

**SYSTEM NAME AND NUMBER:**

Health Emergency Records—NRC 46.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

Headquarters, 11555 Rockville Pike, Rockville, Maryland. Records may be maintained at all locations at which the NRC, or contractors on behalf of the NRC, operate or at which NRC operations are supported.

**SYSTEM MANAGER(S):**

Chief Human Capital Officer, Office of the Chief Human Capital Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Workforce safety Federal requirements, which include: the Occupational Safety and Health Act of 1970; Executive Order 12196; and 5 U.S.C. 7902, "Safety programs." Federal laws that authorize the NRC to create and maintain Federal records of agency activities, which include: 44 U.S.C. 3101; the Religious Freedom Restoration Act of 1933, 42 U.S.C. Chapter 21B; Title VII of the Civil Rights Act of 1964, as amended, 42 U.S.C. 2000e; and the Rehabilitation Act of 1973, as amended, 29 U.S.C. 701 *et seq.* Authorities addressing the federal government's preparation for, and response to, public health threats, including the PREVENT Pandemics Act, 42 U.S.C. § 300hh-3; and Executive Order **13987**, "**Organizing and Mobilizing the United States Government to Provide a Unified and Effective Response to Combat COVID-19 and to Provide United States Leadership on Global Health and Security.**"

**PURPOSE(S) OF THE SYSTEM:**

Maintaining records necessary and relevant to NRC activities responding to and mitigating high-consequence public health threats. Records may include, but are not limited to,

those applicable health related records needed to understand the impact of an illness or disease on the NRC workforce or to assist the NRC in protecting its workforce from a declared public health emergency, pandemic, or other high-consequence public health threat, including records submitted by NRC personnel or by the lawful representative of such personnel.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

NRC's employees.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Records maintained in this system may include:

A. Full name, NRC employee ID number; telephone number, worksite, email address, supervisor's name, address and contact information.

C. Other information about the individual directly related to the disease or illness (e.g., testing results/information, symptoms, treatments, source of exposure, or other applicable health related information).

D. Appointment scheduling information, including the date, time, and location of a scheduled appointment.

E. Medical screening information, including the individual's name, date of birth, age, category of employment, current medical status, related medical history, and any relevant medical history.

**RECORD SOURCE CATEGORIES:**

Records may be obtained from NRC employees or their representative who may provide relevant information on a suspected or confirmed disease or illness, or the prevention of such disease or illness, which is the subject of a high-consequence public health threat.

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

In addition to the other types of disclosures permitted under subsection (b) of the Privacy Act, the NRC may disclose information contained in this system of records without the consent

of the persons or entities mentioned herein if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

A. To appropriate medical facilities, or Federal, State, local, Tribal, territorial or foreign government agencies, to the extent permitted by law, for the purpose of protecting the vital interests of individual(s), including to assist the United States Government in responding to or mitigating high-consequence public health threats.

B. To determine eligibility for access to NRC buildings, NRC licensee facilities or sites, or other Federal facilities.

C. To provide licensees information needed for unescorted access or access to the licensee's facility(s).

D. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law—criminal, civil, or regulatory in nature—the relevant records may be referred to the appropriate Federal, State, local, territorial, Tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.

E. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when the NRC determines that the records are arguably relevant to its proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

F. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an NRC function related to this system of records.

G. A record on an employee from this system of records may be disclosed as a routine use to a Federal, State, local, territorial, Tribal, or foreign agency requesting a record that is relevant and necessary to its decision on a matter of hiring or retaining an employee, issuing a

security clearance, reporting an investigation of that individual, letting a contract, or issuing a license, grant, or other benefit.

H. A record on an employee from this system of records may be disclosed as a routine use to a Congressional office in response to an inquiry from the Congressional office made at the request of that individual.

I. To the National Archives and Records Administration for purposes of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

J. To appropriate agencies, entities, and persons when (1) the NRC suspects or has confirmed that there has been a breach of the system of records. (2) the NRC has determined that as a result of the suspected or confirmed breach there is a risk of harm to an individual(s), the NRC (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 the NRC'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 the NRC determines that information from this system of records is 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 any agency, organization, or individual for the purpose of performing authorized audit or oversight operations of the NRC and meeting related reporting requirements.

M. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

N. A record from this system of records may be disclosed as a routine use to NRC-paid experts or consultants, and those under contract with the NRC on a "need-to-know" basis for

purpose within the scope of the pertinent NRC task. This access will be granted to an NRC contractor or employee of such contractor by a system manager only after satisfactory justification has been provided to the system manager.

O. To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information.

#### **POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

All records in this system of records are maintained and in compliance with applicable executive orders, statutes, and agency implementing recommendations. Electronic records are stored in databases. Paper records are maintained in a secure, access-controlled room, with access limited to authorized personnel.

#### **POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records will be retrieved by any of the categories of records, including name, location, date of applicable health information, or work status.

#### **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

To the extent applicable, to ensure compliance with Americans with Disabilities Act, the Rehabilitation Act, and the Genetic Information Nondiscrimination Act of 2008, medical information must be “maintained on separate forms and in separate medical files and be treated as a confidential medical record.” 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). This means that medical information and documents must be stored separately from other personnel records. As such, the NRC must keep medical records for at least 1 year from creation date. 29 CFR 1602.14. Further, records compiled under this system of records notice will be maintained in accordance with the National Archives and Records Administration General Records Schedule (GRS) 2.7, Employee Health and Safety Records, Items 010, 070, or 080 to the extent applicable.

GRS 2.7 item 010 (DAA-GRS-2017-0010-0001)—Clinic scheduling records. Temporary.

Destroy when 3 years old, but longer retention is authorized if needed for business use.

GRS 2.7 item 070 (DAA-GRS-2017-0010-0012)—Non-occupational individual case files. Temporary. Destroy 10 years after the most recent encounter, but longer retention is authorized if needed for business use.

GRS 2.7 item 080 (DAA-GRS-2017-0010-0013)—Non-occupational health and wellness program records. Temporary. Destroy 3 years after the project/activity/or transaction is completed or superseded, but longer retention is authorized if needed for business use.

GRS 2.7 item 063 (DAA-GRS-2021-0003-0001)—Vaccination attestations and proof of vaccination records. Federal employees and contractors. Temporary. Destroy when 3 years old.

GRS 2.7 item 064 (DAA-GRS-2021-0003-0002)—Vaccination attestations and proof of vaccination records. Visitors. Temporary. Destroy when 30 days old.

#### **ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

The NRC safeguards records in this system according to applicable rules and policies, including all applicable NRC automated systems security and access policies. The NRC has imposed controls to minimize the risk of compromising the information that is being stored. Users of individual computers can only gain access to the data by valid user identification and password. Paper records are maintained in a secure, access- controlled room, with access limited to authorized personnel.

#### **RECORDS ACCESS PROCEDURES:**

Same as "Notification procedures."

#### **CONTESTING RECORD PROCEDURES:**

Same as "Notification procedures."

#### **NOTIFICATION PROCEDURES:**

Individuals seeking to determine whether this system of records contains information about them should write to the Freedom of Information Act Officer or Privacy Act Officer, Office

of the Chief Information Officer, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, and comply with procedures contained in NRC's Privacy Act regulations, 10 CFR part 9.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.