U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collection requirements, and records management requirements.

Employee Medical File (EMF) – COVID19

Date: September 17, 2021

A. GENERAL SYSTEM INFORMATION

1. Provide a detailed description of the system: (*Use plain language, no technical terms.*)

This information is being collected and maintained to promote the safety of Federal workplaces and the Federal workforce consistent with the above-referenced authorities, Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.

2. What agency function does it support? (*How will this support the U.S. Nuclear Regulatory Commission's (NRC's) mission, which strategic goal?)*)

Required per Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (Sept. 9, 2021).

3. Describe any modules or subsystems, where relevant, and their functions.

None.

a. Provide ADAMS ML numbers for all Privacy Impact Assessments or Privacy Threshold Analysis for each subsystem.

N/A.

4. What legal authority authorizes the purchase or development of this system? (*What law, regulation, or Executive Order authorizes the collection and maintenance of the information necessary to meet an official program mission or goal? NRC internal policy is not a legal authority.*)

Pursuant to 5 U.S.C. chapters 11 and 79, and in discharging the functions directed under Executive Order 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (Sept. 9, 2021), we are authorized to collect

this information. The authority for the system of records notice (SORN) associated with this collection of information, OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), also includes 5 U.S.C. chapters 33 and 63 and Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980).

5. What is the purpose of the system and the data to be collected?

This information is being collected and maintained to promote the safety of Federal workplaces and the Federal workforce consistent with the above-referenced authorities, Executive Order 13991, Protecting the Federal Workforce and Requiring Mask-Wearing (Jan. 20, 2021), the COVID-19 Workplace Safety: Agency Model Safety Principles established by the Safer Federal Workforce Task Force, and guidance from Centers for Disease Control and Prevention and the Occupational Safety and Health Administration.

6. Points of Contact: (*Do not adjust or change table fields. Annotate N/A if unknown. If multiple individuals need to be added in a certain field, please add lines where necessary*.)

Project Manager	**Office/Division/Branch**	**Telephone**
N/A		
Business Project Manager	**Office/Division/Branch**	**Telephone**
Bi Smith	OCHCO	301-287-0553
Technical Project Manager	**Office/Division/Branch**	**Telephone**
Basia Sall	OCIO/SDOD	301-415-2174
Executive Sponsor	**Office/Division/Branch**	**Telephone**
Mary Lamary	OCHCO	301-415-3300
ISSO	**Office/Division/Branch**	**Telephone**
Julie Hughes	OCIO/GEMS/CSB	301/415-2362
System Owner/User	**Office/Division/Branch**	**Telephone**
Mary Lamary	OCHCO	301-415-3300

7. Does this privacy impact assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. __X__ New System

____ Modify Existing System

____ Other

b. If modifying or making other updates to an existing system, has a PIA been prepared before?

N/A.

(1) If yes, provide the date approved and the Agencywide Documents Access and Management System (ADAMS) accession number.

N/A.

(2) If yes, provide a summary of modifications or other changes to the existing system.

N/A.

8. Do you have an NRC system Enterprise Architecture (EA)/Inventory number?

Yes.

a. If yes, please provide the EA/Inventory number.

EA Number 20090005.

b. If, no, please contact EA Service Desk to get the EA/Inventory number.

B. INFORMATION COLLECTED AND MAINTAINED

These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.

1. **INFORMATION ABOUT INDIVIDUALS**

a. Does this system maintain information about individuals?

Yes.

(1) If yes, identify the group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public (provide description for general public (non-licensee workers, applicants before they are licenses etc.)).

Federal Employees only.

(2) IF NO, SKIP TO QUESTION B.2.

b. What information is being maintained in the system about an individual (<u>be specific</u> – e.g. Social Security Number (SSN), Place of Birth, Name, Address)?

Name, Vaccination Status, Date of Birth, Vaccination Type, LANID.

c. Is information being collected from the subject individual? (*To the greatest extent possible, collect information about an individual directly from the individual.*)

Yes.

(1) If yes, what information is being collected?

- Name of employee
- Type of vaccine administered;
- Number of doses received;
- Date(s) of administration; AND
- Name of the health care professional(s) or clinic site(s) administering the vaccine(s).
- A copy of the record of immunization from a health care provider or pharmacy;
- A copy of the COVID-19 Vaccination Record Card (CDC Form MLS-319813_r, published on September 3, 2020);
- A copy of medical records documenting the vaccination;
- A copy of immunization records from a public health or state immunization information system; OR
- A copy of any other official documentation containing required data points.

d. Will the information be collected from individuals who are not Federal employees?

