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

NOBLE.MARILYNN.J.1108148930
Digitally signed by NOBLE.MARILYNN.J.1108148930
Date: 2018.08.24 16:40:49 -04'00'

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 Defense Medical Human Resources System – Internet (DMHRSi); Department of Defense Information Technology Portfolio Repository (DITPR) ID #130

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, requiring justification to collect and use the SSN within DoD systems, with respect to DMHRSi. The applicable DHA system of records notice (SORN) is EDHA 11, Defense Medical Human Resources System – Internet (DMHRSi), March 15, 2016, 81 FR 13779) (Attachment A). The draft Privacy Impact Assessment for DMHRSi is currently being updated. The 30-day Notice regarding DMHRSi's information collection (Attachment C) was published in the Federal Register on September 29, 2015, and the OMB Control Number for DMHRSi referenced therein is 0720-0041, expiration date of December 31, 2018.

DMHRSi is an established web-based system that provides enhanced management and oversight of medical personnel from the Services' entire military and civilian workforce in the Military Health System (MHS). DMHRSi consolidates human resource functions across the MHS, providing a single database source of instant query/access for all MHS personnel types and the readiness posture of all Armed Services and MHS medical personnel. DMHRSi permits ready access to essential manpower, personnel, and labor cost assignment, education and training, and personnel readiness information across the DoD medical enterprise.

DMHRSi collects information on Active Duty Military, Reserve, and National Guard personnel, as well as DoD civilian employees (including foreign nationals, DoD contractors, and volunteers). Information about individuals collected within DMHRSi is obtained primarily from DoD pay and personnel systems, the Defense Enrollment and Eligibility Reporting System, and from personnel working at DoD medical facilities. Additional information may be obtained from supervisory personnel or DoD operational records.

In accordance with DoDI 1000.30, continued use of SSNs within DMHRSi 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 DMHRSi are 2.c.(8), Computer Matching, Section; 2.c.(11), Legacy System Interface.

Use Case 2.c. (11), Legacy System Interface:

DMHRSi has several interfaces with DoD-level and Service-level (Army, Navy and Air Force) applications for data ranging from personnel to financial. A number of these systems are currently dependent upon the SSN as the primary identifier. The following list shows inbound or outbound interfaces where SSN is a dependent key identifier for record transfers between the Service source/target system and DMHRSi. For each interface, there is an interface agreement/memorandum of understanding (ICD/MOU)

Inbound Interfaces:

- Defense Civilian Personnel Data System (DCPDS)
- Defense Civilian Pay System (DCPS)
- Military Personnel Data System (MILPDS)
- Medical Operational Data System – Enlisted (MODSE)
- Medical Operational Data System – Guard (MODSG)
- Medical Operational Data System – Officer (MODSO)
- Medical Operational Data System – Reserve (MODSR)
- Medical Readiness Decision Support System – Unit Level Training and Reporting Application (MRDSS-ULTRA)
- Navy Enlisted System (NES)
- Navy Standard Integrated Personnel System (NSIPS) Reserve – Enlisted
- Navy Standard Integrated Personnel System (NSIPS) Reserve – Officer
- Officer Personnel Information System (OPINS)

Outbound Interfaces:

- Enterprise-Wide Provider Data (EWPD)
- Military Health System (MHS) Data Repository (MDR)
- Pacific Joint Information Technology Center (JITC) Integrated Test and Evaluation Center (ITEC)

Bi-Directional Interfaces:

- Center for Medicaid and Medicare Services (CMS)
- Digital Training Management System (DTMS)
- Navy Training Management and Planning System (NTMPS)

Use Cases 2.c (8), Computer Matching:

In order for DMHRSi to continue updating records within DMHRSi with data in these external systems, an individual's SSN must be maintained within DMHRSi. Until DoD systems, from which DMHRSi obtains and/or shares data, have been modified/upgraded to replace SSNs with DoD Electronic Data Interchange Personal Identifiers (EDIPIs), DMHRSi will need to continue using SSNs to assure that an individual's DMHRSi records are accurately updated and exchanged within DoD and Service-level systems.

DMHRSi data is, from time to time, requested by and transferred to other government agencies, such as the Veterans Administration (for the purpose of managing and documenting

provider demographics). The SSN is required when DMHRSi provides data to these other government agencies as the related external, non-DoD systems, are dependent on the SSN as the primary identifier for an individual. Because these other agencies do not recognize the EDIPI, an individual whose data is requested are typically identified by the individual's SSN. These interactions with other government agencies fall within Acceptable Use Case 2.c.(8) Computer Matching.

DMHRSi has taken steps to reduce the vulnerability of the SSN. Specifically:

- DMHRSi, as a relational database, has an internally generated employee identifier that is used as a unique key between tables. The employee number has been used to mask/replace SSN in cases where applicable in order to identify employees within DMHRSi

- DMHRSi does capture and maintain EDIPIs and is migrating towards using this code when sharing data from DMHRSi to other DoD systems. As other dependent systems migrate to the EDIPI as the universal identifier, DMHRSi will be able to adjust the interface and not use the SSN.

- DMHRSi uses role-based access to control visibility to human resource information; thus, visibility of the SSN is limited to a smaller subset of "trusted users".

- DMHRSi has reduced the vulnerability of the SSN by masking the SSN within the application and removing the SSN from reports where possible.

- DMHRSi requires users to take annual training for Health Insurance Portability and Accountability Act (HIPAA), Privacy Act, and Annual Cyber Awareness Training to retain access to the system.

- DMHRSi is CAC enforced – All users must have a CAC in order to access the system.

- For accounts that become inactive, access is removed after 90 days of inactivity.

- DMHRSi maintains its system accreditation, security profile and ensures Information Assurance Vulnerability Alerts are applied in a timely manner.

- DMHRSi is centrally hosted at Defense Information Systems Agency facilities to ensure physical system access is limited.

If you have any questions, my point of contact is Mr. Ernest "Terry" Hogan, telephone 571-777-6909; email ernest.t.hogan.ctr@mail.mil.

JOHNSON.JANET.MARY.1287755763

Digitally signed by JOHNSON.JANET.MARY.1287755763
Date: 2018.07.12 16:51:32 -04'00'

Janet Johnson, CIV
Portfolio Manager, DMHRSi
Solutions Delivery Division, CSPMO
703-882-3951

Attachments: As Stated