

## 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:**

Spectacle Request and Transmission System (SRTS)

**2. DOD COMPONENT NAME:**

Defense Health Agency

**3. PIA APPROVAL DATE:**

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** (Check one. Note: foreign nationals are included in general public.)

- From members of the general public  From Federal employees and/or Federal contractors  
 From both members of the general public and Federal employees and/or Federal contractors  Not Collected (if checked proceed to Section 4)

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

- New DoD Information System  New Electronic Collection  
 Existing DoD Information System  Existing Electronic Collection  
 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.**

The Spectacle Request and Transmission System (SRTS) is a Government developed clinic and laboratory web-based application that serves as the sole electronic system for ordering and tracking military eyewear. SRTS provides the electronic version of DD Form 771, Eyewear Prescription, used to collect the information required to fabricate prescription eyewear. SRTS manages the spectacle requests for personnel within the Department of Defense (DoD) Uniformed Services, United States Coast Guard, Department of Veterans Affairs, Federal Bureau of Prisons, United States Public Health Service, United States Department of State, Bureau of Indian Affairs, Reserve Officer Training Corps (ROTC), various humanitarian missions, as well as manages SRTS for use by other DoD Components and other Federal agencies.

The PII collected includes name, social security number, gender, date of birth, pay grade, mailing address, telephone numbers, e-mail address and medical information. SRTS is managed under the Clinical Support Program Management Office (PMO) Health Information Technology (HIT/J6), Solution Delivery Division (SDD).

**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)

PII is collected to identify the patient when establishing records used to order eyewear, make the eyewear, insure the eyewear is delivered to correct individual, and track eye health for the individual.

**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.

Individuals have the opportunity to object at the face-to-face at the point of care. Individuals are presented Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records for review and signature. This form is placed in the patient's medical record. If individuals does not sign form or object to the collection of their PII, comprehensive medical care and/or eyewear can be delayed or not distributed.

**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.

Individuals have the opportunity to consent to specific uses of their PII face-to-face at the point of care. Individuals are presented Department of Defense (DD) Form 2005, Privacy Act Statement – Health Care Records for review and signature. This form is placed in the patient's medical record. If individuals do not sign form or does not provide consent, comprehensive medical care and/or eyewear can be delayed or not distributed.

**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

**AUTHORITY:** AR 40-63, SECNAVINST 6810.1, and AFI 44-121, Ophthalmic Services; and E.O. 9397 (SSN), as amended.

**PURPOSE:** Collects information to process military eyewear orders and track eye health for individuals.

**ROUTINE USE(S):** Use and disclosure of your records outside of DoD may occur in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)). Collected information may also be shared with the Departments of Health and Human Services, Homeland Security, and Veterans Affairs, and other Federal, State, local, or foreign government agencies, authorized private business entities, including entities under contract with the Department of Defense and individual providers of care, on matters relating to eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.

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, healthcare operations, and the containment of certain communicable diseases.

For a full listing of the applicable Routine Uses, refer to the applicable SORN.

**APPLICABLE SORN:** EDHA 20 DoD, Department of Defense Suicide Event Report (DoDSER) System (April 15, 2016, 81 FR 22240) is the system of records notice (SORN) applicable to DoDSER. The SORN can be found at:  
<https://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/569974/a0040-66b-dasg/>

**DISCLOSURE:** Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in the inability to provide ophthalmic services or process requests.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)**

Within the DoD Component

Specify. 

Defense Health Agency systems Data is shared to help facilitate and document health care.
--

- US Air Force
- US Army
- US Navy

Other DoD Components

Specify. 

- Defense Manpower Data Center (DMDC) - US Army Medical Protection System (MEDPROS) - US Air Force Aeromedical Services Information Management System (ASIMS) Data is shared to help facilitate and document health care.
--

- US Postal Service (USPS)
- US Coast Guard
- Department of Veterans Affairs
- Federal Bureau of Prisons

Other Federal Agencies

Specify. 

- US Public Health Service - US Department of State - Bureau of Indian Affairs - Reserve Officer Training Corps (ROTC) Data is shared to help facilitate and document health care.
--

National Guard

State and Local Agencies

Contractor companies are Bestica and IBA. They are authorized to create accounts which requires the patients PII.

Contractors are required to complete and sign a DD-Form 2875 System Authorization Access Request (SAAR) to input data into SRTS, which includes a Privacy Act Statement authorized by Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. Their respective contracts contain language that mandates compliance with the Privacy Act; complete Health Insurance Portability and Accountability Act (HIPAA) training; and local policy requirements that protect PII.

Contract language: 5.6.3 Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws:

Specify. The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with Defense Federal Regulations Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference current versions DoDD 5400.11, "DoD Privacy Program," and DoD 5400.11-R, "DoD Privacy Program." The Contractor shall also comply with federal laws relating to freedom of information and records management. The Contractor shall analyze any breach of PII/PHI for which it is responsible under the terms of this Contract under both the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA), if applicable, to determine the appropriate course of action under each requirement, if any."

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.)



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
- Existing DoD Information Systems
- Other Federal Information Systems
- Databases
- Commercial Systems

PII is collected from individuals and electronically from Defense Enrollment Eligibility Reporting System (DEERS) via a DMDC interface.

**j. How will the information be collected?** (Check all that apply and list all Official Form Numbers if applicable)

- E-mail
- Face-to-Face Contact
- Fax
- Information Sharing - System to System
- Other (If Other, enter the information in the box below)
- Official Form (Enter Form Number(s) in the box below)
- Paper
- Telephone Interview
- Website/E-Form

The name, address, phone number, email address, SSN, and DoD ID can be collected from official DD-Form 771 Eye-wear Prescription, Defense Enrollment Eligibility Reporting system (DEERS) and Defense Manpower Data Center (DMDC). Patients address will be verified by U.S. Postal Service. Information collected via email, paper, and telephone based on Standard Operating Procedures for account creation and/or help desk troubleshooting.

The SRTS web link: <https://srtswb.amedd.army.mil/> is on the world wide web however, only authorized personnel that have completed and sign a DD-Form 2875 System Authorization Access Request (SAAR).

Information Sharing - SRTS interfaces with the following systems:

- US Army Medical Protection System (MEDPROS)
- US Air Force Aeromedical Services Information Management System (ASIMS)
- Army Optical Lab Management System, Optivision and Optifax (ALMS)
- Navy Optical Lab Management System, VisionStar (NLMS)
- Defense Manpower Data Center (DMDC)
- Defense Optical Fabrication Enterprise Management System (DOFEMS)
- United States Postal Service (USPS) Application Program Interface (API)

**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

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

**l. 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.

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

(3) Retention Instructions.

Permanent. Note: Still with NARA. Pending disposition instructions are Close all completed orders annually. Destroy 10 year(s) after cut off. (DAA-0330-2017-0007-0001)

**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.

AR 40-63, SECNAVINST 6810.1, and AFI 44-121, Ophthalmic Services; and E.O. 9397 (SSN), as amended.

**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.

An OMB number is required to collect data from 10 or more members of the public in a 12-month period. SRTS does not collect data from the public.