No.

(1) If yes, does the information collection have the Office of Management and Budget's (OMB) approval?

N/A.

(a) If yes, indicate the OMB approval number:

N/A.

e. Is the information being collected from existing NRC files, databases, or systems?

No.

(1) If yes, identify the files/databases/systems and the information being collected.

N/A.

f. Is the information being collected from external sources (any source outside of the NRC)?

No.

(1) If yes, identify the source and what type of information is being collected?

N/A.

g. How will information not collected directly from the subject individual be verified as current, accurate, and complete?

Yes.

h. How will the information be collected (e.g. form, data transfer)?

Microsoft Forms.

2. INFORMATION NOT ABOUT INDIVIDUALS

a. Will information not about individuals be maintained in this system?

No.

(1) If yes, identify the type of information (be specific).

N/A.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

N/A.

C. USES OF SYSTEM AND INFORMATION

These questions will identify the use of the information and the accuracy of the data being used.

1. Describe all uses made of the data in this system.

While the information requested is intended to be used primarily for internal purposes, in certain circumstances it may be necessary to disclose this information externally, for example to disclose information to: a Federal, State, or local agency to the extent necessary to comply with laws governing reporting of communicable disease or other laws concerning health and safety in the work environment; to adjudicative bodies (e.g., the Merit System Protection Board), arbitrators, and hearing examiners to the extent necessary to carry out their authorized duties regarding Federal employment; to contractors, grantees, or volunteers as necessary to perform their duties for the Federal Government; to other agencies, courts, and persons as necessary and relevant in the course of litigation, and as necessary and in accordance with requirements for law enforcement; or to a person authorized to act on your behalf. A complete list of the routine uses can be found in the SORN associated with this collection of information.

2. Is the use of the data both relevant and necessary for the purpose for which the system is designed?

Yes.

3. Who will ensure the proper use of the data in this system?

Office of the Chief Human Capital Officer (OCHCO).

4. Are the data elements described in detail and documented?

Yes.
https://forms.office.com/Pages/ResponsePage.aspx?id=dRTQ6LXDakOgZV3vTGT1Lg-8M5WGdLZChbmLN7crQXJUQUhWUFFUMjBSNUtKWk1XNk1KTVNRVDZXMyQlQCN0PWcu

a. If yes, what is the name of the document that contains this information and where is it located?

It is located in a Microsoft Team that is locked down via permissions to the six team members from OCHCO, the Office of the Chief Information Officer (OCIO), and the Office of Administration (ADM).

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

No.

Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data (i.e. tables or data arrays).

a. If yes, how will aggregated data be maintained, filed, and utilized?

N/A.

b. How will aggregated data be validated for relevance and accuracy?

N/A.

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

N/A.

6. How will data be *retrieved* from the system? Will data be retrieved by an individual's name or personal identifier (name, unique number or symbol)? (Be specific.)

Yes.

a. If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

Employee Name.

7. Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register?

Yes.

a. If "Yes," provide name of SORN and location in the Federal Register.

OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), also includes 5 U.S.C. chapters 33 and 63 and Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980).

8. If the information system is being modified, will the SORN(s) require amendment or revision?

No.

9. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No.

a. If yes, explain.

N/A.

(1) What controls will be used to prevent unauthorized monitoring?

N/A.

10. List the report(s) that will be produced from this system.

- Total Employees Covered by the Vaccination Requirement Under EO 14043.
- Total Fully Vaccinated Employees (and whether documentation has been received and reviewed).
- Total Partially Vaccinated Employees with Second Dose (and whether documentation has been received and reviewed).
- Total Partially Vaccinated Employees with First Dose (and whether documentation has been received and reviewed).
- Total Unvaccinated Employees (and whether a request for a legally required exception is pending or approved).
- Total Employees Whose Vaccination Status is Unknown to Agency.

a. What are the reports used for?

The reports are used to provide OMB the status of the NRC staff's compliance with EO 14043.

b. Who has access to these reports?

OCHCO, ADM, and OCIO limited to those that have a need to know.

D. ACCESS TO DATA

1. Which NRC office(s) will have access to the data in the system?

OCIO, OCHCO, and ADM.

(1) For what purpose?

- To assess data and fulfill mandated reporting requirements.
- To maintain system security.
- To provide technical support for system operation and maintenance.

