OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

DEFENSE
HEALTH AGENCY

Chief, DHA
Privacy & Civil
Liberties

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 Privacy Impact Assessment (PIA) for DMHRSi, March 28, 2019 (Attachment B). The 30-day Notice regarding DMHRSi's information collection (Attachment C) was published in the Federal Register on March 27, 2019, and the OMB Control Number for DMHRSi referenced therein is 0720-004, expiration date of March 31, 2022.

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 Section 2.c (8), Computer Matching, and Section 2.c (11), Legacy System Interface.

Use Case 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 when requested is transferred to the Department of Veterans Administration and the Centers for Medicare and Medicaid Services for the purpose of managing and documenting provider demographics. The SSN is required when DMHRSi provides data to the aforementioned government agencies that 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.

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)
- Digital Training Management System (DTMS)
- 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)
- Navy Standard Integrated Personnel System (NSIPS) Active – Enlisted
- Navy Standard Integrated Personnel System (NSIPS) Active – Officer
- Navy Standard Integrated Personnel System (NSIPS) Reserve – Enlisted
- Navy Standard Integrated Personnel System (NSIPS) Reserve – Officer

Outbound Interfaces:

- Department of Defense Healthcare Management System Modernization (DHMSM) Program – CLARIVA
- Joint Centralized Credentials Quality Assurance System (JCCQAS)
- Military Health System (MHS) Data Repository (MDR)

Bi-Directional Interfaces:

- Center for Medicaid and Medicare Services (CMS)
- Defense Manpower Data Center (DMDC) EBLLS
- Joint Knowledge Online (JKO)
- Medical Readiness Decision Support System – Unit Level Training and Reporting Application (MRDSS-ULTRA)
- Navy Training Management and Planning System (NTMPS)

The DMHRSi program office has taken the following steps to reduce the vulnerability of the SSN.

- Masks the SSN within the application and removing the SSN from reports where possible.
- Defense Health Services System Policy DHSS-PM-POL-0003-1.0 System Environment Definitions Policy calls for the masking of PII and PHI data in all environments. DMHRSi contains PII data and has implemented encryption of PII data to meet policy DHSS-PM-POL-003-1.0
- Requires users to take Annual Cyber Awareness Training to retain access to the system.
- Employs role-based access to control visibility to human resource information; thus, visibility of the SSN is limited to a smaller subset of "trusted users."
- Maintains the system accreditation, security profile and ensures Information Assurance Vulnerability Alerts are applied in a timely manner.

Additionally, DMHRSi is Common Access Card (CAC) enforced, requiring all users to have a CAC in order to access the system, and for accounts that become inactive, access is removed after 90 days of inactivity. DMHRSi is centrally hosted at Defense Information Systems Agency (DISA) facilities to ensure physical system access is limited.

As a relational database, DMHRSi has an internal generated employee identifier that is used as a unique key between tables. The employee number has been used to mask/replace the SSN in cases where applicable in order to identify employees within DMHRSi. DMHRSi does capture and maintain EDIPIs and is migrating towards using this number 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.

If you have any questions, my point of contact is Mr. Ernest "Terry" Hogan, telephone 703-678-1334; email ernest't'hogan.ctr@mail.mil.

Janet Johnson, CIV
Portfolio Manager, DMHRSi
SDD/Clinical Support Program
Management Office
Defense Health Agency (DHA)

Attachments: As Stated