PRIVACY IMPACT ASSESSMENT (PIA)

For the

Weekly Obstetrics Forecasting Tool (WOFT)
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, 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.

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 Weekly Obstetrics Forecasting Tool (WOFT) is a tool that is used operationally by hospital staff and leaders to make decisions about the patients receiving obstetric care. Personally identifiable information (PII) contained in the tool is used to collate and assist the obstetrics leadership team in strategic decision making.

PII collected about individuals includes: Name, Social Security Number (SSN), other identification number (DoD ID), gender, birth date, marital status, home telephone number, mailing/home address, spouse information (Family Member Prefix (FMP)/SSN if they are the insurance sponsor for the patient), marital information, child information (estimated delivery date and actual delivery date if one occurred), financial information (a patient's beneficiary category is captured as part of the WOFT. This may seem to be financial information given that it describes how they relate to their TRICARE insurance), medical information (last menstrual period, Para (number of offspring produced), Gravida (number of pregnancies), Delivery date, Estimated Date of Delivery, Scheduled C-section date, Scheduled Induction Date, Assigned Provider, Complicated Obstetric Patient classification (COB) Reason, Deliver Method, Gestational Age, Previous C-Section), military records and other (information on the status of the parking pass, date added to the WOFT, and Military Treatment Facility (MTF) staff member).

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

The privacy issues associated would be the potential release of the PII data contained in the WOFT, however these concerns are addressed by the intranet security protocols and the user group and individual access controls that are administered as part of the MTF Share Point environment.

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. Military Treatment Facility, Bureau of Medicine and Surgery (BUMED), Perinatal Advisory Board

☐ **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. Contractor/Developer-Johns Hopkins University Applied Physics Lab. The contract contains business associate agreement language. Additionally, PII is safeguarded per the Data Sharing Agreement for Task Order Nr 1429, JHU06.

☐ **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.

If a nurse or provider is asking a patient for specific PII during an encounter, the patient has every right to decline providing this information.

Additionally, when a non-active duty beneficiary begins their care in the Obstetrics (OB) clinic they are offered the choice to decline having their information used for analysis. This is done through a Privacy Act Statement.

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

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.

If a nurse or provider is asking a patient specific PII during an encounter, the patient has every right to decline providing this information.

Additionally, when a non-active duty beneficiary begins their care in the OB clinic they are given the choice to consent to having their information used for analysis. This is done through a Privacy Act Statement.

The information is used for medical treatment purposes.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

When patients arrive at the MTF to begin their obstetric care, they are presented with a Privacy Act Statement. (DD Form 2005 Privacy Act Statement - Health Care Records)

Active duty beneficiaries are required to consent to having their information used for analysis, but non-active duty beneficiaries are not. This form is given to every patient who begin their care in the OB clinic.

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.