(2) Will access be limited?

Yes, access will be restricted to only those that have a need to know.

2. Will other NRC systems share data with or have access to the data in the system?

No.

(1) If yes, identify the system(s).

N/A.

(2) How will the data be transmitted or disclosed?

N/A.

3. Will external agencies/organizations/public have access to the data in the system?

No.

(1) If yes, who?

N/A.

(2) Will access be limited?

N/A.

(3) What data will be accessible and for what purpose/use?

N/A.

(4) How will the data be transmitted or disclosed?

N/A.

E. RECORDS AND INFORMATION MANAGEMENT (RIM) - RETENTION AND DISPOSAL

The National Archives and Records Administration (NARA), in collaboration with federal agencies, approves whether records are temporary (eligible at some point for destruction/deletion because they no longer have business value) or permanent (eligible at some point to be transferred to the National Archives because of historical or evidential significance). These determinations are made through records retention schedules and NARA statutes (44 United States Code (U.S.C.), 36 Code of Federation Regulations (CFR)). Under 36 CFR 1234.10, agencies are required to establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. The following question is intended to determine whether the records and data/information in the system have approved records retention schedule and disposition instructions, whether the system incorporates Records and Information Management and NARA's Universal Electronic Records Management requirements, and if a strategy is needed to ensure compliance.

1) Can you map this system to an applicable retention schedule in NRC's Comprehensive Records Disposition Schedule (NUREG-0910), or NARA's General Records Schedules (GRS)?

Yes, however additional guidance and a revised GRS is forthcoming from NARA so these records will need to be scheduled accordingly:

Memorandum to Federal Agency Contacts: New GRS items for vaccination attestations and vaccine testing records.

Additional information/data/records may need to be scheduled; therefore, NRC records personnel will need to work with staff and NARA to develop a records retention and disposition schedule for records created or maintained. Until the approval of such schedule, these records and information are Permanent. Their willful disposal or concealment (and related offenses) is punishable by fine or imprisonment, according to 18 U.S.C., Chapter 101, and Section 2071. Implementation of retention schedules is mandatory under 44 U.S. 3303a (d), and although this does not prevent further development of the project, retention functionality or a manual process must be incorporated to meet this requirement.

a. If yes, please cite the schedule number, approved disposition, and describe how this is accomplished (then move to F.1).

- **For example, will the records or a composite thereof be deleted once they reach their approved retention or exported to an approved file format for transfer to the National Archives based on their approved disposition?**

The following is the retention mentioned in the OPM/GOVT – 10 SORN:

The EMF is maintained for the period of the employee's service in the agency and is then transferred to the National Personnel Records Center

for storage, or as appropriate, to the next employing Federal agency. Other medical records are either retained at the agency for various lengths of time in accordance with the National Archives and Records Administration's records schedules or destroyed when they have served their purpose or when the employee leaves the agency. Within 90 days after the individual separates from the Federal service, the EMF is sent to the National Personnel Records Center for storage. Destruction of the EMF is in accordance with General Records Schedule-1(21). Records arising in connection with employee drug testing under Executive Order 12564 are generally retained for up to 3 years. Records are destroyed by shredding, burning, or by erasing the disk.

GRS 2.7: Employee Health and Safety Records

GRS 2.7 item 070: Non-occupational individual medical case files. Records of treatment or examination created and maintained by a health care facility or dispensary documenting an individual's medical history, physical condition, vaccinations, and first-aid visits for nonwork-related purposes. Also referred to as "patient records" in Title 5 Part 293 Subpart E.

Temporary. Destroy 10 years after the most recent encounter, but longer retention is authorized if needed for business use.

b. If no, please contact the RIM staff at ITIMPolicy.Resource@nrc.gov.

F. TECHNICAL ACCESS AND SECURITY

1. Describe the security controls used to limit access to the system (e.g., passwords).

Restricted access to only those that have a need to know.

2. What controls will prevent the misuse (e.g., unauthorized browsing) of system data by those having access?

Information is locked down as private M365 group . The change would have to be approved by OCHCO.

3. Are the criteria, procedures, controls, and responsibilities regarding access to the system documented?

Yes.

(1) If yes, where?

This information is the standard build for MS365 for system documentation.

4. Will the system be accessed or operated at more than one location (site)?

No.

a. If yes, how will consistent use be maintained at all sites?

N/A.

