PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense and Veterans Eye Injury and Vision Registry (DVEIVR)
TRICARE Management Activity

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☒ **New DoD Information System** ☐ **New Electronic Collection**

☐ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number 13522

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI UII: 007-000001249

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DHA 24

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

10 U.S.C. 1071 note, Centers of Excellence in the Prevention, Diagnosis, Mitigation, Treatment, and Rehabilitation of Military Eye Injuries; 10 U.S.C. Chapter 55, Medical and Dental Care; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

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

Defense and Veterans Eye Injury and Vision Registry (DVEIVR) (formerly called the Military Eye Registry in the Congressional mandate for Department of Defense (DoD) to develop a registry) is a newly created centralized longitudinal clinical database that will integrate both DoD and Veterans Affairs (VA) data sources and be accessible to providers and clinicians in both departments across the continuum. The DVEIVR will be the first ocular and related data registry to combine DoD and VA clinical information into a single data repository for collecting and assessing data for longitudinal analyses of outcomes. The purpose of DVEIVR is to collect data related to eye injuries and vision impairment of Service Members and Veterans in order to promote and facilitate improvements in readiness, treatments, rehabilitation, development of clinical practice recommendations for trauma and diseases and to guide research. Authorized medical providers and clinicians across both the VA and DoD will have the ability to access registry information, such as data pertaining to medical treatments, surgical procedures, and visual outcomes of Service Members and Veterans who received treatment through DoD and/or VA. DVEIVR data includes service-related significant eye injuries and visual disorders due to traumatic brain injury.

The longitudinal analyses capability (i.e. repeated observations of the same data over periods of time) will provide the opportunity to enhance readiness, treatments, rehabilitation, and patient outcomes. It will also provide a critical information management framework needed to optimize outcomes, guide the development of clinical practice recommendations, and identify and guide emerging battlefield, rehabilitation, and restoration research requirements. The reporting capability will allow authorized users to produce and publish periodic reports based on operational and clinical requirements.

Data collection from source systems includes, but it is not limited to: demographic and related information, and clinical data regarding diagnoses, medical treatments, surgical interventions or other clinical procedures, and treatments, and follow-up for each case of significant eye and vision injury incurred by an Active Duty Service Member or Veteran. Data abstractors will enter clinical information that was handwritten by a provider or in a text format, also known as non-computable clinical data located in medical records.

Personally identifiable information (PII)/protected Health information (PHI) collected by this system includes: Name, truncated SSN, Race/Ethnicity, Cell Telephone Number, Mailing/Home Address, Marital Status, Emergency Contact, Other Names Used, Birth Date, Date of Death, Cell and/or Home Telephone Number, Biometrics, Medical Information, Social Security Number, Other ID Number, Electronic Data Interchange Person Number, National Provider Identifier, Gender, Personal E-mail Address, Disability Information, Rank, Military Occupational Specialty (MOS), Citizenship, Place of Birth, Mothers Maiden Name, Duty Status, and Service.

The DVEIVR Pilot was transferred to the DoD/VA Vision Center of Excellence in Fiscal Year 2012 (FY12), located at 2900 Crystal Drive Suite 210 Arlington, VA 22202, Technology Directorate (I&IM) under the direction of the Director of ITechnology.

PII will be used to interface with Defense Manpower Data Center Defense Eligibility Enrollment Reporting System (DEERS), Clinical Data Repository (CDR), Theater Medical Data Store (TMDS), Combat Trauma Registry (CTR), Joint Theater Trauma Registry (JTTR), and VA Eye Injury Data Store systems. The DVEIVR only utilizes the DEERS interface to verify eligibility, and subsequently only collects information from the remaining source systems (CDR, TMDS, CTR, JTTR, and VA Eye Injury Data Store). Communication is unidirectional with these systems.

A Privacy Impact Assessment (PIA) has been previously submitted and approved for this system with a final signature date of August 16, 2011.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

DVEIVR will aggregate data from a number of external sources and bring selected data elements into the vision registry. This data will include PII/PHI.

To mitigate any risks associated with the collection of PII, the application design includes data encryption as well as secured ports and it meets Information Assurance requirements. System security setting will default to shut off after 15 minutes of no activity. On a system level, all access will be tracked to ensure that only appropriate and approved personnel have access to PII/PHI data. The application hardware will be located in a secure and monitored environment.

DoD/VA Vision Center of Excellence (VCE) policies have established user roles and application processes, as well as tracking and monitoring of access and use. Data abstractors and quality reviewers/supervisors will have access to registry and medical records that include PHI and PII in order to perform their duties. Authorized ophthalmology and optometry users' access to the registry will be limited to de-identified registry data. All authorized DoD and VA contractors are required to complete DD Form 2875, System Authorization Access Request, prior to receiving a user name and password and assigned role.

