Affects Members Of the Public?	X

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: http://www.directives.doe.gov/pdfs/doe/doetext/neword/206/o2061.pdf

Please complete electronically: no hand-written submissions will be accepted.

This template may not be modified.

MODULE I – PRIVACY NEEDS ASSESSMENT

Date	06-16-2009	
Departmental Element & Site	Idaho National Laboratory Building Number: WCB Building Name: WCB	
Name of Information System or IT Project	Occupational Medical Surveillance System (OMSS)	
Exhibit Project UID	72	
New PIA □ **Update** ☒	DOE PIA - OMSS Final lxw.doc	
	Name, Title	Contact Information Phone, Email
System Owner	Paul W Johns	(208)526-0404 Paul.Johns@inl.gov
Local Privacy Act Officer	Dale Claflin, Privacy Act Officer	208-526-6477 Dale.Claflin@inl.gov
Cyber Security Expert reviewing this document (e.g. ISSM,	Daniel Jones, Technical Lead Cyber Security	(208) 526-6477 Daniel.Jones@inl.gov

MODULE I – PRIVACY NEEDS ASSESSMENT

CSSM, ISSO, etc.)		
Person Completing this Document	John Brabec	(208) 526-0024 John.Brabec@inl.gov
Purpose of Information System or IT Project	Captures, maintains and reports employees medical data including: work certifications, health surveillances, work restrictions, physical exam data, x-ray data, and immunization data.	
Type of Information Collected or Maintained by the System:	☒ SSN Social Security number ☒ Medical & Health Information e.g. blood test results ☐ Financial Information e.g. credit card number ☐ Clearance Information e.g. "Q" ☐ Biometric Information e.g. finger print, retinal scan ☐ Mother's Maiden Name ☒ DoB, no Place of Birth ☐ Employment Information ☐ Criminal History ☒ Name, Phone, no Address ☐ Other – Please Specify	
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***		YES

MODULE I – PRIVACY NEEDS ASSESSMENT

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.	
If "Yes," what method was used to verify the system did not contain PII? (e.g. system scan)	Manual validation was provided by the Data Services group. Additionally, when performing the Privacy Impact Assessment information was verified.
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, past employees
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 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.

MODULE I – PRIVACY NEEDS ASSESSMENT

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?**	Contract number DE-AC07-05ID14517 10 CFR 851 Worker Safety and Health Program
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)?**	Individuals provide information through a medical questionnaire and physician and nurse interaction. Any information divulged by the patient is done so at the discretion of the patient. Individuals should provide accurate information to allow proper assessment of individual health to allow for appropriate assessment of employees fitness for duty.
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?**	NO

MODULE II – PII SYSTEMS & PROJECTS

4. IMPACT ANALYSIS: **How does this project or information system impact privacy?**	All data is considered confidential PII. No information, other than that required by law is released without written consent of the client.
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.**	Data can be retrieved by name, SSN, S number
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*.**	DOE-33
7. SORNs **If the information system is being modified, will the SORN(s) require amendment or revision?**	NO

DATA SOURCES

8. What are the sources of information about individuals in the information system or project?	Information comes from the individual, from medical personnel, and from other, secure in–house systems.

MODULE II – PII SYSTEMS & PROJECTS

9. Will the information system derive new or meta data about an individual from the information collected?	Yes, if a person requires treatment, medical personnel will collect new data to ensure that the treatment is as correct as possible. All new information is maintained in the individual's record.
10. Are the data elements described in detail and documented?	Data Dictionary and Data Model are available through Enterprise Architecture.
DATA USE	
11. How will the PII be used?	Only to identify the individual.
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?**	If a person requires treatment, medical personnel will collect new data to ensure that the treatment is as correct as possible. All new information is maintained in the individual's record.
13. With what other agencies or entities will an individual's information be shared?	PII information will not be shared with other agencies. Medical information may be shared with other medical providers on a need-to-know basis for medical reasons, and only with the signed consent of the individual.
Reports	
14. What kinds of reports are produced about individuals or contain an individual's data?	20 to 30 reports are available for use in displaying various portions of the individual's medical record. Such reports are used by medical personnel and are shared with the individual as appropriate.
15. What will be the use of these reports?	To make medical decisions and recommended work accommodations concerning individuals.
16. Who will have access to these reports?	Physicians, nurses and other medical personnel, IT developers, administrative personnel all based on a need to know in the performance of official duties. An individual can request his/her own information at any time.
Monitoring	

MODULE II – PII SYSTEMS & PROJECTS

17. Will this information system provide the capability to identify, locate, and monitor individuals?	The system can be used to monitor aspects of an individual's health.
18. What kinds of information are collected as a function of the monitoring of individuals?	Personal medical information, physical health history, family history, work history, social security number, employee number, employee name.
19. Are controls implemented to prevent unauthorized monitoring of individuals?	System access controls and personal integrity.
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.	Information provided voluntarily by the patient will not be checked for accuracy. Medical data is reviewed during physicals if they are required. Medical health information is updated based on physical exams that are required based on OSHA schedules. Voluntary Wellness Profiles proved another opportunity to update information.
21. If the information system is operated in more than one site, how will consistent use of the information be ensured at all sites?	The application is only operated at the Idaho National Laboratory.
Retention & Disposition	
22. What are the retention periods of data in the information system?	Medical records are retained for 75 years from employee termination.
23. What are the procedures for disposition of the data at the end of the retention period?	The records will be destroyed in compliance with federal and company requirements and procedures.
ACCESS, SAFEGUARDS & SECURITY	

MODULE II – PII SYSTEMS & PROJECTS

24. What controls are in place to protect the data from unauthorized access, modification or use?	The Cyber Security Office implemented and tested all baseline security controls appropriate to its FIPS categorization in accordance with the Senior DOE Management PCSP and DOE Directives. The system included in the Business Enclave and was certified and accredited December 19, 2007 and found to have mitigated risk to an acceptable level.
25. Who will have access to PII data?	Physicians, nurses and other medical personnel, IT developers, administrative personnel all on a need-to-know basis in the performance of official duties. An individual can request his/her own information at any time.
26. How is access to PII data determined?	Need to know controlled access via User ID and password.
27. Do other information systems share data or have access to the data in the system? If yes, explain.	No system connects to OMSS. OMSS provides required information to the TRAIN application and OMP reports. The system now sends radiological information to radiologists electronically using encryption rules specified by FIPS-140-2.
28. 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
29. Who is responsible for ensuring the authorized use of personal information?	System Manger

END OF MODULE II

SIGNATURE PAGE

	Signature	Date
PIA Approval Signatures	**Original Copy Signed and On File with the DOE Privacy Office**	