirming vaccination status and maintaining proof of vaccination;
- (3) Manage records related to a testing program including overseeing preventative testing to test personnel working onsite who are not fully vaccinated, and to permit entry to DOI managed or controlled facilities and events to meet Federal requirements and fulfill DOI's responsibilities to the extent permitted by law;
- (4) Conduct screening and testing for select circumstances such as employees

who have a need to physically enter another Federal facility or workspace for official DOI business;

(5) Conduct screening and testing for employees on official travel to meet local requirements where testing is a condition for entry, or for employees on official travel returning from an area of high risk of exposure as a condition of entry to a DOI facility;

(6) Document reports of illness or communicable disease that are the subject of a declaration of public health emergency by HHS or designated state officials that may pose a significant risk of substantial harm to the health of DOI personnel and visitors;

(7) Identify and provide notifications to personnel and visitors who may have been exposed to individuals while working onsite or visiting DOI buildings, facilities or events;

(8) Inform Federal, state or local public health authorities as necessary to protect public health as allowed or when required by law; and

(9) Take appropriate actions as necessary to prevent the introduction, transmission, and spread of communicable disease by persons who have contracted or were exposed to such a disease and came in close physical proximity to or had physical contact with other persons while working in or visiting a DOI facility or event.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

DOI personnel, including non-Title 5 employees, contractors, detailees, interns, volunteers, long-term trainees; DOI partners and employees and detailees from other Federal agencies; visitors or participants at DOI managed meetings, events and conferences; visitors or individuals who participate in health screening at DOI owned, operated, managed, or leased buildings and facilities; and visitors or individuals who are suspected or confirmed to have a disease or illness that is the subject of a declared public health emergency, or may have been exposed to someone who is suspected or confirmed to have a disease or illness that is the subject of a declared public health emergency.

CATEGORIES OF RECORDS IN THE SYSTEM:

Information collected for health screening includes contact information, vaccination and testing program related information, medical reports and assessments, and other related information that may be required. This information may include but is not limited to:

- Full name;
- Address;
- Bureau, office, organization, duty location, facility, work site, and specific work space(s) accessed;
- Official contact information;
- Work or personal phone number(s);
- Work or personal email address(es);
- Employee's supervisor name, address, and contact information;
- Contractor's supervisor/contracting officer representative name, address, and contact information;
- Date(s) and time(s) of entrance and exit from DOI buildings, facilities, workspaces, or events;
- Date(s) and/or circumstances of the individual's suspected or actual exposure to disease or illness including symptoms, as well as locations within DOI workplaces where an individual may have contracted or been exposed to the disease or illness;
- Names and contact information of other personnel or visitors that the individual interacted with at or on a DOI workspace, facility, or grounds during the time the individual was suspected to or had contracted the disease or illness;
- Current work status of the individual (e.g., administrative leave, sick leave, teleworking, in the office);

- Vaccination status, dates of vaccination, type of vaccine, and proof of vaccination including copies of COVID-19 Vaccination Record Card, a copy of medical records documenting vaccination, a copy of immunization records, or other official documentation containing information on vaccination;
- Medical screening information including name, date of birth, age, medical status medical history, and other information that may be required;
- Information directly related to screening and testing for disease or illness including but not limited to testing status, date and location of testing, test type, test results, disease type, symptoms, treatments;
- Dates and source of exposure, and recent dates and DOI locations and workspaces visited; and
- Other information that may be relevant and necessary to achieve the purpose of health screening or the vaccination and testing program.

For other agency Federal employees, detailees, partners, non-DOI contractors, visitors and members of the public at or on DOI owned, operated, leased or managed buildings, facilities, and events, the following information may be collected:

- Full name;
- Preferred phone number(s);
- Preferred email address(es);
- Name(s) and contact information for DOI personnel sponsoring visitors or participants at meetings or conferences or meetings in or at DOI workspaces, facilities, buildings, parks and grounds;
- Name(s) of individuals encountered while in or at DOI workspaces, facilities, buildings, parks and grounds;
- Information directly related to screening and testing for disease or illness including but not limited to date of testing, frequency of testing, test results,

symptoms, treatments;

- Dates and source of exposure, and recent dates and DOI locations and workspaces visited;
- Vaccination status, including fully vaccinated, not vaccinated, or decline to provide status; and
- Date(s) and time(s) of entrance and exit from DOI buildings, facilities, or events, or other related information. Information on entry and exit from DOI buildings may be obtained from the INTERIOR/DOI-46, Physical Security Access Files, system when relevant and necessary to achieve the purpose of this SORN.

