DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

KELETA.RAHWA.AMDEMARIAM.1298456431 Digitally signed by KELETA.RAHWA.AMDEMARIAM.1298456431 Date: 2018.11.15 10:30:14 -05'00'

DHA Privacy
Office Review

MEMORANDUM FOR DEFENSE PRIVACY, CIVIL LIBERTIES AND TRANSPARENCY DIVISION

SUBJECT: Justification for the Use of the Social Security Number (SSN) in the Assistance Reporting Tool, DoD Information Technology Portfolio Repository (DITPR) #13918

This memorandum is to satisfy the requirements of the *Department of Defense Instruction (DoDI) 1000.30, Reduction of Social Security Number (SSN) Use Within DoD*, dated August 1, 2012, that requires justification of the collection and use of SSNs in DoD systems. This memo explains the necessity for SSNs to be collected by the Assistance Reporting Tool (ART). The system of records notice (SORN) applicable to ART is EDTMA 04, Medical/Dental Claim History Files (October 27, 2015, 80 FR 65720) (Attachment 1). The Privacy Impact Assessment (PIA) for ART is currently in currently in development.

ART is a secure web-based system that captures feedback on and authorizations related to TRICARE benefits. ART received an Authority to Operate in compliance with the Department of Defense Information Assurance Certification and Accreditation Process on 03 October 2016. The system undergoes an annual risk assessment to ensure protective controls are maintained during the lifecycle of the system. Users are comprised of customer service personnel, to include Beneficiary Counseling and Assistance Coordinators, Debt Collection Assistance Officers, personnel, family support, recruiting command, case managers, and others who serve in a customer-service support role. The ART is also the primary means by which Military Medical Support Office (MMSO) staff capture medical authorization determinations and claims assistance information for remotely located service members, line of duty care, and care under the Transitional Care for Service-related Conditions benefit. ART allows users to track workload and resolution of TRICARE-related issues.

ART is subject to the Paperwork Reduction Act (PRA) and is currently in the process of completing the required documentation for Office of Management and Budget approval (Attachment 3).

In accordance with DoDI 1000.30, continued use of SSNs within ART must be justified by one or more of the Acceptable Use Cases set forth in DoDI 1000.30, Enclosure 2. The Acceptable Use Cases applicable to ART are Acceptable Use Case 2.c.(8) Computer Matching, and 2.c.(11) Legacy System Interface:

> (8) Computer Matching. Systems, processes, or forms that interact with other Government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to

some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions.

(11) Legacy System Interface. Many systems, processes, or forms that do not meet the criteria in subparagraphs 2.c.(1) through 2.c.(10) of this enclosure for the continued use of the SSN may not be able to transition to another identifier in a timely manner due to an interface with a legacy system still using the SSN, or due to the excessive cost associated with the change. In these cases, the continued use of the SSN may be acceptable for a specified period of time, provided that formalized, written plans are in place for the migration away from the SSN in the future. Plans to alter these use cases must take into account interactions with other applications as well as all methods for entry, processing, or transfer of information from said application. It is critical that transfer away from the SSN does not cause unacceptably long interruptions to continued operations.

ART users rely on other government systems and forms that continue to require the use of SSN as a primary identifier. These systems and forms include:

- Defense Enrollment Eligibility Reporting System (DEERS)
- General Inquiry of DEERS (GIQD)
- Marine Corps Medical Entitlements Data System (MCMEDS)
- Army Line of Duty (LOD) Module
- Managed Care Support Contractors' Claims Systems
- Air Force AF348
- Army DA2173

The following provides a list of the physical, technical, and administrative controls currently in place in ART to reduce exposure of the SSN:

a. Physical Controls: ART data is stored on a single server in a designated room at a single location. Access to the room is limited to government and government-contracted personnel at the facility with both proper keycard to access the building and the appropriate passcode to unlock the cypher lock to the room. ART back-up data is secured in a fire-rated safe on zip drives at a third-party location. Access to the room is limited to government and government-contracted personnel at the facility with the proper cypher code to get into the room and the correct combination to the safe. End-user access to ART is limited to personnel granted an ART account by the Customer Service Support Division of MHS. Users access ART via computers at their duty location or on government-issued laptops. To access the system, users first authenticate to the DHA network through the use of a valid Common Access Card (CAC) ID. Non Associated CAC users, must first authenticate by logging in to the DHA Extranet with user name and password credentials to associate their CAC. Once logged in to the DHA Extranet, users may access ART with their ART username and password.

b. Technical Controls: Access to ART is restricted to authorized users. Users must use their CAC to access the system. ART requires all users to have a CAC. A user name and password is only issued to new users when the account is created, solely for the purpose of associating the CAC. Users who make three failed attempts to access ART are locked out. Accounts may only be unlocked by ART administrative staff. The Intrusion Detection System assures access to only authorized users. ART data exists behind a firewall; assuring communicating networks are secure and trusted. ART data is provided a high level of security and data integrity through encryption via the Oracle 11g Triple Data Encryption Standard (3DES) when data is transmitted to and from the Web server. Backup tapes are 3DES encrypted (for fields containing Personal Identifiable Information) as well as Advanced Encrypted Standard-256 bit (AES-256) encrypted.

c. Administrative Controls: Only authorized users are permitted to access ART. Requests for access are made in writing to MHS Customer Service Support Division. Verification is made that the individual assists beneficiaries with aspects of the TRICARE benefit. Any ART account not accessed in a 25-day period will default to an "Inactive" status. ART administrative staff closes these accounts on a quarterly basis. Users are granted access based on their level of responsibility. The criteria used to determine who has access to different parts of the system are based on position. ART technical staff performs daily audits on the security methods protecting ART. The daily auditing report includes number of logins or failed attempts and identifies any threats to data.

The point of contact for this program is Mr. Richard Masannat, Web and Mobile Technologies (WMT) Program Management Office (PMO), Solution Delivery Division, Information Operations Directorate (J-6), 703-681-7189, richard.g.masannat.civ@mail.

MASANNAT.RICHARD.GEORGE.1103073444
Digitally signed by MASANNAT.RICHARD.GEORGE.1103073444
Date: 2018.11.08 09:32:27 -05'00'

R. G. MASANNAT
Chief, Program Support, WMT PMO

Attachments:
As Stated