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

Administration & Management (J1)

4 October 2024

MEMORANDUM FOR Defense Privacy, Civil Liberties and Transparency Division

THROUGH: Defense Health Agency (DHA), Privacy and Civil Liberties Office

SUBJECT: Justification for the Use of Social Security Numbers (SSNs) in DHMSM Electronic Health Record (DHMSM EHR) MHS GENESIS Electronic Health Record CORE (EHR CORE) system, Department of Defense Information Technology Portfolio Repository (DITPR) # 16913.

This memorandum is written to satisfy the requirement established under Department of Defense Instruction (DoDI) 1000.30, Reduction of Social Security Number (SSN) Use Within DoD, dated August 1, 2012, requiring justification of the collection and use of the SSN in DoD Systems, with respect to MHS GENESIS Electronic Health Record CORE (EHR CORE), eMASS 3202 and the interconnected sub-components; MHS-GENESIS - Infrastructure (Infrastructure), eMASS 3166, MHS-GENESIS - High Assurance/Clinical Application Services (HA-CAS), eMASS 3203, MHS-GENESIS - Test (Test), eMASS 3206, MHS-GENESIS - Train (Train), eMASS 3207, MHS-GENESIS - Build (Build), eMASS 3205.

The MHS GENESIS Electronic Health Record CORE (EHR CORE) provides access to authoritative clinical data sources and is the authoritative source of clinical data to support improved population health, patient safety, and quality of care to maximize medical readiness for the DoD. As the modernization effort continues, the DHMSM EHR system will replace the legacy Electronic Health Record (EHR) systems and become MHS GENESIS. Hereinafter, DHMSM EHR is referred as MHS GENESIS.

MHS GENESIS is an EHR information system that collects, processes, and distributes EHR longitudinally across the Military Health System (MHS), Department of Veterans Affairs (VA), United States Coast Guard (Coast Guard), TRICARE network of service providers, and Federal and State agencies for approximately 9.6 million DoD beneficiaries worldwide.

MHS GENESIS collects, processes, and distributes the following categories of PII, which includes Protected Health Information (PHI) and SSNs. This information is needed for the timely and high-quality delivery of health care services to and the determination and processing of patient benefit information for DoD, VA, Coast Guard, and other beneficiaries, as well as for Defense Health Agency (DHA) authorized clinical trials, medical research, and disease registries.

MHS GENESIS is intended for use by clinicians for the purpose of providing

access to healthcare for the patient populations of DoD, VA, Coast Guard, and their beneficiaries. The application of standardized workflows, integrated healthcare delivery, and data standards enables improved electronic exchange of medical and patient data between the DoD and its external partners, including the VA and private sector healthcare providers. Applicable system of record notice (SORN) is EDHA 07, Military Health Information System. Per DHA Information Management Control Officer (IMCO), MHS GENESIS is not subject to the Paperwork Reduction Act (PRA). Office of Management and Budget (OMB) Control Number is 007-000100033.

The external systems, processes, and DOD forms that rely on MHS GENESIS data utilize SSN as the primary identifier requiring the continued use of the SSN. Mitigation efforts and safeguards are in place to reduce the use, visibility, and printing. SSNs contained within MHS GENESIS are masked from view and removed from reports whenever possible. Continued use of SSNs meets the Acceptable Use Cases set forth in DoDI 1000.30, Enclosure 2.c.(11) Legacy System Interface and 2.c.(13) Other Cases.

(11) Legacy System Interface. DoD ID Number does not transfer or serve as a unique identifier within legacy systems and collections deployed across the Services. Additionally, the excessive cost associated with modifying the millions of historical records and documents utilized by and maintained within MHS GENESIS prohibits transition from SSN to an alternative unique identifier.

(8), Computer Matching. SSNs are used when MHS GENESIS interfaces with legacy EHR systems and Health Information Exchange (HIE) information systems that do not support the Electronic Data Interchange Personal Identifier (EDIPI), i.e., the DoD ID, for matching a patient's identity and medical records. MHS GENESIS does not use SSN as the primary identifier. However, if the system eliminates the use of SSN, it may not be able to properly locate a patient's medical records from legacy EHR systems and mission partners information systems in HIE, which will negatively impact the timing and quality of delivering patient care, as well as patient safety. MHS GENESIS requires SSNs for at as long as it interfaces with legacy DoD, VA and Coast Guard systems relying on the SSN as the primary identifier. The system also requires ongoing use of SSNs as a secondary identifier to ensure patients are properly identified and receive appropriate medical care.

