PRIVACY IMPACT ASSESSMENT (PIA)

For the

Special Needs Program Management Information System (SNPMIS)
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: 163
- ☐ **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: 007-000000117

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 16 DoD

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	In process. The 60 day FRN (published on 4/1/14) lists the OMB Control Number as 0720-TBD. OMB Project ID: 007-000000117
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. Chapter 55, Medical and Dental Care; 20 U.S.C. Chapter 33, Education of Individuals with Disabilities; 20 U.S.C. 921, Defense Dependents' Education System; DoD Instruction 1342.12, Provision of Early Intervention and Special Education Services to Eligible DoD Dependents; 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.

Special Needs Program Management Information System (SNPMIS) provides access to a comprehensive program of therapy, medical support, and social services for young TRICARE beneficiaries with special needs. SNPMIS is DHA's automated information system designed to ensure the DoD meets the unique information requirements associated with implementation of the Individuals with Disabilities Education Act (IDEA).

SNPMIS captures records referral, evaluation, eligibility, and service plan data for children with special needs who are eligible for early intervention and special education services under IDEA. Management reports provide historical analysis to monitor ongoing improvements in quality of care initiatives. It also allows program managers to identify areas where additional services are needed. At the service level, activities of different programs can be compared to determine best practices that can be implemented throughout the Educational and Developmental Intervention Services (EDIS) clinics.

SNPMIS consists of a government-developed application that includes a Graphical User Interface (GUI), an open database management system, and Government Off-the-Shelf (GOTS) and Commercial Off-the-Shelf (COTS) software.

SNPMIS collects the following types of personal information from or about individuals: personal descriptors, identification numbers, ethnicity, health, life, and education information. Records contained in the system may be retrieved by name or other unique identifier.

This system is a distributed data collection application with database servers distributed at various Military Health System Application Access Gateways (MAAGs) located within the Continental United States (CONUS) and Outside the Continental United States (OCONUS). SNPMIS is currently used in 43 EDIS clinics at Army, Navy, and Air Force installations worldwide.

Categories of individuals in the system include children of members of the Armed Forces and civilians who are entitled to receive early intervention and special education services from the DoD under the IDEA.

A PIA has been previously submitted for this system with a final signature date of May 16, 2012.

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

Potential privacy risks include the loss of a provider's notes or stolen data. As to loss of data due to SAN disk failure at a MAAG site, the consequence could be that information entered after the night's scheduled backup must be re-entered into the system. Daily Backups can restore data up to the time the backup took place. Data not included in the daily backup will need to be re-entered. No other system data is impacted.

As to stolen data, the privacy risk involves sensitive data that may identify a particular child or children and their related sponsors. Risk of accessibility to stolen data is low as the data is stored at DHA's MAAG site locations accessible only via the Application Virtualization Hosting Environment (AVHE) infrastructure login using 2-factor authentication. In addition to the 2-factor authentication required by the hosting AVHE infrastructure, and before access into the application is granted, SNPMIS user credentials are required to be entered by the user and are verified against the application's database.

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.

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

Specify. Joint Commission on Accreditation of Healthcare Organizations (JCAHO) during an on-site survey for the purpose of achieving accreditations for compliance with certain standards and accreditation requirements.

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.

Individuals have an opportunity to object to the use(s) of their PII/PHI. The collection of PII/PHI in the system is voluntary. However, failure to provide certain information necessary to determine eligibility may result in denial of services. The information collected is a record of care. Parents are given a copy of their procedural safeguards, which provides them with specific rights and access to dispute resolution. During family interviews, parents have the option to "decline to state" on non-essential data (e.g., race and ethnicity).

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

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.

Individuals have an opportunity to consent to/authorize the use(s) of their PII/PHI. If a child receives care, data on care and the demographic information necessary to retrieve records are required. Data collection of PII is also required to ensure compliance with the Individuals with Disabilities Education Act. Before information is released to an external agency the parents must sign a Health Insurance Portability and Accountability Act (HIPAA) authorization.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Privacy Act Statement is included on forms used to collect information from families. EDIS information is maintained as a secondary record in the clinic and in electronic format.

The purpose of this screening/evaluation is to determine your child's strengths and needs. EDIS recognizes families as a vital part of the screening/evaluation team. All screenings/evaluations will be conducted by qualified staff and reviewed with the family. If a child is determined to have a developmental delay or biological risk a referral to Exceptional Family Member Program (EFMP) will be made.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 20 U.S.C. Chapter 33, Education of Individuals with Disabilities; 20 U.S.C. 921, Defense Dependents' Education System; DoD Instruction 1342.12, Provision of Early Intervention and Special Education Services to Eligible DoD Dependents; and E.O. 9397 (SSN), as amended.

PURPOSE: To collect information necessary to determine a child's eligibility for Educational and Development Intervention Services (EDIS) and to plan and deliver appropriate services to eligible families

ROUTINE USES: Information in your records may be disclosed to the Joint Commission on Accreditation of Healthcare Organizations to comply with certain standards and accreditation requirements. Information may also be provided to other federal, state, and local government units for compliance with laws relating to eligibility, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, coordination of benefits, and civil or criminal litigation.

Your records may be disclosed outside of DoD in accordance with the DoD Blanket Route Uses published at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

Any protected health information (PHI) in your records may be used and disclosed generally as

permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

DISCLOSURE: The collection of your information in the system is voluntary. However, failure to provide certain information necessary to determine eligibility may result in denial of services.

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.