




Department of Energy

Office of Science

ORNL Site Office
P.O. Box 2008
Oak Ridge, Tennessee 37831-6269

September 25, 2023

MEMORANDUM FOR W. KEN HUNT
DEPUTY CHIEF INFORMATION OFFICER
ENTERPRISE RECORDS MANAGEMENT, PRIVACY, AND COMPLIANCE

FROM: JOHNNY O. MOORE 
MANAGER
OAK RIDGE NATIONAL LABORATORY SITE OFFICE

SUBJECT: PRIVACY IMPACT ASSESSMENTS - OAK RIDGE NATIONAL
LABORATORY (ORNL)

Attached are two approved Privacy Impact Assessments for ORNL systems associated with Department of Energy (DOE) System of Records Notices 33 and 38. The three associated ORNL systems are the *Electronic Medical Business Operations System*, the *Days, Away, Restricted, Transferred* drive, and the *Comprehensive Tracking System*. Review and approval of these documents has been coordinated with your office and with the Local Privacy Officer, and they are being provided to you per DOE Order 206.1 requirements.

If there are any questions or additional information required, please contact Doug Reed at Doug.Reed@science.doe.gov.

Attachments

cc w/attachments:

Daniel S. DeVore, ORNL

Director's Files

Christopher D. Hicks, IM-42

Linda G. Chapman, SC-GCS

Michele G. Branton, SC-OSO

K. Mike Hatcher, SC-OSO

Douglas R. Reed, SC-OSO

Privacy@hq.doe.gov



Affects
Members
Of the Public?

Department of Energy

Privacy Impact Assessment (PIA)

Guidance is provided in the template. See DOE Order 206.1, Department of Energy Privacy Program, Appendix A, Privacy Impact Assessments, for requirements and additional guidance for conducting a PIA: <https://www.directives.doe.gov/directives-documents/200-series/0206.1-BOrder/@@images/file>

Please complete form and return via email to Privacy@hq.doe.gov

No hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	12/2/2022	
Departmental Element & Site	U.S. Department of Energy Office of Science Oak Ridge National Laboratory Site Office Oak Ridge National Laboratory	
Name of Information System or IT Project	Electronic Medical Business Operations System (EMBOS) (used for the storage and management of occupational health records associated with DOE-33, Personnel Medical Records)	
Exhibit Project UID		
New PIA <input checked="" type="checkbox"/>		
Update <input type="checkbox"/>		
	Name, Title	Contact Information Phone, Email
System Owner	Johnny O. Moore Manager ORNL Site Office	(865) 576-3536 johnny.moore@science.doe.gov



MODULE I – PRIVACY NEEDS ASSESSMENT

Local Privacy Act Officer	Linda Chapman DOE FOIA/Privacy Act Officer DOE Oak Ridge Office	(865) 576-2129 Linda.chapman@science.doe.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Dustin Reinert ORNL Information Systems Security Officer UT-Battelle, LLC Contractor to the US Department of Energy	865-341-2270 reinertdp@ornl.gov
Person Completing this Document	Dan DeVore ORNL Privacy Officer UT-Battelle, LLC Contractor to the US Department of Energy	(865) 341-1400 devoreds@ornl.gov
Purpose of Information System or IT Project	<p>10 C.F.R. PART 851 requires ORNL to establish and provide comprehensive occupational medicine services to employees. 10 C.F.R. PART 851 APPENDIX A requires records containing any medical, health history, exposure history, and demographic data collected for occupational medicine purposes be developed and maintained for each employee for whom medical services are provided.</p> <p>EMBOS is the web-based electronic medical records (EMR) system used by ORNL to develop, maintain, and process personnel occupational health records in accordance with these requirements. For example, ORNL health services staff use EMBOS to: (1) schedule and track occupational health appointments with employees, (2) document medical evaluations of employees, (3) review previous medical diagnosis/treatment/care of employees, and (4) maintain a complete and accurate occupational medical history for ORNL employees.</p> <p>In general, EMBOS is used to develop and maintain the information necessary to provide comprehensive occupational medicine services to employees in accordance with the requirements of 10 C.F.R. PART 851.</p> <p>The federal information maintained in EMBOS is associated with Department of Energy System of Records, DOE-33, "Personnel Medical Records."</p>	
Type of Information Collected or Maintained by the System:	<input checked="" type="checkbox"/> SSN <input checked="" type="checkbox"/> Medical & Health Information <input type="checkbox"/> Financial Information <input type="checkbox"/> Clearance Information <input type="checkbox"/> Biometric Information	



