



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Virtual Lifetime Electronic Record (VLER) / Direct Project Innovation Initiative (DPPI)

Military Health System (MHS) / TRICARE Management Activity (TMA)

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.

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.

U.S.C. 301, Departmental regulations; 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); 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.

The purpose of the Direct Project Innovation Initiative (DPPI) is to offer an alternative yet complementary solution for health information exchange across organizations by providing a method to share encrypted health information between known and trusted recipients over the Internet. The information exchange includes Personally Identifiable Information (PII) and Protected Health Information (PHI) for the purpose of patient identification and treatment.

DPPI provides the following benefits to the Department of Defense (DoD) and its users:

- Simple - DPPI is based on simple mail transport protocol (SMTP), otherwise known as e-mail. It is a simple and common information exchange method.
- Secure - DPPI uses Secure Sockets Layer (SSL) for secure internet connections in data exchange, as well as public key infrastructure (PKI) for identification and authentication.
- Standards-based - DPPI utilizes proven technology to exchange healthcare information.

The TRICARE Management Activity under the support of the Interagency Program Office (IPO) Virtual Lifetime Electronic Record (VLER) Program Management Officer (PMO) owns and operates DPPI. DPPI will be readily accessible via the web and is currently in testing phase.

DPPI collects and stores PII via the self-registration and course registration process. DPPI will be used to exchange PHI for the purposes of treatment. The following data elements may be collected as part of the user registration process or as part of the medical information exchanged:

- Name
- Social Security Number (SSN)
- Gender
- Birth date
- Place of birth
- Personal cell telephone number
- Home telephone number
- Personal e-mail address
- Employment information
- Medical Information
- Marital status
- Biometric information
- Disability information
- Emergency contact
- Electronic Data Interchange Personal Identifier (EDIPI)

Currently data is collected and exchanged for the following categories of individuals:

- DoD TRICARE beneficiaries
- DoD Military Treatment Facility (MTF) Providers and Staff

Program name: Virtual Lifetime Electronic Record (VLER)

POC: VLER Direct Project Innovation Initiative Project Manager (PM)

Address: 5111 Skyline Drive, Arlington, VA 22302

Phone: (703) 681-2274

E-mail: Shantoyia.Gates@tma.osd.mil

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

Privacy risks associated with Direct Project Innovation Initiative (DPPI) include the potential for misuse of information obtained through DPPI by authorized users, and the potential for the access of records, in whole or in part, by

individuals who are not authorized to access DPPII.

The Military Health System (MHS) represents the authorized users of DPPII. The TRICARE Management Activity (TMA) Privacy and Civil Liberties Office (Privacy Office), a component of MHS, develops and manages the delivery of specialized, role-based Health Insurance Portability and Accountability Act (HIPAA) Compliance and Privacy Act training for all MHS personnel. Privacy Act and HIPAA regulations are strictly enforced. Access to DPPII is limited to approved users within MHS. Additionally the application requires new users to submit a System Authorization Access Request (SAAR) form (DD 2875) and be vetted and approved by the information system data owner.

An individual's privacy is safeguarded throughout the information lifecycle within the DPPII system. Users connect to the DPPII system through an encrypted secure connection protocol. The data is then stored behind various network defense assets and stored securely to ensure privacy of the information is maintained. All incoming and outgoing information is encrypted.

All DPPII support personnel are required to complete initial and annual IA training. This training is given and recorded through the Personnel and Readiness Information Management (P&RIM) Office of the Under Secretary of Defense (Personnel and Readiness) (OUSD (P&R)).

DPPII also safeguards against unauthorized access through Defense Information Assurance Certifications and Accreditation Process (DIACAP) which enforces administrative, technical, and physical controls. The controls are outlined in detail in DoD Instruction 8500.2 Information Assurance Controls publication. The clinical transactions supported by DPPII are HIPAA compliant.

In accordance with the DoD 5400.11-R, "Defense Privacy Program," May 14, 2007, whenever a DPPII user and/or DPPII support personnel becomes aware of an actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purpose where one or more individuals will be adversely affected, DPPII will:

- Notify appropriate leadership personnel within the DPPII Program Office immediately;
- Report to the United States Computer Emergency Readiness Team within one hour of breach discovery;
- Report to the TMA Privacy and Civil Liberties Office within 24 hours at PrivacyOfficerMail@tma.osd.mil; and
- Notify all affected individuals within 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained, if necessary.

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.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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

Specify.

All contracts contain language which require the contractor to comply with the Health Insurance Portability and Accountability Act (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. 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.

DPII 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. DPII receives data from the MHS and private healthcare providers which collects PII / PHI 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.

DPII 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. DPII receives data from the MHS and private healthcare providers which collects PII / PHI 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.

- | | |
|---|--|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

The collection of patient records and their retrieval by a unique personal identifier means that the VLER / DPPII system is a system of records. DPPII receives data from the MHS which collects PII / PHI directly from individuals and provides Privacy Act Statements at the point of collection. Therefore, since DPPII is not the initial point of collection for those records, a Privacy Act Statement is not necessary.

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.