

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:

Virtual Education Center (VEC)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

03/05/24

DHA Component Acquisition Executive (CAE) J-4 Program Manager for Medical Simulation & Training (PM MST)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)

- | | |
|---|--|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees |
| <input checked="" type="checkbox"/> from both members of the general public and Federal employees | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input checked="" type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

Virtual Education Center (VEC) is a customizable patient communication solution to easily distribute information, engage patients, fulfill compliance requirements, and drive utilization of services. VEC is a web-based application used by medical providers to send patients personalized educational material such as videos, website links, articles about medical conditions, pharmaceutical drugs, general health information, etc. Users can sign up for VEC through DS Logon, a secure Department of Defense (DoD) self-service logon credential that allows individuals to access various DoD and VA websites. While VEC does not allow patients to directly register new accounts, users can voluntarily add/update their email addresses and provide PII directly in the VEC application. The system also enables patients to receive notifications that educational material has been sent to them and they can view the material without creating a VEC account.

The personally identifiable information (PII) collected by the system includes last and first name, contact information, date of birth, race/ethnicity, rank, branch of service, and gender/gender identification. The system uses basic PII to communicate with, identify, and authenticate users to their accounts and utilizes demographic data of military service members (including dependents), federal personnel (including dependents), and any other beneficiaries of Tricare for analytical purposes, such as identifying trends in patient health conditions, to improve educational content and resource allocation. The intended users of the system are Tricare beneficiaries and their providers.

Although protected health information (PHI) is not explicitly listed in the application, system-internal chat bots may involve asking for PHI to automatically suggest educational content for the patient. Educational material sent by providers is not necessarily relevant to a patient's PHI, but the materials related to various conditions could potentially be linked to a patient's PHI. Providers may enter basic contact information to send notifications to patients in email or text messages. Patients have the ability to upload their own PII to their personalized library for storage purposes and reference. Patients can also share documents within their library which may contain PII with family members or other users of VEC whom they explicitly authorize.

The system receives PII directly from users of the system, including beneficiaries of the Department of Veterans Affairs (VA), who use DS Logon to access the system. Users can voluntarily add/update their email addresses directly in the VEC application and provide PII through that way. The operators of VEC, including the MTFs, are responsible for ensuring the privacy and security of the data within the system.

VEC is a commercial off the shelf system (COTS) owned by CoherentRx and managed by developers hired by CoherentRX. The system is hosted in the Defense Health Agency (DHA) Amazon Web Services (AWS) GovCloud.

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 PII collected is used to communicate with, identify, and authenticate users to their accounts and for analytical purposes, such as identifying trends in patient health conditions, to improve educational content and resource allocation.

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.

VEC users are required to create an account using DS Logon, which provides a secure Department of Defense (DoD) self-service logon credential allowing individuals to access various DoD and VA websites. As part of the account creation process, users are required to provide certain PII through DS Logon. Users also have the ability to provide PII, add/update their email addresses and/or if users do not wish to provide their contact information can update their account settings to disable notifications, directly in the VEC application. Non-account holding users can receive educational material through VEC's notification system without providing their contact information to a provider. However, they do not have access to a personalized library and are unable to store or reference educational material.

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.

VEC users are not explicitly provided with the opportunity to consent to the specific uses of their PII during the account creation process with DS Logon. However, PII use is limited to specific purposes, such as identifying, authenticating and communicating with users, and utilizing demographic data for analytical purposes, identifying trends in patient health conditions, to improve educational content and resource/funding allocation.

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

This statement serves to inform you of the purpose for collecting personal information as required by the Privacy Act of 1974, as amended, and how that information will be stored and used.

AUTHORITY: Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 USC Chapter Ch. 55, Medical and Dental Care; 10 USC 1097a, TRICARE Prime: Automatic Enrollments; Payment Options; 10 USC 1097b, TRICARE Prime and TRICARE Program: Financial Management; 10 USC 1079, Contracts for Medical Care for Spouses and Children: Plans; 10 USC 1079a, TRICARE Program: Treatment of Refunds and Other Amounts Collected Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 10 USC 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; 10 USC 1095, Health Care Services Incurred on behalf of Covered Beneficiaries: Collection From Third-party Payers; 42 USC 290dd, Substance Abuse Among Government and Other Employees; 42 USC 290dd-2, Confidentiality Of Records; 42 USC Ch. 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); DoD Manual (DoDM) 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs.

