PRIVACY IMPACT ASSESSMENT (PIA)

For the

Data Exchange Service (DES)
Defense Health Agency (DHA)

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: 17586 (DMIX)
- ☐ **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: 007-00100462 (DMIX)

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 EDHA 07

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.

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 Data Exchange Service (DES) is to offer a solution for health information exchanges across organizations. Therefore, DES provides legacy health record data to systems that support clinical decisions and benefit adjudication. DES does not provide a Graphical User Interface (GUI) for providers to enter patient information into the system.

DES uses Department of Defense (DoD) approved encryption method that comply with Privacy Act and system Information Assurance controls, and ensures that the health information is only shared 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.

In summary DES provides the following benefits to the DoD and its users:
• DES is a web application that uses Hypertext Transfer Protocol Secure (HTTPS), Representational State Transfer (REST), and Simple Object Access Protocol (SOAP).
• DES using approved DoD ports.
• DES uses Secure Sockets Layer (SSL) and therefore provides secure internet connections when exchanging data.
• DES has implemented the public key infrastructure (PKI) for identification and authentication.
• DES utilizes Standards-based and proven technologies to exchange healthcare information.

The following data elements may be collected as part of the user registration process or as part of the medical information exchanged includes the following:

Name; Other Names Used; Social Security Number; Electronic Data Interchange Personal Identifier; Gender; Race/Ethnicity; Birth Date; Place of Birth; Personal Cell Telephone Number; Home Telephone Number; Personal Email Address; Mailing/Home Address; Mother's Maiden Name; Spouse Information; Marital Status; Child Information; Medical Information; Disability Information; and Emergency Contact.

DES currently collects and exchanges data for the following categories of individuals, from systems that it interfaces with:
• DoD TRICARE beneficiaries
• DoD Military Treatment Facility (MTF) Providers and Staff

DES is owned and operated by the DHA under the support of the Interagency Program Office (IPO) DES Program Management Officer (PMO).

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

Privacy risks associated with DES PII collected by exchanging information with the systems that it interfaces with include the potential for misuse of information obtained through DES by authorized users, and the potential for the access of records, in whole or in part, by individuals who are not authorized to access DES.

The Military Health System (MHS) represents the authorized users of DES. These include DoD providers in external partner facilities that have been authorized to see DoD data in accordance with the DURSA agreement (http://sequoiaproject.org/ehealth-exchange/onboarding/dursa/).

The Department of Health Agency (DHA) 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) Privacy and Privacy Act training for all MHS personnel. Privacy Act and HIPAA regulations are strictly enforced. Access to DES 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 DES system. Systems connect to the DES 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 DES 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)).

DES also safeguards against unauthorized access through DoD Risk Management Framework (RMF) which enforces administrative, technical, and physical controls. The controls are outlined in detail in DoD Instruction 8500.01, Cybersecurity and National Institute of Standards and Technology (NIST) Special Publication 800.53. The clinical transactions supported by DES are HIPAA compliant.

In accordance with the DoD 5400.11-R, "Defense Privacy Program," May 14, 2007, whenever a DES user and/or DES 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, DES will:
• Notify appropriate leadership personnel within the DES Program Office immediately;
• Report to the United States Computer Emergency Readiness Team within one hour of breach discovery;
• Report to the DHA Privacy and Civil Liberties Office within 24 hours; 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.

DES receives data from:
Bidirectional Health Information Exchange (BHIE)-Share (currently provides access to data from the Composite Health Care System (CHCS) and Essentris)
Clinical Data Repository (CDR)
Theater Medical Data Store (TMDS)
All participants of the eHealth Exchange

Data is exposed to:
TRICARE Online (TOL)
Joint Legacy Viewer (JLV)
Private HIEs (health information exchanges)

Future systems that DES will receive data from:
CHCS
ESSENTRIS
Defense Healthcare Management Systems Modernization (DHMSM)
DoD Health Deployment Assessment Repository
Health Artifact and Image Management Solution (HAIMS)

Future systems that the data will be exposed to include:
DHMSM

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. Department of Veterans Affairs (VA)
- future system includes the VA Enterprise messaging interfaces (VA eMI)

Social Security Administration (SSA)

☐ **State and Local Agencies.**

Specify.

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

Specify. All employees who have contact with PII/PHI are trained in appropriate handling of PII/PHI in accordance with current DoD regulations and complete annual HIPAA training.

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

Specify. All participants of eHealth exchange (registered and authorized by Sequoia)

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.

DES is not an authoritative data source, therefore it is not the initial point of collection of PII / PHI from individuals.

However, systems like AHLTA incorporate the DES capability (opt in/opt out and Medical Record Authorization System (MRAS)) which provides a standardized user interface and process for providing the user the opportunity to object to the collection of their PII. DES is a standalone system and not part of the AHLTA baseline.

DES receives data from the Department of Veterans Affairs, DHA, as well as any future systems that collect PII / PHI directly from individuals as the authoritative data source and each of these systems provide individuals the opportunity to object at the point of collection.

There is one exception, within DoD; Military personnel are not provided this option in accordance with current DoD policies.

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.

DES is not an authoritative data source, therefore it is not the initial point of collection of PII / PHI from individuals.

However, systems like AHLTA incorporate the DES capability (opt in/opt out and MRAS) which provides a standardized user interface and process for providing the user the opportunity to object to the collection of their PII. DES is a standalone system and not part of the AHLTA baseline.

DES receives data from the Department of Veterans Affairs, DHA, as well as any future systems that collect PII / PHI directly from individuals as the authoritative data source and each of these systems provide individuals the opportunity to object at the point of collection.

There is one exception, within DoD; Military personnel are not provided this option in accordance with current DoD policies.

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.

DES only interfaces with systems and no user has direct access to the data, it does leverage the unique personal identifier to retrieve information specific to the individual that the target systems is requesting.

Since DES is not an authoritative data source, the source data systems as defined collect the PII/PHI directly from individuals at the time the information is collected; the source system provides the individual the Privacy Act Statements. Therefore, a privacy advisory is not required for the DES system.

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.