PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Force Corporate Health Information Processing Service (AFCHIPS)
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
- ☐ **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 EDHA 07

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.

10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); 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.

AFCHIPS is a subset of servers and databases within the SPAWAR enclave at Charleston Naval Shipyard, South Carolina. It serves as a centralized repository of military medical data for use in data analysis and patient care. It provides a platform to deliver metrics, supporting data, and informational input utilized to aid decision makers both at the military treatment facility level and at the enterprise management level. This capability subsequently provides an enhanced level of care for the Department of Defense; as well as other authorized individuals seeking medical treatment and interaction within the Military Health System.

The types of personal information about individuals collected in the system include personal descriptors, ID numbers, ethnicity, health, and life information.

The category of individuals includes anyone seen for treatment in a military treatment facility such as all Department of Defense active duty military, dependents, retirees, and retirees dependents. There may also be rare instances of others included if, for example if they were treated for emergent care in a military treatment facility.

This system is managed by the Defense Health Agency, Health Information Technology Directorate, Information Delivery Division, Enterprise Intelligence Branch.

(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 the personally identifiable information/protected health information (PII/PHI) collected are due to sharing, using, and viewing PII/PHI. In response to the risk of unauthorized access to AFCHIPS, the system will contain warning banners in accordance with DoD regulations and implement physical, technical, and administrative safeguards to ensure only authorized personnel that demonstrate "need to know" can access information contained within AFCHIPS. All applicable security and privacy processes and regulations have been defined and implemented, reducing risks and safeguarding privacy.

All systems are vulnerable to "insider threats." System managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to AFCHIPS. These individuals have gone through background and employment investigations. Safeguards include techniques deployed on the system itself, including Common Access Card (CAC) access, password protection, and where applicable, encryption techniques. Software installation includes security patch installation current at the time of that software release.

There are only three groups of individuals who have logical access to the servers where data are collected, stored, processed, and analyzed: military personnel, medical personnel, and database administrators. System administrators have physical access to the servers in order to maintain the security and operational posture of the system but do not have access to the data the system processes, stores, or collects regarding health records. System administrators cannot modify, access, or otherwise view the medical information stored on the system.

To mitigate the potential risks associated with the collection and storage of PII/PHI, AFCHIPS manages all requests for access by Government representation. This "request and approval" process is well documented using DD FORM 2875, AUG 2009, SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR) form for those internal members who have a need to access PHI in the course of product development within the context of the "covered entity" and external members needing access to PII/PHI (i.e., Researcher with approved IRB). External users who do not require access to PII/PHI are managed by the individual application for access to "summary-level" information for reporting and analysis.

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. Defense Health Agency, Military Health System (MHS)

☒ **Other DoD Components.**

Specify. Departments of the United States Air Force, Army, and Navy

☒ **Other Federal Agencies.**

Specify. U.S. Department of Veterans Affairs

☐ **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.

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

AFCHIPS is not the initial point of collection for PII. The individual will not have the opportunity to object to their collection for this system. The opportunity to object is only available at the initial point of data collection. This system is downstream from the initial point of data collection. The responsibility for this belongs with the source system.

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.

AFCHIPS is not the initial point of collection for PII. The individual will not have the opportunity to object to their collection for this system. The opportunity to object is only available at the initial point of data collection. This system is downstream from the initial point of data collection. The responsibility for this belongs with the source system.

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.

AFCHIPS collects PII/PHI into a system of records and is therefore subject to the Privacy Act of 1974. However, because AFCHIPS does not collect information directly from individuals, no Privacy Act Statement is required.

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.