PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Electronic Data for Care History And Readiness Tracking (MED-CHART)
Army National Guard

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: 13515/DA201609
- ☐ **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 A0040-66 ARNG (September 17, 2014, 79 FR 55762)

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 0704-0413

Enter Expiration Date DoD resubmitted for continuation.

☐ **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.

Statutory Authority: 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN), as amended; DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation; Army Regulation 40-501, Standards of Medical Fitness section 7-11 item 16, 10-11 2b; USAREC 601-56 section 2-4, Waiver, Future Soldier Program Separation, and Void Enlistment Processing Procedures.

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.

Medical Electronic Data for Care History and Readiness Tracking (MEDCHART) is an automated information system essential for the day-to-day management of the recruiting, retention and tracking of the medical readiness programs for the Army National Guard (ARNG) and U.S. Army Reserves (USAR) service members. The system is a joint effort among the ARNG and USAR Surgeons, and their respective G-1s. MEDCHART encompasses essential functional areas necessary for the processing and tracking of ARNG medical waivers used for recruiting and retention of the ARNG. The system also supports the ARNG and USAR Medical Readiness processing and tracking which encompasses the following: Case Management and Medical Referrals Management, Immunization and Medical Services tracking, Occupational Health Exams tracking, Dental Classification, Line of Duty processing, Incapacitation Pay claims processing, and Health Record Image Management. MEDCHART supports the ARNG and USAR by providing biostatical data that can be analyzed to enable informed decision making by the ARNG and USAR Surgeons. The MEDCHART Unclassified Network supports the MEDCHART application modules which include the Health Readiness Record (HRR) module, Dental Classification (DenClass) module, Automated Voucher System (AVS) module, Occupational Health (OccHealth) module, Reserve Component Computer Based Training (RCCBT) module, Electronic Medical Management Processing System (eMMPS) module, Electronic Case Management (eCase) module, Medical Readiness Reporting (MRR) module and the Medical Action Tracking System (MATS) module.

The PII collected includes: Demographic data; personal, medical, security clearance; employment information; military records, and education information. This extensive list has been derived mostly because of the multiple Department of Defense (DD) and Department of the Army (DA) standard forms that are collected and stored within the MEDCHART system. These forms are the main source of PII collected by this system.

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

The Army National Guard considered five discreet potential privacy risks in designing and developing MEDCHART:

- Unauthorized access
- Inaccurate information
- Privacy and due process right protection
- Unauthorized disclosure
- Data exchange with external interfaces

In response to the risk of unauthorized access to the sensitive information that records within MEDCHART will contain, the Army National Guard is taking a "defense in depth" approach to protecting this information. Administrative safeguards (e.g., establishing a DIACAP that parallels the MEDCHART system life cycle) are employed in series to ensure security measures are in place to protect the MEDCHART Information Systems. Physical safeguards (e.g., data stored on accredited servers) are employed to ensure the physical protection of MEDCHART. Technical safeguards (e.g., encryption; common access card, DISA Security Technical Implementation Guides implementation) are employed to ensure the information is protected and access to its information is controlled.

In response to the risk presented by including inaccurate information in the system, MEDCHART correlates information from authoritative sources only and all information entered into the system is review and approved by an approving authority.

In response to the risk of violating the rights of the individuals involved in the collection process, the Army National Guard is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. Data is only viewed by approved registered MEDCHART users and

personnel that require access to the information in the performance of their duties.

In response to the risk presented by unauthorized disclosure of information contained, MEDCHART requires that users of MEDCHART receive information assurance awareness, system training, and complete Privacy Act / HIPAA Certification training in order to mitigate risks involved. This multi-faceted approach to safeguarding information provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

In response to the risk of data exchanges with external interfaces, connections between MEDCHART and external systems, whether public or DoD, provide a means of entry and access to system data that must be protected as per DoDI 8500.2 and AR 25-2. Data exchanges are performed using the secure file transfer protocol (SFTP) and/or the SSL/TLS protocol (Web Services). Discretionary access controls are used to secure communications for each external connection. All external data exchanges are formalized with Data Usage and/or Interface Agreements between the ARNG - Office of the Chief Surgeon and the identified external DoD Component and/or Federal Agency. Each individual Interface Agreement specifies the data elements involved in the exchange.

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.

Army National Guard (ARNG) - Human Resources Personnel Division (HRP)
Reserve Health Readiness Program (RHRP)
U.S. Army Dental Command (DENCOM)
U.S. Army Financial Management Command (USAFMCOM) - Defense Finance and Accounting Service (DFAS)
U.S. Army Medical Command (MEDCOM)
U.S. Army Physical Disability Agency (USAPDA)
U.S. Army Reserve (USAR)
U.S. Army Military Entrance Processing Command (MEPCOM)
Office of the Surgeon General (OTSG) - Decision Support Center (DSC)

☐ **Other DoD Components.**

Specify. Defense Manpower Data Center (DMDC)

☐ **Other Federal Agencies.**

Specify. Department of Health and Human Services (HHS) - Federal Occupational Health (FOH)

☐ **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.

The MEDCHART applications are military recruiting, retention, and readiness applications. Providing PII is required for recruitment into the military and maintaining military readiness is a "condition of employment". As such, the requested information is mandatory. Users can object to the entry of PII by not entering the data into MEDCHART.

Applicants entered into MEDCHART are required to complete a Standard Form 86-1, Questionnaire for National Security Positions Authorization Release of Information, a Standard Form 86-2, Authorization for Release of Medical Information Pursuant to the Health Insurance Portability and Accountability Act (HIPAA), and a Credit Check Authorization form.

The MEDCHART Acceptable Use Policy displays the system Privacy Act Statement and Privacy and Security notices in accordance with the law and DoD policy.

(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.

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

Providing PII is required for recruitment into the military and maintaining military readiness is a "condition of employment". As such, the requested information is mandatory.

All data captured by the MEDCHART application modules, including PII, becomes part of the applicant's record and/or the soldier's readiness history. That data is utilized by the MEDCHART system as part of the applicant's record and/or soldier's readiness history and qualification.