PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Defense Healthcare Management System Modernization Electronic Health Record (DHMSM EHR)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

Defense Healthcare Management System Modernization (DHMSM)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The DHMSM EHR system is the core component of the Military Health System (MHS) GENESIS system. It 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 Department of Defense (DoD). As the modernization effort continues, the DHMSM EHR system will gradually replace the legacy EHR systems and become MHS GENESIS. From here in, DHMSM EHR is referred as MHS GENESIS.

MHS GENESIS is an electronic health record (EHR) information system that collects, processes, and distributes EHR longitudinally across the MHS, Department of Veterans Affairs (VA), TRICARE network of service providers, Federal and State agencies for approximately 9.6 million DoD beneficiaries, globe-wide.

MHS GENESIS collects, processes, and distributes the following PII/PHI:
- Patient identity information such as: Name and DoD ID Number for patient identity matching;
- Patient demographics information such as: Date of Birth, Mailing/Home Address, Home/Cell Phone Number, Official Duty Address, Official Duty Telephone Number, Work E-mail Address, Personal E-mail Address, Place of Birth, Race/Ethnicity, Gender/Gender Identification, Emergency Contact, Child Information, Marital Status, Religious Preference, and Social Security Number (if no DoD ID Number);
- Patient benefits information such as: Service record, Medicare, and Medicaid information for benefit determination and qualification;
- Medical information such as problem list, allergy list, medication list, procedure list, and immunization list for healthcare service delivery;
- Coordination of care information for inpatient and outpatient ancillary care services such as: laboratory, radiology, pharmacy orders and results for healthcare service delivery;
- Continuity of care information between VA and TRICARE network of contracted care service providers for coordination of healthcare service delivery; and
- Various population health analytics information for DHA Research Regulatory Oversight Office-authorized clinical trials, medical research, and disease registries. In general, population health information follows HIPAA "Minimum Necessary" rules that varies based on type of research, and the "use and disclosure" requires patient consent. (https://health.mil/Military-Health-Topics/Research-and-Innovation/Research-Oversight).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The selected PII is required for a variety of uses. Primarily, the PII is required for patient identification, verification and authentication in the course of scheduling and administering medical treatment. Additionally, the PII could be used for data matching when interfacing and sharing data with external medical and healthcare provider systems.

The intended use of the collected PII includes both mission-related and administrative applications. Administrative uses include such functions as scheduling, provisioning, dispensing and administering healthcare services. Mission-related uses include such actions as personnel availability, unit readiness, and statistical analysis of health and fitness metrics.

e. Do individuals have the opportunity to object to the collection of their PII? [X] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Submission of information is voluntary. If an individual chooses not to provide their information, comprehensive health care services may not be possible, the individual may experience administrative delays, and the individual may be rejected for service or an assignment. However, care will not be denied.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [X] 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.

Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. PHI is collected for permitted use and disclosures as as set forth in DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DoD 6025.18-R, C10.1. For uses other than treatment, payment and healthcare operations, individuals can authorize the use of their PHI by submitting DD Form 2870 and can request restrictions on the use of the PHI by submitting DD Form 2871.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

Because the MHS GENESIS will collect PII directly from individuals, it will be required to provide those individuals a Privacy Act Statement (PAS) at the time of such collection.

This statement serves to inform you of the purpose for collecting the personal information required by the MHS GENESIS system, and how it will be used.

AUTHORITY: 10 U.S.C. 8111, Sharing of Department of VA and DoD Healthcare Resources; 10 U.S.C. 1104, Sharing of Healthcare Resources with the Department of Veterans Affairs; 38 U.S.C. 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources; National Defense Authorization Act (NDAA) 2017, Defense Health Programs; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoD Regulation 6025.18-R, DoD Health Information Privacy Regulation; DoD Instruction 6040.45, DoD Health Record Life Cycle Management; DoD Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of MHS provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

ROUTINE USES: Information in your records may be disclosed to: Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care; Government agencies to determine your eligibility for benefits and entitlements; Government and non-government third parties to recover the cost of MHS provided care; Public health authorities to document and review occupational and environmental exposure data; and Government and non-government organizations to perform DoD-approved research.

