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	January 12th, 2024	
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	MEDSAFe (Medical Electronic Devices Security and Approval Framework)	
Exhibit Project UID	Funding provided by NNSA to ORNL/UT-Battelle under Contract No. DE-AC05-00OR22725.	
New PIA ☒ **Update** □		
	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	Medically necessary portable electronic devices (MedPEDs) (e.g. hearing aids, pacemakers, etc.) are becoming commonplace in the DOE/NNSA workforce, including some staff and authorized visitors who require access to secure areas. By default, portable electronic devices are prohibited in secure areas across the DOE/NNSA complex. While exception processes exist to permit authorized DOE/NNSA employees, contractors and site visitors with MedPEDs to access secure areas, they are implemented independently at each facility/site. The process used to evaluate and adjudicate MedPED exception requests at each facility may vary, however, there are common aspects of the request and evaluation process that could be leveraged across the DOE/NNSA enterprise to ensure consistency and efficiency, and support fair and timely determinations. Where possible, reciprocity could exist to allow appropriate staff at DOE/NNSA sites to leverage information gathered through MedPED exception requests from other DOE/NNSA sites and facilities. Implementing a common online tool is an ideal way to make this possible. An online tool would allow DOE/NNSA sites to share information with other DOE/NNSA sites in two scenarios. The first scenario would involve sharing information about previously approved MedPED exception requests to enable reciprocal access across DOE/NNSA sites. In this scenario, identifiable information regarding an individual's previously approved MedPED exception request at one site would be shared with other DOE/NNSA site(s) in consideration of the individual's MedPED access at the other site(s). The second scenario would involve sharing device information across DOE/NNSA sites, such as device specifications, characteristics, and risk mitigation methods. This would allow the creation of a library of approved PEDs across DOE/NNSA sites, so that known or newly discovered device-specific vulnerabilities could be more readily identified and communicated to security personnel across DOE/NNSA sites, which would enable locating similar devices already adjudicated and/or in use.	

MODULE I – PRIVACY NEEDS ASSESSMENT

	The proposed online tool to facilitate MedPED exception requests across NNSA sites is called MEDSAFe, and it is the subject of this PIA. The MEDSAFe exception request process will begin with the requestor submitting a request to introduce a portable electronic device into a secure area. At a basic level, the request will require information about the requestor (including limited medical information), specifications of the medical device, and a justification. This information will be collected through a secure online form, from which the data will be securely routed for processing. Processing includes review of the exception request by authorized DOE/NNSA technical staff with pertinent knowledge of the security rules for the requested area and review/approval by the authorized approval authorities for the site and field office. The MEDSAFe system will utilize role-based access controls to limit access to data based on need-to-know. For instance, within the same record for a given exception request, some users of MEDSAFe will be able to view specific medical device information and some will only see generic information, like progress of the request. The electronic library of supporting documentation and final determinations will support many-to-many relationships to enable re-using data across DOE/NNSA sites and facilities wherever possible. For example, data may be shared between DOE/NNSA sites to facilitate reciprocated approvals, however, only the minimum PII required will be shared with the additional site (i.e., only sharing that a certain device was approved for a specific person). When data is shared across DOE/NNSA sites, access to PII will be restricted based on need-to-know (e.g., only authorized staff in the approval chain for the additional site will be able to access PII associated with the original MedPED exception request). Additionally, a shared device library will be accessible across DOE/NNSA sites to authorized users, however, the library will not include identifiers or otherwise be uniquely linkable to a specific person. Request routing and electronic approval will be handled online, utilizing strong authentication common across the DOE complex. Having this information in a central database will also support robust reporting, including a reporting dashboard of requests with corresponding status. The collection of this information and associated approvals for MedPEDs is required by: • DOE Order 473.1A - Physical Protection Program • NNSA Policy SD 470.6 - Technical Security Program
Type of Information Collected or Maintained by the System:	☐ SSN ☒ Medical & Health Information ☐ Financial Information ☒ Clearance Information

MODULE I – PRIVACY NEEDS ASSESSMENT

	☐ Biometric Information ☐ Mother's Maiden Name ☐ DoB, Place of Birth ☒ Employment Information (Name of employer only) ☐ Criminal History ☒ Name, Phone, Address (No home address, work address only) ☒ Other – (Employee number)
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?	YES
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?**	• DOE Order 473.1A - Physical Protection Program • NNSA Policy SD 470.6 - Technical Security Program This collection of information is associated with Department of Energy System of Records, DOE-51, "Employee and Visitor Access Control Records." The Department will draft a new Privacy Act System of Record (SOR) in the future that will be directly applicable to this collection of information, and this PIA will be updated at that time.

MODULE II – PII SYSTEMS & PROJECTS

2. CONSENT **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)?**	Prior to providing information, users of MEDSAFe will be informed of the intended uses of the data and will be given the opportunity to accept or decline the terms.
3. CONTRACTS **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?**	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.
4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	MEDSAFe data is not published or otherwise shared with other systems. MEDSAFe will only collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish its authorized purpose. Data will only be maintained for as long as is necessary to accomplish that purpose. At the point of collection, the individual will be advised of the authority for the collection of PII and the intended uses and disclosures of the PII, and the individual will be given the opportunity to accept or decline those terms. Therefore, the potential for impact on the privacy of individuals due to the use of this system is low.
5. SORNs **How will the data be retrieved? Can PII be retrieved by an identifier (e.g. name, unique number or symbol)?** **If yes, explain, and list the identifiers that will be used to retrieve information on the individual.**	Limited roles will be able to retrieve data for the purpose of determining the permissibility of portable medical devices in limited areas. Yes, PII can be retrieved by employee number by those in limited roles.

