PRIVACY IMPACT ASSESSMENT (PIA)

For the

International SOS (Intl.SOS) TriCase (Case Management and Authorization System)
TRICARE Management Activity (TMA) / Managed Care Support Contractor (MCSC)

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

□ **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

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 DTMA04

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 progress

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; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary and Medical Care; 32 CFR Part 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.

TriCase (Case Management and Authorization System) manages cases involving the coordination of medical care and medical transportation. The system provides International SOS (Intl.SOS) employees with a central application to interact with beneficiaries, providers, family members, and government contacts to manage healthcare delivery activities. TriCase is available in four Intl.SOS offices worldwide and is limited to authorized TRICARE users who meet appropriate clearance levels. The system has been tailored to support TRICARE Management Activity (TMA) over the years for the single worldwide TRICARE Global Remote contract.

The primary purpose of TriCase is to provide support for the core healthcare management functions of the TRICARE Overseas Program (TOP), including medical evacuations and medical / dental authorizations.

The system allows Intl.SOS coordinators and medical staff to:

- View a patient's medical history as documented in TriCase;

- Document interaction with the patient (including e-mails, letters, faxes, and phone conversations). Notes and actions are documented in the system to allow the ability to track progress of all types of cases and authorizations;

- Validate enrollment and eligibility for services;

- Assign Intl.SOS staff with various tasks to manage an incident of care (i.e., a defined case or an authorization where a beneficiary requires assistance);

- Access to all information to administratively and medically manage a case; and

- Arrange for active duty dental care in all remote overseas locations.

Information may be collected on any TRICARE beneficiaries that call into an Intl.SOS Alarm Center for medical support under the TRICARE program. This includes:

- Active Duty Service members
- National Guard members
- Reserve members
- Retired Service, National Guard, and Reserve members
- Families of Active Duty Service, National Guard, and Reserve members
- Anyone covered by any TRICARE health plan

Below is a list of the personally identifiable information (PII) / protected health information (PHI) that are stored in TriCase:

- Name
- Other Names Used
- Social Security Number (SSN)
- Gender
- Date of Birth
- Contact Phone Number
- Contact e-mail Address
- Mailing Address
- Medical Information
- Military Records
- Other (Age; Patient Current Location; Sponsor Name, SSN, Date of Birth, Gender, and Military Records; enrollment location; and Active Duty (AD) / Active Duty Family Members (ADFM) status)

This system will exist in a separate infrastructure environment from the case management system used for other businesses within Intl.SOS.

Enrollment is validated via information obtained from the claims processing subcontractor Wisconsin Physician Services (WPS).

TRICARE Operations POC:

International SOS
3600 Horizon Blvd
Trevose, PA 19053
(215) 942 - 8000

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

This system strictly operates within a DoD Information Assurance Certification and Accreditation Process (DIACAP) environment and does not interact with or share terminals / computers with systems outside of the controlled environment. Calls and cases entered into this system are audited for quality. Intl.SOS has put in place quality checkpoints (e.g., monitoring phone calls and reviewing historical case history) to mitigate, identify, and respond to any privacy issues that occur during case handling.

If a risk is identified, the Global Quality Support Team will review it with the Operations Management Team to determine a course of action. If there is a pattern of consistent issues with personnel managing and protecting PII / PHI, the staff members position will be evaluated by management and Human Resources (HR).

Intl.SOS has put in place the following checkpoints to mitigate privacy risks:

- Only authorized staff who meet appropriate clearance (variable by country) are allowed to utilize the TriCase system.

- Intl.SOS coordinators only access patient information when managing cases or processing authorizations.

- Information is only entered and stored in the TriCase system, not used for other purposes.

- Intl.SOS policy ensures that information and correspondence between Intl.SOS staff working in TRICARE and patients is documented in TriCase.

- All notes, e-mails, phone calls, and activities are tracked. All e-mails are sent through TriCase to monitor the activities of the user.

- Intl.SOS audits all alarm centers to meet the comply with Health Insurance Portability and Accountability Act of 1996 (HIPAA) as the global standard for operations and protecting privacy.

- All personnel are required to attend annual HIPAA and privacy trainings.

- Intl.SOS operates a Continuity of Operations Plan (COOP) for the TOP. This document is included as part of the DIACAP certification.

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. Military Treatment Facilities (MTFs)

☒ **Other DoD Components.**

Specify. Composite Health Care System (CHCS); Defense Enrollment Eligibility Reporting System (DEERS)

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Wisconsin Physician Services (WPS).

The contract with WPS contains language which requires the contractor to comply with the 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.

Submission of information is voluntary. An individual can object to providing information either at the time the referral is provided to the MTF (that will be then provided to Intl.SOS), or at the time they are asked to provide information by telephone, e-mail, or fax.

In the event the MTF is providing the information to Intl.SOS vie referral, individuals cannot object with Intl. SOS and must object with the MTF collecting the information. If an individual refuses to provide information, comprehensive healthcare may not be possible.

Individuals who contact Intl.SOS for support must supply PII in order to validate enrollment in TRICARE. If the information is not supplied, Intl.SOS cannot support them for the program. This is the only way to validate enrollment for TRICARE beneficiaries.

(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.

Intl.SOS staff follow a script for new callers. Some of the script asks members for PII in order to validate their enrollment in a TRICARE health plan.

In the event a referral is received from the MTF, PII appears on the MTF form submitted. In these instances, Intl.SOS does not have direct contact with the member, and so no consent is necessary as consent has already been given at the time of collection.

Consent to the specific uses of PII is obtained as necessary in accordance with DoD 5400.11-R, Department of Defense Privacy Program, C.4.1.3.

PHI is collected for permitted uses and disclosures as set forth in DoD 6025.18-R, DoD Health Information Privacy Regulation. Individuals are informed of these uses and are given the opportunity to authorize or restrict the use of their PHI based on the procedures in place at the local facility where the data is collected and maintained, in accordance with DOD 6025.18-R.

(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.

This statement serves to inform you of the purpose for collecting personal information required by the TriCase (Case Management and Authorization System) and how it will be used.

AUTHORITY: 10 U.S.C. Chapter 55, Medical and Dental Care; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); and E.O. 9397 (SSN), as amended.

PURPOSE: To obtain information on an individual necessary to manage and coordinate medical/ dental care and medical transportation for the individual and to interact with beneficiaries, providers, family members, government representatives and others to manage the delivery of healthcare services to the individual.

ROUTINE USES: Information collected may be used and disclosed generally as permitted under 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, as implemented by DoD 6025.18-R, the DoD Health Information Privacy Regulation. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the DoD “Blanket Routine Uses” under 5 U.S.C. 552a (b) (3) apply to this collection. Collected information may be shared with the Departments of Health and Human

Services, Homeland Security, and Veterans Affairs and other Federal, State, local, and foreign government agencies, private business entities under contract with the Department of Defense, individual providers of care, and third parties on matters relating to eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance and appraisal, peer review, program integrity, third-party liability, coordination of benefits, and civil and criminal litigation.

DISCLOSURE: Voluntary: If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays or may result in the inability to process an individual's request or provide comprehensive healthcare.

NOTE: A Privacy Act Telephone Script is currently under development for this 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.