PRIVACY IMPACT ASSESSMENT (PIA)

For the

Career History Archival Medical and Personnel System (CHAMPS)
Department of the Navy - TMA DHP Funded System - BUMED

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 N06150-2, NM06150-3 and NM06150-7

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.

SORN Authorities:

1) N06150-2 - Health Care Record System

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 1095, Collection from Third Party Payers Act
10 U.S.C. 5131, as amended, Bureaus: names; location
10 U.S.C. 5132, Bureaus: distribution of business; orders; records; expenses
44 U.S.C. 3101, Records management by agency heads; general duties
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN), as amended

2) NM06150-3 - Health/Dental Research Center Data File

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 3013, Secretary of the Army
10 U.S.C. 8013, Secretary of the Air Force
10 U.S.C. 5041, Headquarters, Marine Corps
14 U.S.C. 93, Commandant, U.S. Coast Guard General Powers
E.O. 9397 (SSN), as amended

3) NM06150-7 - Combat Trauma Registry Expeditionary Medical Encounter Database

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OASD/HA Policy 04-031, Coordination of Policy to Establish a Joint Theater Trauma Registry
DoD 6025.18-R, DoD Health Information Privacy Regulation
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 Career History Archival Medical and Personnel System (CHAMPS) is a comprehensive database that provides an individually based longitudinal record of career events and hospitalizations from the date that an individual's military service began until the date of separation or retirement. Most routinely collected administrative or medical data are a collection of discrete events that are compiled and updated in monthly files. CHAMPS organizes these routinely collected cross-sectional files into an individually based history that is organized by the event date and type of event. CHAMPS chronologically tracks career events that include deployments, duty station or ship assignments, job designations, changes in the number of dependents and many other types of personnel and military career events. Outcomes include medical events such as hospitalization discharge diagnoses, coded using an International Classification of Diseases Code (ICD), HIV testing results, service separation (including type of discharge), or death with ICD or external cause code. CHAMPS provides a rapid, cost-effective method for defining cohorts of military personnel and following them longitudinally for subsequent medical or personnel events. CHAMPS enhances the DoD's ability to conduct epidemiologic research and provide force health protection for active duty forces and has been used to study a wide variety of potential exposures and health outcomes of military importance.

Personally Identifiable Information (PII) collected about individuals includes: Name, Social Security Number (SSN), gender, race/ethnicity, birth date, place of birth, religious preference, marital status, medical information (includes: discharge reason, International Classification of Diseases (ICD) 9 codes, procedure Codes, pharmaceutical data, prescription information, hospitalization discharge diagnoses, HIV testing results, death with ICD or external cause code), disability information (includes: discharge reason, discharge date, deployment information, injury type or diagnostic code), military records, education information (includes: education degree, education years).

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

All systems are vulnerable to "insider threats". The manager is 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 the system. These individuals have gone through extensive background, security clearances and employment investigations.

The CHAMPS system and its data files are maintained on an IBM Z o/s mainframe at the Naval Postgraduate School (NPS) in Monterey CA. Data on the mainframe disks at NPS Monterey is encrypted. This is the same computer system used by Defense Manpower Data Center (DMDC). Data mined or extracted from CHAMPS is transferred to Naval Health Research Center (NHRC) servers in San Diego, CA for analysis by investigators and researchers.

Even though contract staff will be working on the project, all data will be housed on-site at NHRC and DMDC's mainframes maintained at NPS. All data will be kept on encrypted computers requiring Common Access Card (CAC) card access, and will be restricted to investigators on this project who have signed the Investigator Compliance Attestation for this protocol. This project operates under a Bureau of Medicine and

Surgery (BUMED)-approved Institutional Review Board (IRB) protocol that is reviewed annually. The reports prepared from the data will rely entirely on aggregate data and will not report data on any one individual. The data will be retained until all research issues have been addressed.

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. Within Naval Health Research Center (NHRC) only

☐ **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. Eagle Applied Sciences, Inc. with Standard Business Associate Agreement ("BAA")

☐ **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.

CHAMPS does not collect PII directly from individuals.

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.

CHAMPS does not collect PII directly from individuals.

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.

CHAMPS does not collect PII directly from individuals.

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.