

PRIVACY IMPACT ASSESSMENT: Pantex – OCCUPATIONAL HEALTH SYSTEM

Template - January 30, 2009, Version 2



Department of Energy
Privacy Impact Assessment (PIA)

Affects Members Of the Public?	X
--------------------------------	----------

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.

Module I – Privacy Needs Assessment

Date	Original November 2008. Redone 3/11/2009.	
Departmental Element & Site	National Nuclear Security Administration Pantex Site Office Amarillo, Texas B & W Pantex, M&O Contractor	
Name of Information System or IT Project	Pantex Occupational Health System (OHS)	
Exhibit Project UID	None	
	Name, Title	Contact Information Phone, Email
System Owner	Jerry G. Simpson, M.D. Site Occupational Medicine Director (SOMD)	806.477.3001 jgsimpson@pantex.com
Privacy Act Officer	Carolyn Becknell NNSA Privacy Officer	505.845.4869 cbecknell@doeal.gov
Cyber Security Expert reviewing this document (e.g. ISSM, CSSM, ISSO, etc.)	Shane Parsley, ISSM John D. Doggett, DAA/ISOM	806.477.6291 sparsely@pantex.com 806.477.3194 jdoggett@pantex.doe.gov

PRIVACY IMPACT ASSESSMENT: Pantex – OCCUPATIONAL HEALTH SYSTEM

Template - January 30, 2009, Version 2

Module I – Privacy Needs Assessment

<p>Person Completing this Document</p>	<p>Nancy Barr, OHM System Administrator</p>	<p>(806) 477-5993 nbarr@pantex.com</p>
<p>Purpose of Information System or IT Project</p>	<p>Electronic medical record system (EMR).</p>	
<p>Type of Information Collected or Maintained by the System:</p>	<p><input checked="" type="checkbox"/> SSN Social Security number</p> <p><input checked="" type="checkbox"/> Medical & Health Information e.g. blood test results</p> <p><input type="checkbox"/> Financial Information e.g. credit card number</p> <p><input checked="" type="checkbox"/> Clearance Information e.g. "Q"</p> <p><input type="checkbox"/> Biometric Information e.g. finger print, retinal scan</p> <p><input type="checkbox"/> Mother's Maiden Name</p> <p><input checked="" type="checkbox"/> DoB, Place of Birth</p> <p><input checked="" type="checkbox"/> Employment Information</p> <p><input type="checkbox"/> Criminal History</p> <p><input checked="" type="checkbox"/> Name, Phone, Address</p> <p><input type="checkbox"/> Other – Please Specify</p>	
<p>Has there been any attempt to verify Information about an Individual in Identifiable Form does not exist on the system?</p> <p><i>OMB 03-22 defines Information in identifiable form as information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).</i></p>	<p>NO—it clearly does contain such information.</p>	
<p>If "Yes," what method was used to verify the system did not contain Information in Identifiable Form? (e.g. system scan)</p>	<p>N/A</p>	

Module I – Privacy Needs Assessment

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

If the answer to the 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.

For information systems that collect, maintain or disseminate information in identifiable form from or about members of the public, please complete Modules II and III. 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. This template may not be modified. 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 (and III if necessary).

Module II – System Information for All Systems

Module II – System Information for All Systems

<p>1. What categories of individuals are collected or maintained by the information system?</p>	<p><input checked="" type="checkbox"/> Federal Employees</p> <p><input checked="" type="checkbox"/> Contractor Employees</p> <p><input checked="" type="checkbox"/> Members of the Public Individuals in non-employee or contractor context. This includes individuals for whom DOE maintains information, as required by law, who were previously employed or contracted by DOE.</p> <p><input checked="" type="checkbox"/> Other, Please Specify Pre-placement candidates; sub-contractors; other entities on site such as Sandia Labs personnel.</p>
<p>2. What is the source(s) of information about individuals in the information system?</p>	<p>Employee information is imported from the Human Resources Employee Database; results from various testing equipment and outside lab test results are downloaded. Other data acquisition is via direct data input by Medical staff.</p>
<p>3. With what other agencies or entities will an individual's information be shared? How will the information be used?</p>	<p>None. Data is used as described in question #4 below.</p>
<p>4. Is the use of the information in identifiable form both relevant and necessary for the mission of the organization and DOE?</p>	<p>Yes, the information is used to determine the individual's health status and suitability for employment, including membership in the Human Reliability Program (HRP).</p>
<p>5. Are the data elements described in detail and documented?</p>	<p>Yes.</p>
<p>REPORTS</p>	
<p>6. What kinds of reports are produced about individuals or that contain an individual's data?</p>	<p>Multiple types of reports can be generated. Reports are used to provide supervisors with personnel job restrictions/clearances or health status; copies of medical records may be provided to personal health care providers. Annual health exam results are provided to employees in the HRP.</p>
<p>7. What will be the use of these reports?</p>	<p>Please see response to #6 above.</p>
<p>8. Who will have access to these reports?</p>	<p>Access is limited to certain Occupational Medicine personnel based on need-to-know; supervisors, and health care providers. Access to specific reports is granted on a need-to-know basis.</p>