This system may also include records on individuals created, collected or required to be reported to health officials in accordance with the requirements of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which requires laboratories that perform or analyze a test that is intended to detect or to diagnose a possible case of COVID-19 to report the result of that testing to public health officials. This information includes:

- Full Name;
- Address; and
- Test results.

RECORD SOURCE CATEGORIES:

Records are obtained from DOI personnel, partners, other Federal agency employees, and individuals who provide relevant information on vaccination, testing or exposure to COVID-19 or other high-consequence public health threat; visitors at DOI owned, operated, leased or managed buildings, facilities or events; their family members or other potential source of exposure to COVID-19 or other high-consequence public health threat; DOI, bureau, and office records including other systems of records; contractors or service providers performing testing, screening or related services; other

Federal or state agencies, public health organizations, or physicians with consent of the subject individual or when authorized by law; employers and other entities and individuals who may provide relevant information on a suspected or confirmed disease or illness that is the subject of a declared public health emergency.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOI as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

- (1) DOI or any component of DOI;
- (2) Any other Federal agency appearing before the Office of Hearings and Appeals;
- (3) Any DOI employee or former employee acting in his or her official capacity;
- (4) Any DOI employee or former employee acting in his or her individual capacity when DOI or DOJ has agreed to represent that employee or pay for private representation of the employee; or
- (5) The United States Government or any agency thereof, when DOJ determines that DOI is likely to be affected by the proceeding.

B. To a congressional office when requesting information on behalf of, and at the request of, the individual who is the subject of the record.

C. To the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's

behalf, or for a purpose compatible with the reason for which the records are collected or maintained.

D. To any criminal, civil, or regulatory law enforcement authority (whether Federal, state, territorial, local, tribal or foreign) when a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature, and the disclosure is compatible with the purpose for which the records were compiled.

E. To an official of another Federal agency to provide information needed in the performance of official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains.

F. To Federal, state, territorial, local, tribal, or foreign agencies that have requested information relevant or necessary to the hiring, firing or retention of an employee or contractor, or the issuance of a security clearance, license, contract, grant or other benefit, when the disclosure is compatible with the purpose for which the records were compiled.

G. To representatives of the National Archives and Records Administration (NARA) to conduct records management inspections under the authority of 44 U.S.C. 2904 and 2906.

H. To state, territorial and local governments and tribal organizations to provide information needed in response to court order and/or discovery purposes related to litigation, when the disclosure is compatible with the purpose for which the records were compiled.

I. To an expert, consultant, grantee, or contractor (including employees of the contractor) of DOI that performs services requiring access to these records on DOI's behalf to carry out the purposes of the system.

J. To appropriate agencies, entities, and persons when:

(1) DOI suspects or has confirmed that there has been a breach of the system of records;

(2) DOI has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOI (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 DOI's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

K. To another Federal agency or Federal entity, when DOI 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.

L. To the Office of Management and Budget (OMB) during the coordination and clearance process in connection with legislative affairs as mandated by OMB Circular A-19.

M. To the Department of the Treasury to recover debts owed to the United States.

N. To the news media and the public, with the approval of the Public Affairs Officer in consultation with counsel and the Senior Agency Official for Privacy, where there exists a legitimate public interest in the disclosure of the information, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

O. To appropriate Federal, state, local, tribal, or foreign governmental agencies

or multilateral governmental organizations, to the extent permitted by law, and in consultation with legal counsel, for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats.

P. To Federal agencies such as the Health and Human Services (HHS), State and local health departments, and other public health or cooperating medical authorities in connection with program activities and related collaborative efforts to deal more effectively with exposures to communicable diseases, and to satisfy mandatory reporting requirements when applicable.

Q. To missing person or location organizations where DOI does not have sufficient contact information to the extent necessary to obtain information to aid in locating persons who were possibly exposed or exposed others to a communicable disease at a DOI facility.

