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:

Defense Optical Fabrication Enterprise Management System (DOFEMS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

11/06/2024

sub-component: Bureau of Medicine and Surgery (BUMED)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ 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 Defense Optical Fabrication Enterprise Management System (DOFEMS) is a Commercial Off-the-Shelf (COTS) Information Technology (IT) solution designed to provide centralized management of optical fabrication in the Military Health System (MHS). DOFEMS receives prescription work order information from the Spectacle Request Transmission System (SRTS). The transmission of work orders is initiated, controlled, and terminated in SRTS.

The Personally Identifiable Information (PII) data elements in DOFEMS are originated in and received from SRTS. PII received includes: personal information, user type (e.g. active duty, reservist, retiree, etc.), truncated Social Security Number (i.e. last four of SSN), mailing address, rank, pay grade, command information (e.g. address, unit identification code (UIC)) and spectacle prescription. DOFEMS utilizes batch work order information provided on a scheduled basis. The batch work order minimizes DOFEMS users from having to query PII. Prescription protected health information (PHI) data elements in the work order include physical geometry fabrication lens parameters such as: axis, cylinder, diameter, distance, frame type and color, horizontal prism, material, near, sphere, style, and vertical prism which are used in lens cutting, polishing, tint coating and frame selection. PHI is linked to the work order associated with the Military Health System beneficiary.

The categories of individuals with records in this system are Department of Defense (DoD) Active Duty, retirees and qualified dependents, other entitled DoD and Federal Government Beneficiaries, and qualified North Atlantic Treaty Organization (NATO) foreign nationals.

DOFEMS core components reside in data centers that implement strict physical security access controls as well as High Availability (HA) infrastructure such as redundant storage arrays and uninterruptible power supply (UPS) units. The system deploys appropriate administrative, physical and technical controls to minimize risks to PII and PHI. Access to DOFEMS is restricted to authorized DoD personnel.

DOFEMS is owned and operated by the Naval Ophthalmic Readiness Activity (NORA).

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)*

The PII is collected for verification purpose and matching purposes. The intended use of the PII received from SRTS includes verification purpose and data matching to ensure individuals receive the appropriate eye-wear prescription.

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 point of care. If individuals 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 at the point of care. If individuals do not consent to specific uses of their PII, 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

DOFEMS does not collect PII directly from individuals. DOFEMS has the appropriate Controlled Unclassified Information (CUI) applied to the system.

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 32, Third Party Liability for Hospital and Medical Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DoDI 6055.05, Occupational and Environmental Health (OEH); AR 40-63, SECNAVINST 6810.1, and AFI 44-121, Ophthalmic Services; and E.O. 9397 (SSN), as amended.

PURPOSE: Information may be collected from you to provide and document your medical care; determine your eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Military Health System (MHS) provided healthcare and recover that cost; evaluate your fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the MHS and its programs; and perform administrative tasks related to MHS operations and personnel readiness.

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 SORNs.

APPLICABLE SORNS: EDHA 07, Military Health Information System (November 18, 2013, 78 FR 69076). The SORN can be found at: https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/DHA/EDHA-07.pdf

N06150-2, Navy Health Care Records (June 16, 2003, 68 FR 35657). The SORN can be found at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570394/

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/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Defense Health Agency
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Spectacle Request Transmission System (SRTS) Project Management Office (PMO); Air Force, Army and Navy DoD Optical Fabrication Enterprise (OFE) laboratories
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Veteran's Health Administration
☐ State and Local Agencies	Specify.	

☒ 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.)*

Specify.

Optical Lab Software Solutions Inc. (OLSS) - Contract Number: N6264521P2012
The vendor's contract contains Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement clauses and the associated Code of Federal Regulations (CFR) regarding HIPAA Privacy, Security and Breach Notification Rules compliance.
Contract language: Personally Identifiable Information (PII), Protected Health Information (PHI) and Federal Information Laws: 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
Additional privacy and cybersecurity clauses:
-52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a)
-52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a)
-Risk Management Framework and Cybersecurity performance work statements are incorporated via pages 9-11
Contract References include:
-DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
-NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems of February 2010, as amended
-NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, of 30 April 2013, as amended
-DoDI 8510.01 DoD Cybersecurity, 14 March 2014
- DHA AI 77, Security Categorization and Control Selection for Information Technology of 28 May 2015
-DoDM 6025.18, Implementation of HIPAA Privacy Rule in DoD Health Care Organizations
-DoD Instruction 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs

☐ 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

Spectacle Request Transmission System (SRTS).

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

☐ E-mail
☐ In-Person 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

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 EDHA 07/N06150-2

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

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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 statue 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.

5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; AR40-63, SECNAVINST 6810.1, and AFI 44-121, Ophthalmic Services; 10 U.S.C., Ch. 55, Medical and Dental Care; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 45 CFR Part 164, Security and Privacy; Department of Defense (DoD) Instruction 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTF); 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.

Information collected from individuals of the general public (e.g., retirees and family members) is maintained within or creates a medical record, therefore OMB requirement is exempt.