PRIVACY IMPACT ASSESSMENT (PIA)

For the

FASOR - FAMILY ADVOCACY SYSTEM OF RECORDS
US Army Medical Command

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**
- [x] **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?

- [x] **Yes, DITPR** Enter DITPR System Identification Number: 13777 DA 201263
- [ ] **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?

- [x] **Yes**
- [ ] **No**

If "Yes," enter UPI UII: 000009991

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.

- [x] **Yes**
- [ ] **No**

If "Yes," enter Privacy Act SORN Identifier A0608-18 DASG

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.

Altered SORN request submitted to Army Priv

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 Request for OMB Control Number submitted to Army Privacy Office on 17 August 2015.

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. 3013, Secretary of the Army; 42 U.S.C. 10606 et seq., Victims' Rights, as implemented by Department of Defense Instruction 1030.2, Victim and Witness Assistance Program; Army Regulation 608-18, The Family Advocacy Program (FAP); and E.O. 9397 (SSN).

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 U.S. Army Medical Command (MEDCOM) has functional proponency for the treatment and case management of the Army Family Advocacy Program (FAP). Installation Management Command - Family Programs has primary proponency over Army FAP. The US Army Family Advocacy System Of Records (Army FASOR) web-based, information system was procured by the MEDCOM to be used by the Army's FAP to collect and manage data regarding incidents of domestic violence and child abuse. The system stores FAP data for statistical analysis required for program management and reporting to Congress and the Department of Defense. The Army FASOR provides an electronic environment to facilitate incident management, including: (1) Case Review Committee meetings; (2) the decision process of domestic violence and child abuse incident determinations; (3) communications with the command; and (4) a treatment approach for the alleged offender and victim.

The types of PII collected include demographics, financial, medical, employment, and educational information.

This PIA updates the previously approved PIA.

(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 PII collected are (1) unauthorized access; (2) inaccurate information entered into the application; and (3) unauthorized disclosure of PII. Administrative, physical, and technical security safeguards are in place to mitigate these risks as described in Section 3d below.

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.

US Army Public Health Command
G-1, Army Center for Substance Abuse Programs
US Army Medical Command
US Army Installation Management Command
Army Criminal Investigation Command
Army Deputy Chief of Staff for Personnel
Army Intelligence and Security Command
Army Recruiting Command
Department of the Army Inspectors General
Provost Marshal General
Army Human Resources Command

☒ **Other DoD Components.**

Specify. Defense Manpower Data Center

☒ **Other Federal Agencies.**

Specify.

US Coast Guard
Federal child protection services and family support agencies
Federal law enforcement and confinement/correctional agencies

☒ **State and Local Agencies.**

Specify.

Law enforcement, child and protective service agencies, and courts of law for each state as ordered.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

FAP employees contracted by the federal government use FASOR to conduct FAP duties and have access to this information based on privileging by the Army Central Registry System Administrators. There are provisions in the contract requiring compliance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA). The contractors also receive training in these areas.

☒ **Other** (e.g., commercial providers, colleges).

Specify.

Researchers with an approved Institutional Review Board application and MEDCOM Data Sharing Agreement.

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.

Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records, is provided to the patient for review. This all inclusive Privacy Act Statement applies to all requests for personal information made by care treatment personnel for medical/dental treatment purposes and will become a permanent part of the health care record. If the individual objects to the collection of their PII, comprehensive health care may not be possible, but care is not denied.

(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.

After reviewing the DD Form 2005, Privacy Act Statement – Health Care Records, regarding privacy if patients have concerns about consent and/or withholding PII, patients are referred to the Patient Administration Division at each military treatment facility for further information and guidance. If individuals object to the specific uses of their PII, comprehensive health care may not be possible, but care is not denied.

(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.

A. DD FORM 2005, June 2016, PRIVACY ACT STATEMENT - HEALTH CARE RECORDS

1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN):
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6055.05, Occupational and Environmental Health (OEH); and E.O. 9397 (SSN), as amended.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED:
Information may be collected from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Military Health System (MHS) provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

3. ROUTINE USES:
Information in your records may be disclosed to:
• Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care;
• Government agencies to determine your eligibility for benefits and entitlements;
• Government and nongovernment third parties to recover the cost of MHS provided care;
• Public health authorities to document and review occupational and environmental exposure data; and
• Government and nongovernment organizations to perform DoD-approved research.

Information in your records may be used for other lawful reasons which may include teaching,