PURPOSE: The system uses basic PII to communicate with, identify, and authenticate users to their accounts and utilizes demographic data for analytical purposes, such as identifying trends in patient health conditions, to improve educational content and resource allocation. Although protected health information (PHI) is not explicitly listed in the application, system-internal chat bots may involve asking for PHI to automatically suggest educational content for the patient.

ROUTINE USE: In addition to those disclosures generally permitted under the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the DoD as a routine use pursuant to 5 USC § 552a(b)(3) as follows: to contractors and others performing or working for the Federal Government when necessary to accomplish an agency function related to this System of Records; to the Department of Health and Human Services, other federal agencies, and academic institutions for the purposes of public health activities and conducting research; to the Department of Veteran's Affairs (VA) for the purpose of providing medical care, to determine the eligibility for benefits, to coordinate cost sharing activities, and to facilitate collaborative research activities between the DoD and VA; to the National Research Council, National Academy of Sciences, National Institutes of Health, Armed Forces Institute of Pathology, and similar institutions for authorized health research. For a complete listing of the Routine Uses for this system, specifically those regarding disclosures to the Department of Justice, competent law enforcement authorities, Court and administrative law proceedings, the National Archives, and Records Management, Congress, and other appropriate Federal and non-Federal agencies, entities, and persons related to DoD breach detection and response efforts, refer to the applicable SORN. Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Rules, as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

Applicable SORN: EDHA 07, Military Health Information System (June 15, 2020; 85 FR 36190) <https://dpcl.d.defense.gov/Portals/49/Documents/Privacy/SORNS/DHA/EDHA-07.pdf>

DISCLOSURE: Voluntary. If you choose not to provide the requested information, there may be an administrative delay; however, care will not be denied and no penalties will be imposed.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?

(Check all that apply)

Within the DoD Component

Specify. Defense Health Agency (DHA) MTFs

Other DoD Components (i.e. Army, Navy, Air Force)

Specify. Air Force, Navy, Army, Marine Corps, and National Guard MTFs

Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify. Coast Guard MTF

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.

CoherentRx - The contractor shall protect all Personally Identifiable Information (PII) and Protected Health Information (PHI) and meet Federal information requirements in accordance with DoDI 5400.11. If the information is DoD CUI-specific (e.g., PII/PHI), then the contractor shall ensure the external cloud service provider meet the security requirements equivalent to FedRAMP High baseline. Per DFARS clause 252.204-7012, rapidly report (within 72 hours) cyber incidents involving DoD CUI to DoD Cyber Crime Center (DC3) via <https://dibnet.dod.mil/portal/intranet/>. In the event of a cyber-security incident involving a CUI-Specific breach, the contractor, in addition to reporting to the DC3, shall follow the incident reporting guidance prescribed in the TRICARE Operations Manual, Chapter 1, Section 5, Compliance with Federal Statutes at <https://manuals.health.mil/>.

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

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)

In-Person Contact

Paper

Fax

Telephone Interview

Information Sharing - System to System

Website/E-Form

Other (If Other, enter the information in the box below)

In-person collection of PII by healthcare providers may occur during medical visits or interactions with patients.

Website/E-Form: Here is the URL where the website is located <https://vec.health.mil/>

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 07

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

I. 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. GRS 5.2, item 020 (DAA-GRS-2017-0003-0002)

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

(3) Retention Instructions.

FILE NUMBER: 103-14
DISPOSITION: Temporary. Delete no more than 7 years from the date last modified. (See DoD DTM 22-001 on default disposition policies and OSD Records Manager guidance which file number to associate).

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 statute 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.

Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 USC, Chapter Ch. 55, Medical and Dental Care; 10 USC.1097a, TRICARE Prime: Automatic Enrollments; Payment Options; 10 USC 1097b, TRICARE Prime and TRICARE Program: Financial Management; 10 USC 1079, Contracts for Medical Care for Spouses and Children: Plans; 10 USC 1079a, TRICARE Program: Treatment of Refunds and Other Amounts Collected Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 10 USC 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; 10 USC 1095, Health Care Services Incurred on behalf of Covered Beneficiaries: Collection From Third-party Payers; 42 USC 290dd, Substance Abuse Among Government and Other Employees; 42 USC 290dd-2, Confidentiality Of Records; 42 USC Ch. 117, Sections 11131-11152, Reporting of Information; 45 CFR 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFS); DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs.

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.

VEC does not currently have an OMB control number but may require one as it collects PII directly from users.