Authorized users of the DVEIVR system are also prompted with DoD banners on the use of data they are accessing and their promise to protect it. At a minimum each user is expected to be currently working or assigned to DoD or VA facility or agency. The VCE will review/approve all access requests. Access to the DVEIVR will be role-based and may permit a user to access and query the system for single patient look-up. Only persons with an authorized and demonstrated need for PII/PHI will be granted the PHI/PII level of access. All users of the DVEIVR will be required to read and complete user application form related to privacy and protection of personal health information, training, access limitation, as well as violations for unauthorized use of data, monitoring of system access.

All users must have a Common Access Card (CAC) or PKI certificate in order to access the application. In addition users must input a user name and password in order to gain access to the system. Passwords will be periodically changed in accordance with DoD policy. VA users will access the system using a PKI certificate. Data abstractors work in a government approved location with limited access to visitors and/or unauthorized personnel. The use of "username/password" is to provide an initial log on that associates a CAC or Personal Identity Verification (PIV - issued by VA to VA users) card to a user account that was created by the system admin per a submitted and approved SAAR. Once the initial log on occurs and the CAC/PIV card is associated with the account, the user will authenticate using just the CAC/PIV. The "username/password" also satisfies the IA requirement that passwords need to be changed every 60 days. After 60 days, the system will be required to change the password even when using CAC/PIV

Other activities to protect PHI and PII include executed Memorandums of Understanding, data use agreements, and data transfer agreements. Quality assurance measures are in place and monitor access of the system.

The VCE implemented various processes to identify and mitigate any privacy risks, including but not limited to: specific authorization for each person requesting access to the system; training of users in privacy requirements; require each user to agree to comply with Privacy Act and HIPAA regulations; and periodically monitor each user's access of the registry. In addition the DVEIVR hardware (physical) is stored in a secure DoD environment (in compliance with DoD 8500.2, policies, and STIGs); and require encrypted access by each user (logical). Encryption is handled through SSL and is device agnostic. Backup functions are inherited from the hosting entity at DHHQ. Data at rest encryption is not required by the information owner. Data in transit is in compliance with FIPS 140-2.

Policies and procedures govern user access, consequences of violation of privacy and security breaches; and require users to annually comply with Privacy Act and HIPAA requirements.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Clinical Data Repository (CDR), Theater Medical Data Store (TMDS), Combat Trauma Registry (CTR), Joint Theater Trauma Registry (JTTR) will transfer data to the DVEIVR.

☒ **Other DoD Components.**

Specify. Navy, Air Force, Army, and Defense Manpower Data Center (DMDC) Defense Eligibility Enrollment Reporting System (DEERS)

Future requirements may result in an approved Institutional Review Board (IRB) project that permits the researcher to access PII/PHI in the DVEIVR to be shared with other DoD/VA Centers of Excellence (e.g. Defense Centers of Excellence (DCoE) Physiological Health (PH)/Traumatic Brain Injury (TBI), Hearing Center of Excellence (HCE), Extremities and Amputation Center of Excellence (EACE)).

☒ **Other Federal Agencies.**

Specify. Department of Veterans Affairs (VA) – future requirements such as an approved IRB project, PII/PHI in DVEIVR may be shared with other DoD/VA Centers of Excellence (e.g., Defense Centers of Excellence (DCoE) Physiological Health (PH)/Traumatic Brain Injury (TBI), Hearing Center of Excellence (HCE), EACE, National Intrepid Center of Excellence (NICOE)).

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Harris Corporation was awarded the data abstraction contract September 2011 to provide data abstraction support. Contract language explicitly states that the Contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in DoD 6025.18-R and DoD 8580.02-R, as amended. This includes all data abstractors completing annual Privacy and Health Insurance Portability and Accountability Act of 1996 (HIPAA) Training programs offered by either DoD or VA, and other mandatory training (e.g. Sexual Harassment, and Anti-Terrorism) as dictated by DoD and VA policy for Contractor who have access to or work on their information systems. Additional requirements shall be addressed when implemented.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

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

☐ **Yes** ☒ **No**

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

(2) If "No," state the reason why individuals cannot object.

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

DVEIVR receives data from CDR, CTR, TMDS, JTTR, DEERS, and VA Eye Injury Data Store, all of which collect PII directly from individuals and provide individuals the opportunity to object at the point of collection.

j. 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.

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

DVEIVR receives data from CDR, CTR, TMDS, JTTR, DEERS, and VA Injury Eye Data Store, all of which collect PII directly from individuals and provide individuals the opportunity to object at the point of collection.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☒ **None**

Describe each applicable format.

DVEIVR is not the initial point of collection of PII; therefore no Privacy Act Statement is required. This statement is given only at the initial point of collection.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.