MODULE II – PII SYSTEMS & PROJECTS	
6. SORNs **Has a Privacy Act System of Records Notice (SORN) been published in the *Federal Register*?** **If "Yes," provide name of SORN and location in the *Federal Register*.**	Yes. Department of Energy Privacy Act of 1974; Publication of Compilation of Privacy Act Systems of Records 74 FR 993, January 9, 2009. DOE-51 Employee and Visitor Access Control Records. Pages 1053-1055
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	N/A.
DATA SOURCES	
8. What are the sources of information about individuals in the information system or project?	All information is entered/provided into MEDSAFe by the individual requesting access to a limited area with a portable electronic device.
9. Will the information system derive new or meta data about an individual from the information collected?	No.
10. Are the data elements described in detail and documented?	Yes, all data elements and their relationships are described in detail in the database schemas and documentation.
DATA USE	
11. How will the PII be used?	PII will be used by authorized DOE/NNSA technical staff with pertinent knowledge of the security rules for the requested area at the site and the associated authorized site and field office approval authorities to make access determinations about whether an individual with the specified personal medical device(s) will be allowed into an access-controlled area/facility.

MODULE II – PII SYSTEMS & PROJECTS

12. If the system derives meta data, how will the new or meta data be used? **Will the new or meta data be part of an individual's record?**	N/A.
13. With what other agencies or entities will an individual's information be shared?	None (DOE/NNSA use only).
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	Reports will provide information about medical devices and associated access decisions. Anticipated reports include: • DOE/NNSA areas an individual has access to; • DOE/NNSA areas in which a device is authorized for certain individuals; • Approved personal medical device list; • Number of personal medical devices approved in a given site/area.
15. What will be the use of these reports?	Technical Surveillance Countermeasures Operations Managers (TSCMOMs) will use these reports to understand and communicate which individuals have medical devices and the DOE/NNSA areas for which these devices are approved.
16. Who will have access to these reports?	Approved TSCMOM users or other designated security personnel only. PII will only be accessible by staff with an official need to know.
Monitoring	
17. Will this information system provide the capability to identify, locate, and monitor individuals?	No.
18. What kinds of information are collected as a function of the monitoring of individuals?	N/A.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	N/A.

MODULE II – PII SYSTEMS & PROJECTS	
DATA MANAGEMENT & MAINTENANCE	
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.	An annual verification process completed by the individual will be used for accuracy, relevancy, and completeness of data.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	MEDSAFe will be hosted by and its data will reside under the purview of ORNL. It will be accessible by authorized users at other DOE/NNSA sites via a secure network, authenticated connection. The access controls established within the MEDSAFe application apply to all users, regardless of a user's site location.
Records Management	
22. Identify the record(s).	**Title**: MEDSAFe **Description**: Records related to medically necessary portable electronic devices (MedPEDs) and their associated requests for allowing such devices into secure/limited areas. Records include but are not limited to device specifications and characteristics, risk mitigation methods, known or newly discovered device-specific vulnerabilities, employment information about the requesting employee, and a justification.
23. Identify the specific disposition authority(ies) that correspond to the record(s) noted in no. 22.	X Unscheduled □ Scheduled (cite NARA authority(ies) below)
24. Records Contact	Mark Ferraiolo, NNSA NA-772, (202) 287-6061
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS

25. What controls are in place to protect the data from unauthorized access, modification or use?	This system will be hosted in the ORNL instance of Azure Government Cloud, FedRamp approved at the Moderate level for confidentiality, integrity and availability. As such, and consistent with NARA Electronic Records Requirements, records are uniquely identified with security controls limiting access to authorized users only. Security Information and Event Management (SIEM) provides logs that can be used to substantiate create, read, update, and archival actions. All records in the system are retrievable and will be usable for as long as needed to conduct agency business and to meet NARA-approved dispositions. Any deviations from the system security plan will be documented according to ORNL Cyber Security policies and procedures.
26. Who will have access to PII data?	Authorized users will have access to PII as it pertains to adjudicating an access request. Individual authorized users will have access to only their own data. User-specific system usage information is only available to authorized MEDSAFe system administrators.
27. How is access to PII data determined?	Designated DOE/NNSA staff approves end-user MEDSAFe system access. The MEDSAFe IT Project Manager approves MEDSAFe system administration access.
28. Do other information systems share data or have access to the data in the system? If yes, explain.	No.
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?	N/A.
30. Who is responsible for ensuring the authorized use of personal information?	Designated DOE/NNSA staff approves end-user MEDSAFe system access. The MEDSAFe IT Project Manager approves MEDSAFe system administration access.

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
System Owner	**Johnny Moore** **(Print Name)** Date: 2024.03.15 13:32:43 -04'00' **(Signature)**	________________
Local Privacy Act Officer	**Linda Chapman** **(Print Name)** LINDA CHAPMAN Digitally signed by LINDA CHAPMAN Date: 2024.03.11 08:40:42 -04'00' **(Signature)**	________________
Ken Hunt **Chief Privacy Officer**	**William K. Hunt** **(Print Name)** William K. Hunt Digitally signed by William K. Hunt Date: 2024.03.08 10:01:02 -05'00' **(Signature)**	________________