R. To a contractor or shared service provider conducting health screening, testing or notification activities on behalf of DOI, to help DOI manage vaccination and testing program records and procedures, and implementation of health screening, testing, and contact tracing.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Electronic records are stored in secure facilities. Confidential employee records are maintained with appropriate administrative, physical and technical controls to protect individual privacy. Paper records are contained in file folders stored in file cabinets in secure office locations.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by any of the categories of records, including name, location, date of exposure, or work status.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

In accordance with the ADA and the Rehabilitation Act, information in this system must be maintained as confidential medical records, on separate forms and in separate medical files (42 U.S.C. 12112(d)(3)(B); 42 U.S.C. sec 2000ff-5(a); 29 CFR 1630.14(b)(1), (c)(1), (d)(4)(i); and 29 CFR 1635.9(a)). Therefore, these records must be stored separately from other personnel records and must be maintained for at least one year from creation date (29 CFR 1602.14).

Records in this system are maintained in accordance with the NARA General Records Schedule (GRS) 2.7, Item 060, Occupational individual medical case files, which covers OSHA medical records and medical surveillance records that include personal and occupational health histories. The disposition is temporary. Short-term records are destroyed one year after employee separation or transfer (DAA-GRS-2017-0010-0010). Long-term records are destroyed 30 years after employee separation or when the employee's Official Personnel Folder is destroyed, whichever is longer (DAA-GRS-2017-0010-0009). Visitor processing records are covered by GRS 5.6, Items 110 and 111, and must be destroyed when either two or five years old, depending on security level, but may be retained longer if required for business use, pursuant to DAA-GRS-2017-0006-0014 and -0015.

Approved destruction methods for temporary records that have met their retention period include shredding or pulping paper records, and erasing or degaussing electronic records in accordance with DOI policy and NARA guidelines.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records contained in this system are safeguarded in accordance with 43 CFR

2.226 and other applicable security and privacy rules and policies. During normal hours of operation, paper records are maintained in locked file cabinets under the control of authorized personnel. Computer servers on which electronic records are stored are located in secured DOI controlled facilities with physical, technical and administrative levels of security to prevent unauthorized access to the DOI network and information assets. Access is only granted to authorized personnel and each person granted access to the system must be individually authorized to use the system. A Privacy Act Warning Notice appears on computer monitor screens when records containing information on individuals are first displayed. Data exchanged between the servers and the system is encrypted. Backup tapes are encrypted and stored in a locked and controlled room in a secure, off-site location.

Computerized records systems follow the National Institute of Standards and Technology privacy and security standards as developed to comply with the Privacy Act of 1974, as amended, 5 U.S.C. 552a; Paperwork Reduction Act of 1995, 44 U.S.C. 3501-3521 et seq.; Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq.; and the Federal Information Processing Standards 199: Standards for Security Categorization of Federal Information and Information Systems. Security controls include user identification, multi-factor authentication, database permissions, encryption, firewalls, audit logs, and network system security monitoring, and software controls.

Access to records in the system is limited to authorized personnel who have a need to access the records in the performance of their official duties, and each user's access is restricted to only the functions and data necessary to perform that person's job responsibilities. System administrators and authorized users are trained and required to follow established internal security protocols and must complete all security, privacy, and records management training and sign the DOI Rules of Behavior. DOI has conducted privacy impact assessments on the collection of information for the vaccination program

and the supporting IT system to identify and evaluate potential privacy risks and ensure appropriate safeguards are implemented to protect privacy.

RECORD ACCESS PROCEDURES:

An individual requesting records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked “PRIVACY ACT REQUEST FOR ACCESS.” A request for access must meet the requirements of 43 CFR 2.238.

CONTESTING RECORD PROCEDURES:

An individual requesting corrections or the removal of material from his or her records should send a signed, written request to the System Manager identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. A request for corrections or removal must meet the requirements of 43 CFR 2.246.

NOTIFICATION PROCEDURES:

An individual requesting notification of the existence of records on himself or herself should send a signed, written inquiry to the System Manager identified above. The request must include the specific bureau or office that maintains the record to facilitate location of the applicable records. The request envelope and letter should both be clearly marked “PRIVACY ACT INQUIRY.” A request for notification must meet the requirements of 43 CFR 2.235.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Teri Barnett,
Departmental Privacy Officer,
Department of the Interior.

[FR Doc. 2021-24024 Filed: 11/1/2021 11:15 am; Publication Date: 11/4/2021]