PRIVACY IMPACT ASSESSMENT (PIA)

For the

Clinical Business Intelligence Suite (CBIS)
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

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:

5 U.S.C. 301, Departmental Regulations;
10 U.S.C. 1095, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act;
10 U.S.C. 5131 (as amended), Bureau: Name, Location;
10 U.S.C. 5132, Bureau: Distribution of Business, orders, records, expense;
44 U.S.C. 3101, Record Management by Agency Head;
10 CFR part 20, Standards for Protection Against Radiation;
5 CFR 293.502, Subpart E, Employee Medical File System Records;
5 CFR 339.106-306, Coverage;
10 CFR part 20, Standard for Protection against Radiation;
29 CFR Part 5, Labor Standards;
DoD 6025.18R, DoD Health Information Privacy Regulation
E.O. 9397 (SSN), as amended

Other authorities:

Title 10, Chapter 55, U.S.C., Section 1071 through Section 1106
5 USC, 552a, The Privacy Act of 1974

Office of Management and Budget (OMB) M-06-16, Protection of Sensitive Agency Information, June 23, 2006
OMB Circular Number A-130, Management of Federal Info Resources Appendix III, Nov 28, 2002
Military Health Systems Information Assurance Implementation Plan
Health Affairs Policy 06-010
Health Affairs HIPPA (Health Insurance Portability and Accountability Act)
Security Compliance Policy, June 27, 2006
DoD Instruction 8910.1-M, DoD Procedures for Management of Info Requirements, June 30, 1998

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 CBIS system is a centrally managed Navy Medicine enterprise-wide architecture comprised of a suite of applications that provides Bureau of Medicine and Surgery (BUMED), Navy Medicine Regional Headquarters, and Military Treatment Facilities (MTFs) with tools for reporting, monitoring, and improving health-care data quality. CBIS receives data on a daily and monthly basis from over 24 Composite Health Care System (CHCS) host sites, the Navy and Marine Corps Public Health Center (NMCPHC), the Clinical Coding community, Defense Medical Human Resources System Internet (DMHRSi) and the general public that gathers, stores, and transmits computerized information about patient satisfaction, performance levels, resources, type of care and severity of illness of patients at Navy MTFs and/or within the TRICARE Network.

Data is transmitted to Navy Medicine Information Systems Support Activity (NAVMISSA) from each host CHCS site, via the Navy Customer Survey (NAVCUS) file in CBIS. NAVCUS files contain PII and non-PII and are used to provide a means to associate patient information with corresponding customer survey inputs; this information allows BUMED to measure resource intensity for delivering care, and a means to resource MTFs based on the quality of care being provided. For the Navy Population Health Navigator program and the Clinical Coding applications, non-PII data is retrieved from from NMCPHC and DMHRSi for processing; information is reported to appropriate BUMED decision makers and staff members.

In all cases, after data files have been received and processed they are then moved to a repository where they are maintained for historical purposes if needed.

PII included in the NAVCUS files contain the patient (sponsor, spouse and/or child), sponsor's name, Spouse & Child Information: name, reversed and scrambled SSN, mailing/home address, birth date, gender, medical information (healthcare delivery plan), and other non-PII demographic information such as appointment date, name of clinic, provider ID, PCM team, family member prefix, and alternate care value. Provider information included in the NAVCUS file contains name, rank, class, reversed and scrambled SSN, provider ID and specialty number.

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

All CBIS systems are vulnerable to "insider threats." CBIS managers are vigilant to this threat by limiting system access to those individuals who have a defined need, and meet the criteria to access the information. These individuals have gone through DoD background and employment investigations.

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. Only SPAWAR New Orleans and CBIS system administrators and Program Management authorized personnel have access to this data.

☐ **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. NAVMISSA and designated contractor (Five Stones Research Group and SPAWAR New Orleans) support personnel have access to CBIS data files and databases.

Contract Verbiage: the contractor may require access to information which may be sensitive and is to be handled as "For Official Use Only", and which may be covered by the privacy act and the Health Insurance Portability and Accountability Act (HIPAA). The contractor shall ensure that staff assigned to this task understands the meaning of these categories of data, have the appropriate HIPAA training and handle them accordingly.

☐ **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.

Patient surveys are generated by numerous methods to include mail, web, email, direct dial, social media and Interactive Voice Response (IVR) survey instruments. Surveys only include providers name, location and date of appointment; it does not include patient's name or any other PII. All surveys are created/ submitted by the patient (customer) on a voluntary basis.

(CBIS) 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.

CBIS 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.

CBIS 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.