MODULE I – PRIVACY NEEDS ASSESSMENT

- Mother's Maiden Name
- DoB, Place of Birth
- Employment Information
- Criminal History
- Name, Phone, Address
- Other – (Badge Number, Gender, Race/Ethnicity)

Has there been any attempt to verify PII does not exist on the system?

DOE Order 206.1, Department of Energy Privacy Program, defines PII as any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

N/A – PII and Privacy Act Information are known to exist on this information system.

If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)

N/A – system is known to contain PII.

Threshold Questions

1. Does system contain (collect and/or maintain), or plan to contain any information about individuals?

YES

2. Is the information in identifiable form?

YES

3. Is the information about individual Members of the Public?

NO

4. Is the information about DOE or contractor employees?

YES

- Federal Employees
- Contractor Employees

If the answer to all four (4) Threshold Questions is "No," you may proceed to the signature page of the PIA. Submit the completed PNA with signature page to the CPO.



MODULE I – PRIVACY NEEDS ASSESSMENT

Module II must be completed for all systems if the answer to any of the four (4) threshold questions is “Yes.” All questions must be completed. If appropriate, an answer of N/A may be entered.

The goal of the threshold questions is to legitimately and efficiently determine whether additional assessment is necessary. If there is doubt, it is in the System Owner’s best interest to complete Module II.

PIAs affecting Members of the Public are posted on the DOE Privacy website. For this reason, PIAs affecting Members of the Public should be written in plain language and at a high level so they are easily understandable and do not disclose sensitive information.

END OF PRIVACY NEEDS ASSESSMENT

MODULE II – PII SYSTEMS & PROJECTS

AUTHORITY, IMPACT & NOTICE

1. AUTHORITY

What specific authorities authorize this system or project, and the associated collection, use, and/or retention of personal information?

10 C.F.R. PART 851 APPENDIX A requires Department of Energy (DOE) contractors to develop and maintain records containing medical history, health history, exposure history, and demographic data for each individual to whom occupational medical services are provided.

With regard specifically to the collection and storage of SSNs in occupational health records by contractors, DOE G 440.1-1B Chg 1 Section 6.6 states that “[e]xposure monitoring data should include ... [n]ame, social security number, employee identification number if different from the social security number, and job classification of the employee monitored...”



MODULE II – PII SYSTEMS & PROJECTS

<p>2. CONSENT</p> <p>What opportunities do individuals have to decline to provide information (e.g. where providing information is voluntary) or to consent only to particular uses of the information (other than required or authorized uses)?</p>	<p>Any required medical testing (blood work, x-rays, etc.) or examinations may be declined by the employee at any time, however, declination may impact an employee’s authorization to perform certain work tasks or work in specific areas. There is currently no formalized opportunity for an individual to consent to uses of information beyond what is required or authorized.</p>
<p>3. CONTRACTS</p> <p>Are contractors involved with the design, development and maintenance of the system? If yes, was the Privacy Order CRD or Privacy Act clauses included in their contracts?</p>	<p>Yes. The ORNL M&O contract includes FAR 52.224-1 Privacy Act Notification, FAR 52.224-2 Privacy Act, and requires compliance with DOE O 206.1.</p>
<p>4. IMPACT ANALYSIS:</p> <p>How does this project or information system impact privacy?</p>	<p>EMBOS maintains personally identifiable information (PII) including the types of PII indicated on page 2 of this assessment. Under Federal Information Processing Standards (FIPS) Publication 199 impact analysis, a loss of confidentiality involving the PII in EMBOS could result in a moderate potential impact to individuals (i.e. could be expected to have a serious adverse effect on individuals due to the loss of privacy).</p> <p>EMBOS is designed to protect PII and mitigate privacy risk via the following administrative, technical, and physical controls:</p> <ul style="list-style-type: none"> • Strict access control enforcement based on need-to-know <p>The Servers enclave (where EMBOS is located) implements the NIST SP 800-53 baseline controls for Moderate systems, with very limited exceptions as approved by the DOE Authorizing Official. These controls are implemented to protect the confidentiality, integrity, and availability of the PII within EMBOS.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>5. SORNs</p> <p>How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?</p> <p>If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Yes, the data can be retrieved by searching by unique identifiers of individuals. The medical records are retrievable by name, personnel number, and social security number.</p>
<p>6. SORNs</p> <p>Has a Privacy Act System of Records Notice (SORN) been published in the <i>Federal Register</i>?</p> <p>If "Yes," provide name of SORN and location in the <i>Federal Register</i>.</p>	<p>Yes.</p> <p>Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-33 Personnel Medical Records. Pages 993-1090</p>
<p>7. SORNs</p> <p>If the information system is being modified, will the SORN(s) require amendment or revision?</p>	<p>N/A.</p>