Module II – System Information for All Systems

MAINTENANCE

<p>9. If the information system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?</p>	<p>N/A—OHMS is limited to the Pantex site.</p>
<p>10. What are the retention periods of data in the information system?</p>	<p>75 years after employment terminates.</p>
<p>11. What are the procedures for disposition of the data at the end of the retention period?</p>	<p>Printed reports are used for their specific purpose such as restrictions to a supervisor and are destroyed at the end of their retention period. Electronic data will be erased at the end of the retention period.</p>
<p>12. How does the use of this information system affect privacy? Consider also the use of emerging technologies and how those technologies may impact privacy.</p>	<p>OHMS and the Occupational Medicine personnel comply with HIPAA requirements.</p>

ACCESS

<p>13. What controls are in place to protect the data from unauthorized access, modification or use?</p>	<p>The OHM System hardware is housed in a vault type room on the Pantex Plant site. Graded levels of both physical and electronic security are also in effect. Access to system information must be authorized in writing by management, and granted by the Data Owner.</p>
<p>14. If processes are being consolidated, do the proper controls remain in place to protect the data and prevent unauthorized access?</p>	<p>N/A</p>

PRIVACY IMPACT ASSESSMENT: Pantex – OCCUPATIONAL HEALTH SYSTEM

Template - January 30, 2009, Version 2

Module II – System Information for All Systems

<p>15. Who will have access to this information system and its data (all data)? Will other agencies share data or have access to the data in this system? How will the data be used by the other agency?</p>	<p>N/A</p>
<p>16. Who will have access to information in identifiable form or and PII?</p>	<p>Direct access is limited to Occupational Medicine personnel. Access at each level is restricted by need to know and is controlled by system security. Access by personal health care providers, employees and management is in report form only, and is based on need-to-know.</p>
<p>17. How is access to the data determined?</p>	<p>Access to system information must be authorized in writing by management, and granted by the OHMS Administrator. Access is granted only after documented approval is processed for a request.</p>
<p>18. 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>No</p>
<p>19. Do other information systems share data or have access to the data in the system? If yes, explain.</p>	<p>OHMS only imports data. Nothing is exported to another application or system.</p>
<p>20. For connecting information systems, is there an ISA other agreement between System Owners to ensure the privacy of individuals is protected?</p>	<p>OHMS receives updates to personnel data via nightly interface from the Pantex Peoplesoft HR system. Lab data is imported via a one-way modem that is only connected for the period of the download. There is a signed contract with Lab Corps that includes HIPAA protection.</p>
<p>21. Who is responsible for assuring proper use of the information system's information in identifiable form?</p>	<p>Jerry G. Simpson, MD, Occupational Medicine Director</p>

Module III – Systems with Information About Members of the Public

<p>1. What legal authority authorizes the purchase, development or maintenance of this information system?</p>	<p>Atomic Energy Act of 1954, (42 U.S.C. 2051a), section 31a Economy Act of 1932, as amended, (31 U.S.C. section 1535) 42 U.S.C. 7101 <i>et seq.</i>; 50 U.S.C. 2401 <i>et seq.</i> Implementation Guide for DOE Order 440.1 10 CFR 851 (Replaced DOE O 440.1)</p>
<p>2. Has a Privacy Act System of Records Notice been published in the Federal Register? If "Yes," provide name of SORN and location in the Federal Register.</p>	<p>No, as no determination has been made yet that the Occupational Health Management System is a "System of Records".</p>
<p>3. If the information system is being modified, will the SORN require amendment or revision?</p>	<p>Unknown at this time.</p>
<p>4. How will data collected from sources other than DOE records be verified for accuracy, relevance and completeness?</p>	<p>Individuals personally submit medical information/records from their health care provider. Information is reviewed with the individual for accuracy and completeness.</p>
<p>5. Are records in the system about individuals current? What steps or procedures are taken to ensure the data is current?</p>	<p>Medical data is current. Personal data kept in the Peoplesoft HR system is updated nightly; SSN doesn't change. Data input by medical staff is reviewed with the individual involved. It is reviewed by an OMD staff member for completeness.</p>
<p>6. Will the information system derive new or meta data about an individual through aggregation from the information collected? How will this be maintained, including verified for relevance completeness, and accuracy?</p>	<p>Medical information is aggregated throughout an individual's employment. As stated in #5 above, the information is reviewed by both OMD staff and the individual involved for accuracy.</p>
<p>7. Will the new or meta data be part of an individual's record?</p>	<p>Yes, Medical records are retained in the individual's medical file.</p>

Module III – Systems with Information About Members of the Public

<p>8. How will the new or meta data be used? Will it be used to make determinations about members of the public?</p>	<p>See #2, Module II.</p>
<p>9. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.</p>	<p>Data on the individual is normally accessed using Pantex badge number as an input parameter, but can also be searched for using Name or SSN if provided by the employee. SSN is not printed on any public reports. Access to see SSN is granted by the OHMS Administrator based on job duties.</p>
<p>10. 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>Providing the information is a condition of employment. In the case of visitors/contractors, providing the information is a condition of access to the plant.</p> <p>Personnel must sign a Release of Information for data to be released to other than required agencies.</p>
<p>11. Will this information system provide the capability to identify, locate, and monitor individuals?</p>	<p>Yes.</p>
<p>12. What kinds of information are collected as a function of the monitoring of individuals?</p>	<p>Medical histories including medications taken; physical restrictions; suitability for employment; suitability for inclusion in the Human Reliability Program; suitability for certain types of work.</p>
<p>13. What controls will be used to prevent unauthorized monitoring?</p>	<p>Users must be authorized in writing by management, and based on need-to-know. Access is granted only by the Data Owner. Access is limited to specific parts of the program based on job duties.</p>

SIGNATURE PAGE

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