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:

Purchased Care Operations System (PCOS) – TRICARE Encounter Data (TED)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

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)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] 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.

TRICARE Encounter Data (TED) is the core collection point for Military Health System (MHS) purchased care claim related data. Health care providers submit claims to insurance carriers for payments of services rendered to TRICARE beneficiaries. The carriers then electronically transmit their claims payment information to TRICARE using TED. (Note: TED is not allowed to replace data in an individual's record. The system can not make determinations about beneficiaries or employees using this data.)

TED receives data resulting from purchased care encounters from military personnel, dependents, and retirees.

Personally identifiable information (PII) and protected health information (PHI) collected in this system include:

Personal descriptors, ID numbers, health information, and life information.

Defense Health Agency (DHA) owns the requirements to the system. MHS operates the system. The sites accessing the system will be located at Managed Care Support Contractors (MCSCs) operations and DHA locations.

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 / PHI is collected in TED because it is the minimum amount of PII / PHI required to efficiently and effectively process a purchase care claim. The PII / PHI collected allows TED to be the global MHS industry leader in purchased care claims data records processing, and have one of the fastest claims processing cycles in the health care industry.The intended use of PII / PHI collected is to ensure that the following mission-related goals for TED and
MHS are met:

- Claims are tracked immediately after submission
- Payments claims are validated within three days
- Claims reimbursement is guaranteed to be faster and more efficient
- Electronic claims processing is streamlined
- Claims acceptance is automated
- Claims processing takes hours instead of days

e. Do individuals have the opportunity to object to the collection of their PII? ☐ 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.

TED is not the initial point of collection of PII / PHI from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII / PHI.

The initial point of collection for this system is the Health Care Provider. Health Care Providers submit claims to insurance carriers for payments of services rendered to TRICARE beneficiaries. The carriers then electronically transmit their claims payment information to TRICARE, using TED.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ 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.

TED is not the initial point of collection of PII / PHI from individuals; therefore individuals do not have the opportunity to consent to the specific uses of their PII / PHI.

The initial point of collection for this system is the Health Care Provider. Health Care Providers submit claims to insurance carriers for payments of services rendered to TRICARE beneficiaries. The carriers then electronically transmit their claims payment information to TRICARE, using TED.

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.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

PCOS TED is a system of records that collects personally identifiable information (PII) through system to system transfers only. Because the system does not collect PII directly from individuals, a Privacy Act Statement is not required.

TED is not the initial point of collection of PII / PHI from individuals; The initial point of collection for this system is the Health Care Provider.

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

☒ Within the DoD Component	Specify.	DHA
☒ Other DoD Components	Specify.	Claim information required for fraud and abuse litigation will be shared by the DHA Program Integrity (PI) Office with the Defense Criminal Investigative Services (DCIS) for legal/litigation purposes and with the Defense Information Systems Agency (DISA) for system administration purposes. Note: all DISA contractors have secret clearances.
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	

☐ 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: Planned Systems International (PSI) and General Dynamics Information Technology (GDIT)

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data, to ensure the confidentiality, integrity, and availability of government data. The contractor shall ensure that data which contains PHI is continuously protected from unauthorized access, use, modification, or disclosure. The contractor shall comply with all previously stated requirements for HIPAA, Personnel Security, Electronic Security, and Physical Security.

(Note: tier 3 contractors are required to undergo the DHSS personnel security process and have annually refreshed DD Form 2875 on file.)

All contracts contain language which require the contractor to comply with the HIPAA Privacy Rule and the HIPAA Security Rule. In addition, the contractor is required to comply with the Privacy Act of 1974, as amended.

☐ 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)*

- ☒ Individuals
- ☒ Databases
- ☒ Existing DoD Information Systems
- ☒ Commercial Systems
- ☐ Other Federal Information Systems

Professional and institutional health care providers, MCSCs, and other health insurance plans (including workers compensation).

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

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

Information Sharing from System-to-System – TED collects and distributes information via a dedicated collection environment (i.e., feed nodes). All feeds are transmitted using a combination of mechanisms including Secure Shell (SSH) / Secure File Transfer Protocol (SFTP), and Connect : Direct.

External partners use the Enterprise Infrastructure Program Office (EI) / DISA Business to Business (B2B) gateway to encrypt Wide Area Network (WAN) transfers. Internal partners (within the DoD / Defense Information Systems Network (DISN)) use the MHS Virtual Private Network (VPN) to encrypt WAN transfers. Data transmissions outside of these Internet Protocol Security (IPsec) VPNs use SFTP or Connect : Direct.

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier EDHA 04

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.

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

(3) Retention Instructions.

TED is currently in the Operations and Support phase of the system development life cycle.

Collection / Processing – TED collects and distributes information via a dedicated collection environment (i.e., feed nodes). All feeds are transmitted using a combination of mechanisms including SSH / SFTP, and Connect : Direct.

