PRIVACY IMPACT ASSESSMENT (PIA)

For the

Army Behavioral Health Integrated Data Environment (ABHIDE)
Department of the Army - 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:

- [x] 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?

- [x] Yes, DITPR — Enter DITPR System Identification Number: 12097 (DA193961)
- [ ] 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
- [x] 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.

- [x] Yes
- [ ] No

If "Yes," enter Privacy Act SORN Identifier: A00405b 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.

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.

10 U.S.C. 3013, Secretary of the Army; DoD Instruction 6490.2E, Comprehensive Health Surveillance; DoD Instruction 6015.23, Delivery of Health Care at Military Treatment Facilities (MTFs); DoD Instruction 1300.18, Personnel Casualty Matters, Policies, and Procedures; Army Regulation 40-66, Medical Record Administration and Health Care Documentation; Army Regulation 195-2, Criminal Investigation Activities; Army Regulation 600-85, Army Substance Abuse Program; Army Regulation 600-8-104, Military Personnel Information Management/Records; Army Regulation 608-18, The Family Advocacy Program; 42 U.S.C. 290dd-2, Substance Abuse and Mental Health Services; 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 information collection is to provide the US Army Public Health Command (Provisional) [USAPHC(Prov)] [formerly US Army Center for Health Promotion and Preventive Medicine (USACHPPM)] a standardized, enterprise-wide, information management and technology capability, known as the Army Behavioral Health Integrated Data Environment (ABHIDE). The ABHIDE will integrate information from non-related/dispersed databases into a comprehensive health surveillance database to support mental, behavioral, social health and public health activities. Surveillance refers to the systematic collection, analysis, and interpretation of health data that has a significant impact on Army public health, which is then used to drive decisions about health policy and prevention strategies. Objectives include establishing event-specific registries, such as a suicide registry, identifying risk factors, developing mitigation strategies, evaluating intervention and prevention programs, and prospectively monitoring Army communities with respect to their mental, behavioral, and social health. Categories of information maintained in the database include personnel, medical and legal data. Examples of the type of data are: amount of education completed, deployment history, drug and alcohol screenings, medical diagnoses and criminal investigations.

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

Risks include unauthorized access to PII, inaccurate information in the system, and unauthorized disclosure of PII. These risks are addressed by the following:

1) The system will have role-based access.

2) ABHIDE is receiving data exports from other systems. Information is matched via SSN, first name, last name, middle initial and date of birth. If there is not a match, data is not used.

3) ABHIDE data is maintained in a controlled government facility. Physical entry is restricted by the use of key cards, guards, and is accessible only to authorized personnel with a need-to-know. Access to personal data is limited to person(s) responsible for maintaining and servicing the ABHIDE data in performance of their official duties and who are properly trained, screened and cleared for a need-to-know. Access to personal data is further restricted by the use of Common Access Card (CAC) and/or strong password, which are changed periodically according to DoD security policy.

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. Vice Chief of Staff of Army - Suicide Prevention Task Force and Suicide Prevention Program

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Data will be shared with National Institute of Mental Health (NIMH)

☐ **State and Local Agencies.**

Specify.

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

Specify. NMR Consulting and Computer Sciences Corporation (CSC) provide information technology (IT) staff (Database administrators, data analysts) to support USAPHC (Prov) under contract W91ZLK-08-P-1423. These contract employees are required to comply with DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation, January 2003 and complete the following annual mandatory training:

1. Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Training
2. Information Assurance User Awareness Training
3. Network Security Focus Training: Includes Removable Media Handling, Anti-Phishing, Safe Home Computing and Personally Identifiable Information.

Contract IT support staff are also required to adhere to: AR 25-2, Information Systems Security; AR 380-5, Information Security Program; AR 380-40, Security Policy for Safeguarding and Controlling Communications; and DoD Information Assurance Certification and Accreditation Process (DIACAP).

☐ **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.

The individual soldier does not participate in the data collection process. The ABHIDE is using data that is already collected and maintained in other Army and DoD data sources (personnel, medical and legal data).

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.

The individual soldier does not participate in the data collection process. The ABHIDE is using data that is already collected and maintained in other Army and DoD data sources (personnel, medical and legal data).

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.

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.