



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Armed Forces Health Surveillance Center (AFHSC)
Electronic Surveillance System for the Early Notification of Community-based
Epidemics (ESSENCE)

US Army Medical Command - Defense Health Program Funded System

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

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

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.

Authorities to collect PII are as follows:

- 5 U.S.C. 301, Departmental Regulations.
- 10 U.S.C. Chapter 55, Medical and Dental Care.
- 32 CFR 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
- E.O. 9397 (SSN), as amended.
- National Strategy for BioSurveillance, The White House, July 2012.
- National Strategy for the Pandemic Influenza, Implementation Plan, Homeland Security Council, The White House, May 2006.
- DoD Directive 6490.02E, Comprehensive Healthcare Surveillance, February 8, 2012; Incorporating Change 1, Effective October 3, 2013.
- DoD Instruction 6200.03, Public Health Emergency Management within the Department of Defense, Incorporating Change 2, Effective October 2, 2013

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 AFHSC ESSENCE is a commercial web-based syndromic surveillance application. It is an enhanced electronic disease surveillance application developed by the Johns Hopkins Applied Physics Laboratory (APL) for use by public health organizations. The AFHSC ESSENCE provides timely accessible information for the detection and analysis of disease outbreak, chemical, biological, terrorist threat and/or emergency to the authorized end users located at the AFHSC via an intranet website. This application screens the Military Health System (MHS) enterprise for rapid or unusual increases in the occurrence of certain syndromes. Central to this strategy is the emphasis on the consolidation of data and resources and the alignment of medical surveillance processes across the entire population at risk. In the event of a potential outbreak, military officials are alerted immediately via e-mail or text-enabled device.

The AFHSC ESSENCE is also known as the Civilian ESSENCE because it only collects data on the military family member healthcare beneficiaries. It is different from the DoD ESSENCE system that is currently used to collect information on Federal employees and their family members and is managed by the Defense Health Agency (DHA) Program Executive Office. While the DoD ESSENCE system has experienced performance problems and lacks many of the functionality improvements of the AFHSC ESSENCE, it will continue to be used. The AFHSC ESSENCE will serve as another tool to fulfill this public health mission.

The PII in the application is only available to the system administrators. Most of the PII elements collected by this application are processed to create anonymity. For example, the date of birth is processed to age. Only the processed (de-identified) data is available to the application users and communicated when an alert is published. The following describes the PII collected and its disposition:

- PII processed and discarded: name, social security number, and date of birth.
- PII retained in the system: Electronic Data Interchange Person Numbers (EDIPN), race/ethnicity, gender, zip code, and medical information.

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

The privacy risks associated with PII include unauthorized access and unauthorized disclosure. The privacy risks are mitigated through the implementation of various administrative, technical and physical security controls. These security controls are listed in Section 3 below.

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.

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.

System Administrator contractor staff at AFHSC with the appropriate level of certification will be granted access as a result of a National Agency Check with Law and Credit (NACLC) or DoD-determined equivalent investigation. All access is on a need to know basis.

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.

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

AFHSC ESSENCE is not the initial point of collection of PII from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII. The PII is collected from existing systems, records, and reports.

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.

AFHSC ESSENCE is not the initial point of collection of PII from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII. The PII is collected from existing systems, records, and reports.

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 type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

AFHSC ESSENCE is not the initial point of collection of PII from individuals; therefore, no Privacy Act Statement can be provided. The PII is collected from existing systems, records, and reports. A Privacy Act Statement is provided only at the initial point of collection of the PII.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.