Information in your records may be used for other lawful reasons which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD by DoD 6025.18-R. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

APPLICABLE SORN: The SORN applicable to this system is EDHA 07, Military Health Information System, until the completion and approval of the standalone MHS GENESIS SORN is completed.

DISCLOSURE: Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[X] Within the DoD Component	Specify.	System to system data exchanges between MHS GENESIS, Defense Medical Information Exchange (DMIX), and Joint Operational Medicine Information Systems (JOMIS). Where: - DMIX EHR systems facilitate data exchanges between MHS GENESIS and legacy EHR systems such as AHLTA and CHCS. - JOMIS EHR systems facilitate data exchanges between MHS GENESIS and theater EHR systems such as TMDS and TMIP-J.
[X] Other DoD Components	Specify.	Army, Navy, Air Force and Defense Manpower Data Center (DMDC) DEERS. Where: - Army, Navy, Air Force Military Medical Services are a part of MHS. - DMDC is the authoritative data source for patient identity and benefits information.

[X] Other Federal Agencies	Specify.	To the Department of Veteran Affairs (VA) for the purpose of enabling DoD data retrieval from the Federal/Bi-Directional Health Information Exchange (FHIE/BHIE) framework. Where: - VA EHR systems such as VistA for coordination and continuity of care via BHIE. - Department of Health and Human Services (HHS) information systems for Medicare and Medicaid benefits information via FHIE. - Social Social Administration's (SSA) Death Master File (DMF) for patient mortality status.
[X] State and Local Agencies	Specify.	To state and local public health agencies for mandatory reporting of infectious diseases.
[X] Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Leidos Partnership for Defense Health (LPDH). The contract Performance Work Statement (PWS) paragraph 5.1.10.12 and sub-paragraphs serve as required Business Associate Agreement (BAA).
[ ] Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [X] Commercial Systems

MHS GENESIS obtains:
- Patient identity, service status, immunization, and benefits information from DMDC via DMIX EHR systems;
- Continuity of care information from legacy EHR systems from AHLTA and CHCS via DMIX EHR systems;
- Coordination and continuity of care information from VA EHR systems via DMIX EHR systems using BHIE;
- Medicare and Medicaid benefits information from HHS information systems via DMIX EHR systems using FHIE; and
- Patient identity and mortality status information from SSA DMF system using FHIE.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [X] Face-to-Face Contact
- [ ] Fax
- [X] Information Sharing - System to System
- [X] Other *(If Other, enter the information in the box below)*
- [X] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [X] Website/E-Form

Patient information are collected via:
- Face-to-face contact at the time of patient registry within MTFs;
- Various Official Forms via TRICARE website (https://tricare.mil/forms)
- MHS GENESIS Patient Portal web site. This is not a web site open to public access. Rather, access is limited only to personnel with a current and appropriate affiliation with the DoD. Web site access is regulated through DoD Self-service Log-on (DS Log-on or DSL) which is a secure, self-service logon ID created by the Defense Manpower Data Center (DMDC) as an enterprise identity credential that allows access to individuals affiliated with the DoD. The MHS GENESIS Patient Portal web site (https://patientportal.mhsgenesis.health.mil) does use cookies; however, it does not employ persistent cookies that would be utilized to track users' patterns and/or trends. The patient portal web site employs only single session cookies.
- Other: Existing healthcare records that contain PII in legacy EHR systems, such as AHLTA and CHCS, or from commercial systems such as commercial hospitals, clinics pharmacies, laboratories or private medical/healthcare providers in general, will be transmitted using electronic interfaces and imported into the MHS GENESIS system.