Use / Disclosure – Only privileged users can access the information, which is classified as For Official Use Only (FOUO). FOUO / SI may be disseminated within DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO / SI may also be released to officials in other departments and agencies of the Executive and Judicial branches in performance of a valid government function. TED follows the DHSS policy regarding marking / labeling. Each part of electrically transmitted messages containing FOUO information shall be marked appropriately.

Retention / Destruction – This system of records will be maintained according to the retention and disposition requirements for PCOS data which is the 911-01.3 TRICARE Contractor Claims Records record series number in the OSD Records Disposition Schedule (AI-15): Close out at end of the calendar year in which created; hold on-site 6 additional years.

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. Chapter 55, Medical and Dental Care; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary, and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; 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.

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	

person Identifier (Sponsor), Person Name (Patient), Person Identifier (Patient), Patient Identifier (DoD), DEERS Identifier (Patient).

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.

Pending

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

(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".

(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 designee.

c. How will the PII be secured?

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

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

TED has extensive physical security controls in place to prevent unauthorized access or accidental loss to the hardware and software components within. The physical facilities housing and supporting TED are sufficient to protect sensitive information and to mitigate the risks identified per the physical security risk analysis.

TED is housed at the Defense Enterprise Computing Center Detachment (DECCD) in Oklahoma City, OK. Entry to this facility is controlled by an Access Control System (ACS) using proximity card readers. During normal duty hours, the DECCDs access control staff located at the lobby security desk process all visitors. Entry is also controlled for the computer room and classified open storage area. All entry / exit points are locked and controlled by the ACS.

All external doors are alarmed and connected to the ACS. One internal room is approved for open storage for classified material / processing and is alarmed with motion sensors, all connected to the ACS. During normal business hours access control staff man the lobby security desk.

Access control staff maintain the entry access list, check badges, and issue VIP, visitor, and permanent badges. All persons with unescorted access will have a badge issued by DECCD. A visitor-cleared badge will be issued to persons with unescorted access that have forgotten their badge. A visitor-uncleared badge will be issued to all visitors who do not have a clearance. These visitors will be escorted at all times. The local Commander or Security Manager can designate free zones for areas under construction, and personnel with access to these areas that do not have a clearance will wear an uncleared visitor badge. Escort is required beyond these free zone areas.

All packages entering into DECCD are inspected by the access control staff for possible bombs. Access control staff conduct daily inspections of the building for suspicious activity. The Security Police Office receiving a phone call from the access control staff will immediately notify all post and patrols and furnish them with all available information. If suspicious activity is observed, the immediate area is sealed off by base patrols or the installation entry exit points may be blocked. Sealing off the installation is normally done in incidents with a high probability of obtaining suspect or vehicle descriptions. After entry and exit points are blocked, an on scene assessment must be made by the responding police force. This assessment is made within a few minutes after notification.

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

- [x] 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
- [x] If Other, enter the information in the box below

TED has extensive administrative security controls in place to prevent unauthorized access or accidental loss to the hardware and software components within the environment.

SDD is using DISA's Symantec NetBackup as its Backup and Recovery Strategy. Symantec NetBackup is a high-performance data protection application. Its architecture is designed for large and complex distributed computing environments. NetBackup provides scalable storage servers (master and media servers) that can be configured for network backup, recovery, archiving, and file migration services.
TED provides the data to be backed up with its schedule; DISA encrypts the data prior to storing it to tape.
DISA performs daily incremental and weekly full backups of the SDD Applications processing. Unless specified otherwise by the SDD Project Manager, the following backup retentions will apply: daily incremental backups – two weeks, weekly full backups – five weeks. Daily incremental backups are intended for local recovery use and will not be stored off-site. Weekly full backups are intended for remote disaster recover use and will be maintained off-site for the duration of the retention period. Failed backup processing will be reported on a daily basis to the applicable System Administrator for resolution and restarted as required.
Backup and retention of audit trails or other data which must be retained for time periods in excess of the standard DISA process indicated above are detailed in the SDD Project specific questions which appear at the end of this section and within Section 2.7.3.

Procedures are in place to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software. Per Defense Information Systems Agency (DISA) Enterprise Information Services (EIS) Service Level Agreement (SLA) this Cybersecurity control is shared. DISA is responsible for ensuring all devices are maintained within computer room floors, which require badge/Personal Identification Number (PIN) access. Symantec NetBackup is used for the DISA operating environments. Network devices are backed up using the defined DISA policy. DISA performs daily incremental and weekly full backups that are encrypted of the Defense Health Services System (SDD) processing environments which include Production and Production Test. DISA maintains a contractual relationship with Iron Mountain for storage and protection of back-ups. Mount points have been setup and storage allocated to perform backups via NetBackup for the application servers and database servers.