5. Which user groups (e.g., system administrators, project managers, etc.) have access to the system?

The user group created is only accessible to the six team members identified at the beginning of the document.

6. Will a record of their access to the system be captured?

Yes, logging information is captured when accessing the data.

a. If yes, what will be collected?

Yes, logging information is captured when accessing the data.

7. Will contractors be involved with the design, development, or maintenance of the system?

No.

If yes, and if this system will maintain information about individuals, ensure Privacy Act and/or Personally Identifiable Information (PII) contract clauses are inserted in their contracts.

- *Federal Acquisition Regulation (FAR) clause 52.224-1 and FAR clause 52.224-2 should be referenced in all contracts, when the design, development, or operation of a system of records on individuals is required to accomplish an agency function.*

- *PII clause, "Contractor Responsibility for Protecting Personally Identifiable Information" (June 2009), in all contracts, purchase orders, and orders against other agency contracts and interagency agreements that involve contractor access to NRC owned or controlled PII.*

8. What auditing measures and technical safeguards are in place to prevent misuse of data?

The Information Technology Infrastructure (ITI) has an ongoing authorization. The system is assessed quarterly and all significant changes to the system are assessed. The system currently meets all of its FISMA requirements and has implemented a robust continuous monitoring program. ITI is protected by firewalls, proxies, authentication gateways, encryption, network segmentation, and auditing tools that monitor for suspicious behavior. The system utilizes data

loss prevention techniques to ensure NRC sensitive data does not go beyond the boundaries of the NRC infrastructure.

9. Is the data secured in accordance with the Federal Information Security Management Act (FISMA) requirements?

Yes.

a. If yes, when was Certification and Accreditation last completed? And what FISMA system is this part of?

March 19, 2020 ITI.

b. If no, is the Certification and Accreditation in progress and what is the expected completion date? And what FISMA system is this planned to be a part of?

N/A.

c. If no, please note that the authorization status must be reported to the Chief Information Security Officer (CISO) and Computer Security Office's (CSO's) Point of Contact (POC) via e-mail quarterly to ensure the authorization remains on track.

N/A.

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OCIO/GEMSD/CSB Staff)

System Name: Employee Medical File – COVID19

Submitting Office: Office of Chief Human Capital Officer

A. PRIVACY ACT APPLICABILITY REVIEW

____ Privacy Act is not applicable.

__X__ Privacy Act is applicable.

Comments:
Covered by OPM/GOVT-10, Employee Medical File System of Records, 75 Fed. Reg. 35099 (June 21, 2010), amended 80 Fed. Reg. 74815 (Nov. 30, 2015), also includes 5 U.S.C. chapters 33 and 63 and Executive Order 12196, Occupational Safety and Health Program for Federal Employees (Feb. 26, 1980).

Reviewer's Name	Title
Signed by Hardy, Sally on 09/24/21	Privacy Officer

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

__X__ No OMB clearance is needed.

____ OMB clearance is needed.

____ Currently has OMB Clearance. Clearance No._____

Comments:
Information is being collected from only current Federal employees so no OMB clearance is needed.

Reviewer's Name	Title
Signed by Cullison, David on 09/23/21	Agency Clearance Officer

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

____ No record schedule required.

____ Additional information is needed to complete assessment.

__X__ Needs to be scheduled.

__X__ Existing records retention and disposition schedule covers the system - no modifications needed.

Comments:

Reviewer's Name	Title
 Signed by Dove, Marna on 09/24/21	Sr. Program Analyst, Electronic Records Manager

D. BRANCH CHIEF REVIEW AND CONCURRENCE

__X__ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

____ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

 Signed by Nalabandian, Garo on 09/24/21

Chief
Cyber Security Branch
Governance and Enterprise Management
Services Division
Office of the Chief Information Officer

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: Mary Lamary, Office of Chief Human Capital Officer	
Name of System: Employee Medical File – COVID19	
Date CSB received PIA for review: September 17, 2021	**Date CSB completed PIA review:** September 22, 2021
Noted Issues:	
Chief Cyber Security Branch Governance and Enterprise Management Services Division Office of the Chief Information Officer	Signature/Date: Signed by Nalabandian, Garo on 09/24/21
Copies of this PIA will be provided to: *Thomas G. Ashley, Jr.* *Director* *IT Services Development and Operations Division* *Office of the Chief Information Officer* *Jonathan R. Feibus* *Chief Information Security Officer (CISO)* *Office of the Chief Information Officer*	