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier EDHA07

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. Unscheduled

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

MHS GENESIS is currently under a records management survey to determine records and non-records held by the system. Until completion the records maintained by MHS GENESIS are considered unscheduled. Unscheduled records may not be destroyed or deleted. DHA will treat data within the MHS GENESIS system as Permanent until there is a complete schedule approved.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

10 U.S.C. 8111, Sharing of Department of VA and DoD Healthcare Resources; 10 U.S.C. 1104, Sharing of Healthcare Resources with the Department of Veterans Affairs; 38 U.S.C. 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources; National Defense Authorization Act (NDAA) 2017, Defense Health Programs; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoD Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoD Health Care Programs; DoD 6025.18-R, DoD Health Information Privacy Regulation; DoD Instruction 6040.45, DoD Health Record Life Cycle Management; DoD Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☒ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB paper is pending. 60-day FRN was published on 12/27/2017.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)***?** *(Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☐ Citizenship	☒ Disability Information	☒ DoD ID Number
☐ Driver's License	☐ Education Information	☒ Emergency Contact
☐ Employment Information	☐ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☐ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☒ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☒ Place of Birth	☐ Position/Title	☒ Protected Health Information (PHI)[1]
☒ Race/Ethnicity	☐ Rank/Grade	☒ Religious Preference
☐ Records	☐ Security Information	☒ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

MHS GENESIS collects the Social Security Number (if no DoD ID Number). Medical information includes information such as problem, allergy, medication, procedure, and immunization for continuity of care.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

The SSN Justification Memo is currently pending approval.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

Spouse information. Per DoDI 1000.30 (Enclosure 2), acceptable use case (11) Legacy System Interface, for SSN justification.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

All patients are given a "Cerner Unique ID" and it is associated with a DoD ID Number.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☐ No

b. What is the PII confidentiality impact level[2]? ☐ Low ☐ Moderate ☒ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

[x]	Cipher Locks	[x]	Closed Circuit TV (CCTV)
[x]	Combination Locks	[x]	Identification Badges
[x]	Key Cards	[x]	Safes
[x]	Security Guards	[ ]	If Other, enter the information in the box below

The MHS GENESIS system is hosted in a government-authorized commercial data centers using a centralized data and services architecture. Both the primary and alternate backup data centers provide physical security controls such as: cipher locks, combination locks, key cards, CCTV, safes, as well as 24/7 security guards.

The security Assessment Authorization boundary for the MHS GENESIS system includes the clinical application software operated at both the primary and alternate hosting data centers (locations TBD) and a limited number of hardware devices and software located a Medical Treatment Facilities (MTF) world-wide. The System Design Description (SDD, CDRL A021) provides a listing of hardware and software configuration items (CI) to be deployed to both MTFs and primary/alternate data centers.

Network connectivity, transport and boundary defense are outside the security assessment and authorization boundary and are provided by the enterprise-wide Medical Community of Interest (Med-COI) network that leverages Department of Defense Information Network (DODIN) transport and conforms to DoD Joint Information Environment (JIE) objectives. Cyber Security Service Provider (CSSP) services for the Med-COI network and connected MHS GENESIS systems are provided by SPAWAR Systems Center (SSC) Atlantic.

Data will be synchronized between the primary and alternate hosting data centers using various database methods. The disaster recovery plan (DRP, CDRL A037) defines the specific methods that implement data synchronization between the primary and alternate hosting data centers. The CONOPS for fail-over between the primary and alternate hosting centers is also outlined in the DRP (CDRL A037). Essentially, the alternate site is "warm" with all products installed and patched to current levels and all data is replicated from the primary site using an out-of-brand network. At the fail-over decision, the systems in the alternate site will be severed from replication and will be brought on-line for operations. When everything is on-line, the network connection (e.g., DNS record for the DHMSM URLs) will be adjusted by Med-COI and/or hosting data center network engineers. Once active, verification of connectivity for end users and interfaces will be performed.

Two MHS GENESIS software applications deployed at the MTFs (i.e., 7/24 Downtime Viewer and FetaLink Application) are installed and operated on local MTF-owned and operated computer hardware (e.g., servers, workstations, laptops). These two software applications are part of the DHMSM PMO delivered system; however, the operations and maintenance (O&M) concept of operations (CONOPS) for these two software applications specifies that the local MTF information technology (IT) and cybersecurity support staffs will perform all necessary system sans and software patching and updates at the direction of the DHMSM PMO.

In addition, the DHMSM PMO provides the MTFs with a pair of application servers (i.e., FetaLink) and a communications device (i.e., Cerner Communication Connectivity Engine [CCE]) if the MTF does not have an existing Data Innovations device for medical device integration. These two components are part of the DHMSM PMO managed system. The O&M for these two FetaLink servers and the CCE is performed by DHMSM staff. The O&M includes all necessary system scans and software patching and updates and monitoring of cyber events. The DHMSM PMO will remotely patch the FetaLink servers and CCE utilizing the DHMSM automation tools to push patches and updates over the Med-COI network.