As contractually provided for by the DISA (EIS) Service Level Agreement (SLA) 2014, DISA is responsible for establishing, maintaining, and executing robust backup and restore procedures on behalf of all SDD APPLICATIONS servers staged within the Defense Enterprise Computing Center Detachment (DECC), San Antonio environment. At minimum, DISA performs daily incremental backups and weekly full backups of all SDD APPLICATIONS servers housed in Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) in 3326 General Hudnell Drive, San Antonio, TX 78226. Additional backups of SDD APPLICATIONS servers in the DECC, San Antonio environment are also provided by DISA, on an as necessary basis. DISA stores the recovery media used to backup SDD APPLICATIONS data in the DECC, San Antonio environment off-site at the Iron Mountain facility 11300 Partnership Drive Suite D, Oklahoma City, Oklahoma 73131.

Auditing is done at OS, Database and Application level. At each level, all successful/unsuccessful attempts are tracked and documented. TED auditing is enforced by the AIX operating system and is focused at recording system level events and aindividual users, including the date and time the event occurs. The audit function is configured to:
Create, maintain, and protect from modification or unauthorized access or destruction, an audit trail of access to objects it protects; limit access to the audit trail limit to only those personnel authorized access to such data; include in the audit record the origin (e.g., terminal ID) of the request for identification and authentication; include in the audit record the name of the object when an object is entered into a user's address space or when an object is deleted; configure the audit process so that the actions of one or more users be selectively audited based on individual identity; and record and ensure that the audit record identifies the following for each recorded events:
• Use of identification and authentication mechanisms.
• Introduction of objects into a user's address space (e.g., file open, program initiation).
• Deletion of objects.
• Actions taken by computer operators and system administrator and/or system security officers, and other relative security events.
• Date and time of the event.
• User.
• Type of event.
• Success (or failure) of the event.
Within the TED DECC, Oklahoma City and San Antonio environments, DISA, consistent with its assigned security responsibilities in the DISA-MHS SLA, maintains all TED audit records and conducts regular manual reviews of operating system audit trails on TED servers for inappropriate or unusual activity. DISA uses automated tools to facilitate the generation of reports and analysis based on audit records. DISA staff also performs daily and weekly backups of all TED audit records on external media, as required by DISA-MHS SLA and AU-9(2) Protection of Audit Information, Audit Backup On Separate Physical Systems / Components) control in DoDI 8510.1.
Within the TED DECC, Oklahoma City and San Antonio environments, TED Tier III vendor (ABSi) conducts daily manual reviews of application and database-level audit trails on TED servers for inappropriate or unusual activity. Examination of audit trails by TED Tier III vendor encompasses all instances of Informatica, Business Objects, and IBM DB2 incorporated into the Purchased Care Operating Systems (PCOS) accreditation boundary.

TED User Group personnel receive computer based training scenarios that take the following form and for some systems is required prior to being granted a system account. These training scenarios are initiated through the SDD Web Portal, self paced and, on a system basis, may be geared to the Level of Access specific to the job responsibilities for their position.
TED systems training is currently initiated and conducted through the SDD Web Portal. The training available presently through the SDD Web Portal will migrate to MHS Learn under a schedule to be determined by SDD leadership.
Required security training for all TED systems account holders is conducted and maintained through the SDD Web Portal. This training includes the following:
• Security Awareness Training prior to granting of a TED account request.
• Security Awareness Refresher training within one year from the account activation date and yearly thereafter until the account holder's access expires.
• Required reading of the SDD Rules of Behavior (ROB).

There is no user's manual for TED. There is no process in place for periodic review of PII contained in the system to ensure data integrity, availability, accuracy, and relevancy. If the data processed passes all of the edits in place, the data integrity should be intact. No further verification is currently done.

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

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

TED has extensive technical security controls in place to prevent unauthorized access or accidental loss to the hardware and software components within the environment.

A facility penetration testing process is in place that includes periodic, unannounced attempts to penetrate key computing facilities. Unless there is an overriding technical or operational problem, workstation screen-lock functionality is associated with each workstation. When activated, the screen-lock function places an unclassified pattern onto the entire screen of the workstation, totally hiding what was previously visible on the screen. Such a capability is enabled either by explicit user action or after a specified period of workstation inactivity (e.g., 15 minutes). Once the workstation screen-lock software is activated, access to the workstation requires knowledge of a unique authenticator. A screen lock function is not considered a substitute for logging out.

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

The privacy risks associated with PII / PHI collected include the mishandling of PII / PHI by authorized users of the system.

To mitigate these risks, PII / PHI in TED is protected with appropriate physical, technical, and administrative safeguards to ensure its continuing confidentiality, integrity, and availability in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

The privacy rights of beneficiaries and employees will be protected by ensuring access is only granted to authorized users who are required to have a sponsor to fulfill the standard Defense Health Services Systems (DHSS) procedures for gaining access to application data and functionality. Proper paperwork (DD Form 2875, System Authorization Access Request) is processed and vetted before access is granted to the system.