PRIVACY IMPACT ASSESSMENT (PIA)

For the

Integrated Clinical Management and Risk Mitigation System (ICM-RMS) (revised 5-25-2016 to update SORN information)
Department of Navy - United States Marine Corps (USMC)

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 DITPR ID: 17137 DITPR DON ID: 22935

☐ **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: 007-000009990

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 M01040-3; N06150-2; EDHA 20 DoD

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.

Marine Corps Order (MCO) 1500.60 establishes Force Preservation Councils within each command that oversee the preservation of the organization by evaluating several human risk factors that under the Order's Task section are to provide commanders with a holistic view of their Marines. This holistic view alongside the additional task to identify unit trends before they become endemic necessitates the collection of personally identifiable information to include medical information that resolves the lack of insight into a commands force preservation status.

SORN M01040-3 authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; 10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas; 32 CFR 64.4, Management and Mobilization; DoD Dir 1215.13, Reserve Component Member Participation Policy; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural and Manmade Disasters; CJCSM 3150.13B, Joint Reporting Structure Personnel Manual; DoD Instruction 6490.03, Deployment Health; MCMEDS: SECNAVINST 1770.3D, Management and Disposition of Incapacitation Benefits for Members of the Navy and Marine Corps Reserve Components (Renamed Line of Duty(LOD)); and MCO 7220.50, Marine Corps Policy for paying Reserve Marines; and E.O. 9397 (SSN), as amended.

N06150-2 SORN authorities:
55 U.S.C. 301, Departmental Regulations; 10 U.S.C. 1095, Collection from Third Party Payers Act; 10 U.

S.C. 5131 (as amended); 10 U.S.C. 5132; 44 U.S.C. 3101; 10 CFR part 20, Standards for Protection Against Radiation; and, E.O. 9397 (SSN), as amended.

EDHA 20 DoD SORN authorities:

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 10 U.S.C. Chapter 55, Medical and Dental Care; DoD Directive (DoDD) 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)); DoDD 5136.01, Assistant Secretary of Defense for Health Affairs (ASD(HA)); DoDD 6490.02E, Comprehensive Health Surveillance; DoDD 6490.14, Defense Suicide Prevention Program; Army Regulation 600-63, Army Health Promotion; OPNAV Instruction 1720.4A, Suicide Prevention Program; Air Force Instruction 90-505, Suicide Prevention Program; 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 purpose of this DoD information system is to comply with MCO 1500.60 and mitigate specific command and medical vulnerabilities, which can result in service members falling through the cracks. The system captures risk-related information for individuals assigned to a unit's force preservation program by enabling key players in force preservation to independently input risk-related information into a single repository, which automatically generates an empirical risk score, and allows sustained coordination and communication between "need to know" entities (Medical, Command, and Mental Health) while also providing medical and mental health capabilities such as automated alerts and controlled medication tracking. These capabilities allow for better informed decision support for commanders in developing risk mitigation plans, and will promote the transition from reactive to proactive mental health treatment. This tool is vital for Force Preservation Councils to consolidate data, review cases, add command concerns, and build full-resource action plans as required by MCO 1500.60.

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

Risks associated with this collection of already routinely collected Marine Corps personnel information consist of hackers, foreign espionage, internal threat, etc. This initiative to comply with MCO 1500.60 refocuses the collection of Marine Corps personnel information to include the analysis of this information in order to spot trends among a select group of Marines and advise commanders about appropriate risk mitigation plans based on that trend analysis. Access to the system and all its associated components or web-based dashboards are CAC-enabled and only provisioned to privileged individuals of trust with need-to-know access requirements.

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. USMC Commanders, Health Professionals and USN Health Professionals.

☐ **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.

☐ **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.

PII is not collected directly from the individual.

The system is used to manage medical clinics where the individuals are patients who are required to fill out certain information on paper forms, which this system will draw data from. Therefore, individuals do not have the ability to object to this collection since, as a matter of requirement, they are incoming patients.

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.

PII is not collected directly from the individual.

The system is used to manage medical clinics where the individuals are patients who are required to fill out certain information on paper forms, which this system will draw data from. Therefore, individuals do not have the ability to object to this collection since, as a matter of requirement, they are incoming patients.

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.

PII is not collected directly from the individual.

The system is used to manage medical clinics where the individuals are patients who are required to fill out certain information on paper forms, which this system will draw data from. Therefore, individuals do not have the ability to object to this collection since, as a matter of requirement, they are incoming patients.

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.