(13) Other Cases. The continued use of the SSN as the unique identifier is required to maintain the integrity and continuity of data for longitudinal analysis and studies linking historical data to new data for the same individual. SSN is the sole identifying characteristic for individuals who left the military, foreign nationals, and/or for historical data entered prior to issuance of DoD ID numbers.

In limited instances where a beneficiary requests the provision of medical services at a Military Treatment Facility (MTF) but cannot adequately prove his or her identity or eligibility, timely provision of the medical services requested by a beneficiary at that MTF requires the beneficiary's SSN to prove identity or eligibility. Were the MTF and/or its personnel to deny a beneficiary services because of an inability or refusal to use the patient's SSN to verify identity or eligibility, the MTF and/or the personnel could be exposed to liability.

MHS GENESIS is hosted in government-authorized commercial data centers using a centralized data and services architecture. The primary data center is in Kansas City, MO, and backup data center in Lee's Summit, MO. The primary data center provides production operations, with clinical data mirrored over to the COOP/DR

environment at Lee's Summit providing an ability to fail-over in the case of a system outage. Each data center implements the 800-53 RMF PE controls documented in eMass. Network connectivity, transport, and boundary defense are outside the security assessment/authorization boundary and are provided by the enterprise wide MedCOI network leveraging DODIN transport and conforms to DoD Joint Information Environment (JIE) objectives. CSSP services for the MedCOI network and connected MHS GENESIS systems are provided by Naval Information Warfare Center (NIWC).

The primary Oracle database for MHS GENESIS is journaled and transactions are replicated in the backup database. The transmission of transactional journals and the backup database are encrypted. Audit logs are maintained for all assets in the enclave, per Security Technical Implementation Guide (STIG) and SRG requirements. Regular external audits are conducted on MHS GENESIS, per ATO requirements.

Encryption of Data at Rest uses approved DoD encryption methods (i.e., NIST FIPS 140-2 validated cryptographic modules) and by the hardware platform hosting the client or server application. In MHSG2, data center storage is encrypted by the Storage Area Network (SAN) or the server (for locally hosted storage). MHSG2 end-user devices encrypt local storage. MHS GENESIS-Theater (MHSG-T) hardware encrypts local disk. Data exchanges between MHS GENESIS and end-user devices is encrypted using Hypertext Transfer Protocol (HTTP) Transport Layer Security (TLS) HTTPS. Data exchanged between MHS GENESIS, and external systems is encrypted using TLS. For data exchanges between MHS GENESIS and trusted external systems is encrypted using TLS using X.509 certificates issued by DoD Certificate Authorities (CAs). MHS GENESIS and its clinical applications provide users data access rights based upon job functionality, authority, and responsibility within the enterprise.

Access to the system requires use of a CAC or RSA SecurID, and a valid account that is vetted prior to access being granted. Regular external audits are conducted on MHS GENESIS, per requirements in the ATO memo for the system. No user has direct access to an MHS GENESIS data store; role-based access control (RBAC) is enforced through end-user applications. The applications access a local Lightweight Directory Access Protocol (LDAP) with the user's credentials to pull the list of associated attributes which extends the DoD schema with MHS GENESIS-specific least-privilege attributes to identify the system capabilities and data access available to that user. Some access control attributes are maintained internally to the clinical applications within MHS GENESIS.

For questions related to this memorandum contact please contact Mr. Gurpreet Brar, the DHMSM Information Systems Security Manager (ISSM), at 571-314-3191 or gurpreet.brar.civ@health.mil.

Recommend Approval

SHEDRICK.CHARLES.JOSE.1125538459 Digitally signed by SHEDRICK.CHARLES.JOSE.1125538459 Date: 2024.10.08 13:56:21 -05'00'

Charles J. Shedrick, GS14, DHA
Supervisor, Privacy Compliance
J-1 Administration and Management Directorate

BRAR.GURPREET.1300416469 Digitally signed by BRAR.GURPREET.1300416469 Date: 2024.10.07 10:22:36 -04'00'

Gurpreet Brar
Information Systems Security Manager
Defense Healthcare Management Systems Modernization