



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Occupational and Environmental Health Readiness System - Industrial Hygiene (DOEHRS-IH)

TRICARE Management Activity (TMA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR** Enter DITPR System Identification Number
- Yes, SIPRNET** Enter SIPRNET Identification Number
- No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes**
- No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes**
- No**

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

DoD Clearance and OMB Licensing requirements are currently being reviewed by the TMA Information Collection Management Officer. The PIA will be updated accordingly with their decision.

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority (“internal housekeeping”) as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C §552a, Privacy Act of 1974; 10 U.S.C. §§1071-1085, 1086, 1097(a) – (b), Processes for Patient Safety in Military and Veterans Health Care Systems (§1071 Note), Medical and Dental Care, Civilian Health and Medical Program of the Uniformed Services, Contracts for Health Benefits for Certain Members, Former Members, and their Dependents, TRICARE Prime and TRICARE Standard/Extra Program; 10 U.S.C. §1120, Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants; DoD 6025.18-R, DoD Health Information Privacy Regulation; 42 U.S.C. §201, Patient Safety and Quality Improvement Act of 2005; 42 U.S.C. §§11131-11152, Reporting of Information; 29 C.F.R. §1910.1020, Access to Employee Exposure and Medical Records; 32 C.F.R. Part 199.17 (TRICARE Program); 45 C.F.R. Parts 160, 162, and Subparts A and E of 164, Health Insurance Portability and Accountability Act Privacy and Security Rules; DoDI 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoDI 6055.1, Sec. 4.1, DoD Safety and Occupational Health Program; DoDI 6055.5, Industrial Hygiene and Occupational Health, reissued May 6, 1996; and E.O. 9397 (as amended for SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Defense Occupational and Environmental Health Readiness System – Industrial Hygiene (DOEHRS-IH) is a comprehensive, automated information system (AIS) for assembling, comparing, using, evaluating, and storing personnel exposure information. In its current state of development, DOEHRS-IH supports collecting data on potential personnel exposures to occupational hazards and environmental hazards, workplace environmental monitoring data, personal protective equipment usage data, observation of work practices data, and employee health hazard educational data. DOEHRS-IH promotes reduction in redundant data entry through timely and efficient sharing of data among Occupational and Environmental (OEH) personnel. DOEHRS-IH is a key enabling technology within the mandated Presidential Force Health Protection (FHP). In addition, DOEHRS-IH interfaces with clinical, safety, environmental and personnel AISs within DoD as well as interfacing with systems external to DoD that provide Federal standards and compliance information.

DOEHRS-IH has been fully deployed to the Army at 96 sites. Deployment to the Army National Guard, the Navy and the Air Force is underway and is expected to be fully deployed by the end of the second quarter of FY10.

The system collects an individual's name, Social Security Number, and date of birth. All categories of individuals about whom DOEHRS-IH collects environmental and workplace exposure data have the potential to have personal information collected (military, civilian, foreign national, contractor or other categories).

System point of contact:
Defense Health Services Systems (DHSS)
5111 Leesburg Pike, Suite 810
Falls Church, VA 22041-3206

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risk posed by the collection, use, and sharing of information is that a user may inadvertently disclose personally identifiable information (PII) to an unauthorized user. This risk has been minimized through system design and implementation of various administrative, technical, and physical security controls.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify.

Ultimately, DOEHRS-IH will be interfaced with AHLTA and will provide exposure data for the Clinical Data Repository (CDR). As requirements are incorporated into the system, DOEHRS-IH will include corporate reporting, which will provide even more timely and efficient worldwide access of data and information to users throughout the Department of Defense (DoD), including Military Treatment Facility (MTF) Commanders, Industrial Site Commanders, Deployed Site and MTF Commanders, Lead Agents, and

Installation Agencies. However, only personnel with the appropriate level of access will be able to see PII, and they will only have access to data specific to their area of responsibility.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Other (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

Yes **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

In the case of military personnel, the requested information is required due to the need to document all active duty medical incidents for the proper administration of care and benefits. In the case of all other personnel, the requested information is voluntary. However, the collection of PII is required to identify potential exposures and mitigate hazards in the workplace.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

Yes **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The collection of personally identifiable information from individuals is required, and not optional, objections to the contrary will prevent the provision of comprehensive care. Additionally, personally identifiable information is required to identify potential exposures and mitigate noise hazards in the workplace.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input checked="" type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

The DOEHRS Project Management Office (PMO) is currently working with the TMA Privacy Office to draft a PAS for DOEHRS-IH.