The pair of FetaLink servers operating on Red Hat Enterprise Linus 6.7 is required to ensure high availability. If there is a failure within the facility, DHMSM will leverage the local DRP to recover system connectivity. In the event of an outage, the FetaLink devices will leverage the direct connection to the bedside monitor to view the information (which is normal operation). When connectivity is returned, data will be flowed to the central (Data Center) record. The CCE is a standalone device that provides MHS GENESIS connectivity to medical devices located at the MTF. CCE is not a high availability component; however, spares will be deployed to provide replacement capability in the event of component failure.

Physical security for the MHS GENESIS system components deployed within the MTF's security authorization boundary will be provided through common MTF security controls implemented and operated by the MTF.

(2) Administrative Controls. *(Check all that apply)*

- [ ] Backups Secured Off-site
- [x] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

In accordance with the "DISA Database Security Requirements Guide (SRG) Version 2, the primary database for MHS GENESIS is journaled where all the database transactions are replicated in the backup database located in the alternate backup data center. The transmission of transactional journals are encrypted, so does the backup database.

(3) Technical Controls. *(Check all that apply)*

- [ ] Biometrics
- [x] Command Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [x] External Certificate Authority Certificates
- [x] Firewall
- [x] Intrusion Detection System (IDS)
- [x] Least Privilege Access
- [x] Role-Based Access Controls
- [ ] Used Only for Privileged (Elevated Roles)
- [x] User Identification and Password
- [x] Virtual Private Network (VPN)
- [ ] If Other, enter the information in the box below

The MHS GENESIS system provides for the encryption of Data at Rest for all system data using approved DoD encryption methods (i.e., NIST FIPS 140-2 validated cryptographic modules). Encryption of Data at Rest is provided by the hardware platform hosting the client or server application. In Garrison all data center storage is encrypted by the SAN or the server (for locally hosted storage). All Garrison end-user devices are expected to encrypt local storage. All Theater hardware is expected to encrypt local disk.

The system provides for the encryption of Data in Transit for all system data using approved DoD encryption methods (i.e., NIST FIPS 140-2 validated cryptographic modules).
For 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 are encrypted using TLS as well.
For data exchanges between MHS GENESIS and trusted external systems, the transmission of data are also encrypted using TLS using X.509 certificates issued by DoD Certificate Authorities (CAs).

The MHS GENESIS system and its clinical applications provide users data access rights based upon job functionality, authority, and responsibility within the enterprise. This role-based access control (RBAC) is enforced through end-user applications. No user has direct access to a MHS GENESIS data store. The applications access a local Lightweight Directory Access Protocol (LDAP) with the user's credentials to pull the list of associated attributes.
This local LDAP (Active Directory) extends the DoD schema with the MHS GENESIS-specific least-privilege attributes. These attributes are used by the application as flags to identify many of the system capabilities and data access available to that user. When attributes/ authorizations change, the user receives the modified attributes/authorizations the next time the user logs on. Some access control attributes are maintained internally to the clinical applications within MHS GENESIS.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

To ensure adherence to HIPAA privacy and security rules, the following "Uses and Disclosures" agreements are in place for coordination and continuity of care:
- For data exchanges between MHS GENESIS and contracted-care service providers EHR systems: "Restatement I of the Data Use and Reciprocal Support Agreement (DURSA)", May 3, 2011; "Amendmen I to the Data Use and Reciprocal Support Agreement", September 25, 2014.
- For data exchanges between MHS GENESIS and VA EHR systems: "Memorandum of Understanding between the Department of Defense (DoD) and the Department of Veterans Affairs (VA) for Sharing Personal Information", March 14, 2014.
- For data exchanges between MHS GENESIS and LPDH-provided Clinical Application Services/Value-Added Networks (CAS/VAN): The contract Performance Work Statement (PWS) paragraph 5.1.10.12 and sub-paragraphs serve as required Business Associate Agreement (BAA).