DATA SOURCES



MODULE II – PII SYSTEMS & PROJECTS

<p>8. What are the sources of information about individuals in the information system or project?</p>	<p>The individuals are the sources of information—the personal information in this system is collected directly from the individuals by ORNL.</p> <p>Specifically, the name (first, middle, last), date of birth, social security number, badge number, home phone number, gender, race/ethnicity, and work/employment information used in EMBOS are collected from and generated for employees as a part of the new employee onboarding process and for non-employees as a part of the visitor registration process (last 4 of SSN only for non-employees). After this information is collected/generated, it is maintained in the ORNL enterprise data repository (SAP), which then provides the information to EMBOS.</p> <p>This data is refreshed regularly through a daily data import from SAP to EMBOS to keep the information updated, accurate, and complete. The medical and health information in EMBOS is collected directly from the individual by ORNL Health Services and/or generated through the individual's participation in ORNL's occupational health program (e.g. medical evaluations, medical assessments, diagnostic testing, etc.)</p>
<p>9. Will the information system derive new or meta data about an individual from the information collected?</p>	<p>No.</p>
<p>10. Are the data elements described in detail and documented?</p>	<p>Yes.</p>
<p>DATA USE</p>	
<p>11. How will the PII be used?</p>	<p>The PII in EMBOS is used to develop and maintain an occupational medical record for each individual to whom occupational medical services are provided at ORNL. This enables proper medical evaluations, diagnosis, treatment and care, an accurate occupational medical history, and—in general—the information necessary to provide comprehensive occupational medicine services to employees in accordance with the requirements of 10 C.F.R. PART 851.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>12. If the system derives meta data, how will the new or meta data be used?</p> <p>Will the new or meta data be part of an individual's record?</p>	<p>N/A.</p>
<p>13. With what other agencies or entities will an individual's information be shared?</p>	<p>This information will be shared within DOE. As necessary, information may be shared with other agencies or entities as permitted by the applicable SORN cited below.</p> <p>Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-33 Personnel Medical Records Pages 993-1090</p>
<p>Reports</p>	
<p>14. What kinds of reports are produced about individuals or contain an individual's data?</p>	<p>Routine reports produced from EMBOS include appointment/scheduling reports, reports provided to individuals about themselves (exposure testing reports, lab results, etc.), work restriction reports, and fit-for-duty reports.</p>
<p>15. What will be the use of these reports?</p>	<p>Appointment/scheduling reports are used for administrative/operational purposes within ORNL Health Services. Reports provided to individuals about themselves are provided as required by 10 C.F.R. PART 851 and/or in response to a request by the individual. The restriction reports and fit-for-duty reports are provided to the individual and the individual's management to inform of work restrictions or fitness for duty.</p>
<p>16. Who will have access to these reports?</p>	<p>The appointment/scheduling reports are accessible by health services personnel. The reports provided to individuals about themselves are accessible by the individual and limited members of the ORNL health services staff. The restriction reports and fit-for-duty reports are accessible by the individual, the individual's supervisor, the workers compensation coordinator, and limited members of the ORNL health and safety team.</p>
<p>Monitoring</p>	
<p>17. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>No.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>18. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>N/A.</p>
<p>19. Are controls implemented to prevent unauthorized monitoring of individuals?</p>	<p>N/A.</p>
<p>DATA MANAGEMENT & MAINTENANCE</p>	
<p>20. How will records about individuals be kept current and verified for accuracy, relevance and completeness? Include PII data collected from sources other than DOE records.</p>	<p>Individual medical records are reviewed, updated, and verified as required by the ORNL Health Services internal operating procedure governing the management of digitized medical records. PII within EMBOS can only be updated by authorized users with EMBOS user accounts. Demographic and employment data are updated via a daily, one-way feed from ORNL’s enterprise data repository (SAP).</p>
<p>21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?</p>	<p>N/A.</p>
<p>Records Management</p>	
<p>22. Identify the record(s).</p>	<p>DOE-33 – Title: Electronic Medical Business Operations System (EMBOS) (SOR) DOE-33</p> <p>Description: Files contain employee medical information. Consists of clinical visits, incident reports, periodic physicals, lab data, x-ray data, EKG reports and outside doctor’s information, etc. Files contain medical tests results (audiograms, chemistry profile results, urinalysis, visual performances, spirometer readings, chest X-ray results, etc.). The Sent-Off-Work Log contains the name of the doctor who requested that employee be sent home. The records of current employees are in EMBOS.</p>



