PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE)
Defense Health Agency (DHA)

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: 140 (EI/DS)
- ☐ **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 UII: 007-000000510 (EI/DS)

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.

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); DoDD 6490.02E, Comprehensive Health Surveillance; DoDI 6055.05, Occupational and Environmental Health (OEH); DoDI 6200.03, Public Health Emergency Management within the Department of Defense; and E.O. 9397 (SSN), as amended.

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 Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE) is a web-based syndromic surveillance application that screens the Military Health System (MHS) enterprise for rapid or unusual increases in the occurrence of certain syndromes.

ESSENCE provides timely accessible information for the detection and analysis of disease outbreak, chemical, biological, terrorist threat and/or emergency to authorized end users consisting of users at the medical treatment facility level, intermediate headquarters level Major Commands (MAJCOM), Major Army Commands (MACOM)s, Healthcare Support Office (HSO)s, Military Health Care System Regions, and corporate level Service Surgeons General (SG)s, DHA and Health Affairs (HA) via the ESSENCE website. 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.

ESSENCE collects the following types of personal information about information about individuals: personal descriptors, identification numbers, health information and medical information.

System Contact information: Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE), ESSENCE Project Manager.

A PIA has been previously submitted for this system with a final signature date of November 30, 2011.

(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/PHI being collected stems from internal or external exploitation. The internal risk of disclosure is when employees or business associates gain access to PHI/PII with malicious intentions to misuse the PHI/PII. The external risk of disclosure is when users fail to lock their workstations when not in use or a hacker breaking into the system and exploiting the PII/PHI. System risks are mitigated through the implementation of various administrative, technical and physical security controls, such as the Common Access Card (CAC), use of Secure Sockets Layer (SSL) to access ESSENCE environment, implementation of role-based access control application and mandatory security awareness training. Also, system users are required to submit an Account Authorization Request Form (AARF) and have the need for access validated.

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. ESSENCE users are authorized epidemiologists and preventive medicine specialists. They are primarily located at the military treatment facility (MTF) level, but may also be located at the intermediate headquarters level Major Commands (MAJCOM), Major Army Commands (MACOM), Healthcare Support Office (HSO)s, Military Health System (MHS) Regions, corporate level Service Surgeon Generals (SG)s - Army, Air Force, and Navy, Defense Health Agency (DHA) and Health Affairs levels. System users do not disclose or share PII/PHI with any other Federal agencies or private organizations.

☐ **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. MTF personnel with the appropriate level of certification will be granted access as a result of a National Agency Check with Written Inquires (NACI) or DoD-determined equivalent investigation and personnel on a need to know basis. ESSENCE users include all contractor personnel with access to PII/PHI that must maintain an Automated Data Processing/Information Technology (ADP/IT) Level II or higher security clearance.

While end users are primarily located at the military treatment facility (MTF) level, they may also be located at the intermediate headquarters level Major Commands (MAJCOM), Major Army Commands (MACOM), Healthcare Support Office (HSO)s, Military Health System (MHS) Regions, corporate level Service Surgeon Generals (SG)s - Army, Air Force, and Navy, Defense Health Agency (DHA) and Health Affairs levels.

☐ **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.

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.

PII/PHI are periodically transmitted from various sources within MHS to DHSS ESSENCE. These data include: Comprehensive Ambulatory/Professional Encounter Record (CAPER) and pharmacy records from the Pharmacy Data Transaction Service (PDTS) Comprehensive Ancillary Data Record Extract(Laboratory

and Radiology orders), via the Composite Health Care System (CHCS) and demographic (VM6) data from the Defense Enrollment Eligibility Reporting System (DEERS).

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.

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.

PII/PHI are collected (system to system) from multiple MTFs and DEERS. Individuals are given the opportunity to consent to the use of their PII/PHI when they initially provide consent to provide personal information to MTFs and DEERS/DMDC.

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

☐ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

ESSENCE is not the initial point of collection of PII/PHI from individuals; therefore, no Privacy Act Statement is required. This statement is given only at the initial point of collection.

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.