MODULE II – PII SYSTEMS & PROJECTS

<p>23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.</p>	<p><input type="checkbox"/> Unscheduled <input checked="" type="checkbox"/> Scheduled (cite NARA authority(ies) below)</p> <p>DOE Admin 1: 21.1B Individual Health Record Files (N1-434-98-4(21.1b))</p> <p>Retention: Destroy 75 years after date of last entry. Note: DOE EPI Hold/Moratorium is in effect.</p>
<p>24. Records Contact</p>	<p>David Whittaker whittakerdm@ornl.gov 865-576-3470</p>
<p>ACCESS, SAFEGUARDS & SECURITY</p>	
<p>25. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>The <i>Servers Enclave</i>, where this system resides, operates under a current DOE granted Authority to Operate (ATO). The security controls for this system are based on FISMA requirements to achieve compliance with Federal law and Department of Energy (DOE) policy and to protect the confidentiality, integrity, and availability of this Information System. The <i>Unclassified Cyber Security Program Plan</i> (CSPP), and the <i>Servers Enclave System Security Plan</i> (SSP) describe the technical, operational, and management controls to secure this Information System at a Moderate level.</p>
<p>26. Who will have access to PII data?</p>	<p>Access is limited to approved medical staff with a need-to-know and have approved accounts in EMBOS.</p>
<p>27. How is access to PII data determined?</p>	<p>The director of Occupational Medical determines who needs an account in the EMR.</p>
<p>28. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>Yes. Enterprise data from ORNL SAP containing employee and non-employee information will be imported into the system via a daily, one-way feed. See answer to question #8 above for additional detail.</p>
<p>29. For connecting information systems, is there an Interconnection Security Agreement (ISA) or other agreement between System Owners to ensure the privacy of individuals is protected?</p>	<p>N/A - there are no persistent connections between the EMR and other entities. Any data exchange will implement processes and requirements required for handling, storing, and transmitting PII and sensitive information as defined in ORNL Standards Based Management System (SBMS) requirements for handling sensitive information.</p>



MODULE II – PII SYSTEMS & PROJECTS

30. Who is responsible for ensuring the authorized use of personal information?

The ORNL Information System Owner (ISO) / Designee(s) of the system.

END OF MODULE II



SIGNATURE PAGE		
	Signature	Date
System Owner	<p>_____</p> <p>(Print Name)</p> <p><i>Jogam</i></p> <p>Date: 2023.09.25 15:31:47 -06'00'</p> <p>_____</p> <p>(Signature)</p>	_____
Local Privacy Act Officer	<p>_____</p> <p>(Print Name)</p> <p>Linda Chapman</p> <p>Digitally signed by Linda Chapman Date: 2023.09.11 09:11:48 -04'00'</p> <p>_____</p> <p>(Signature)</p>	_____
Ken Hunt Chief Privacy Officer	<p>_____</p> <p>(Print Name)</p> <p>William K. Hunt</p> <p>Digitally signed by William K. Hunt Date: 2023.09.08 11:26:13 -04'00'</p> <p>_____</p> <p>(Signature)</p>	_____