PRIVACY IMPACT ASSESSMENT (PIA)

For the

Zeiss FORUM
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

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 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.

10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR 199, Civilian Health and Medical Program for the Uniformed Services (CHAMPUS); DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs) (February 23, 2015); 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.

Zeiss FORUM (FORUM) is a clinical health system utilized by the DHA National Capital Region Medical Directorate (NCR-MD) and is located at Walter Reed National Military Medical Center (WRNMMC). FORUM operates as a hub for multiple ophthalmology and optometry-specific medical modalities (i.e., stand-alone eye scanners). These modalities are independently controlled at the machine level and the resulting eye scans are populated into FORUM. After FORUM receives and analyzes these separate medical device reports, FORUM generates a summary report which can be scanned into AHLTA to complete encounters. FORUM functions as an archive server for various medical documents such as images, videos, reports and raw data. Its user interface displays patient information and related medical files stored on the FORUM server. FORUM automatically forwards patient files to an enterprise level repository, the Enterprise Clinical Imaging Archive (ECIA) to enable health care providers global visibility and access to artifacts and images generated during the health care delivery process.

Personally identifiable information (PII) and protected health information (PHI) is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in patient files in AHLTA and ECIA. Data is used for patient care management. The Composite Health Care System (CHCS) is the source system for patient validation and demographic data, which are also used to match patient records in other systems.

The personal information collected in this system are as follows. Name, Birth Date, Medical Information, Social Security Number, Other ID Number, Gender, DoD ID Number, and Defense Enrollment Eligibility Reporting System (DEERS) Prefix Number.

The information stored in this system consists of PII protected by the Privacy Act and PHI protected by the Health Insurance Portability and Accountability Act (HIPAA). The individuals whose information is stored in this system include active duty, contractors, foreign nationals, former spouses, reservist, national guard personnel, retirees, and dependents (anyone who is eligible for healthcare within the military health system).

The system does not host a website accessible by the public.

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

FORUM is susceptible to the same privacy risks inherent in any system collecting, using, and sharing PII/PHI. If this system is not properly protected then PII/PHI contained therein could be accessed by unauthorized individuals through various methods such as data interception, unauthorized access, internal threats, and external threats.

Physical, technical , and administrative safeguards are in place to ensure only authorized personnel that demonstrate "need to know" can access information contained within FORUM. In response to the risk of inaccurate information in FORUM, the system correlates information from authoritative sources only. In response to the risk presented by unauthorized disclosure of PII/PHI, DoD and the Military Health System (MHS) require all users receive information assurance, Privacy Act, and HIPAA training annually. FORUM data are encrypted in transit to protect against data interception. Unauthorized access and internal threats are mitigated by limiting the access to PII/PHI to trusted individuals only; these individuals have clearances and a "need to know" in order to access data. External threats are mitigated by following Defense Information System Agency (DISA) provided checklists as part of the FORUM accreditation process under the DoD Information Assurance Certification & Accreditation Program (DIACAP). This process ensures compliance with all necessary requirements in order to maintain the security of the FORUM system. Therefore, all applicable security and privacy processes and regulations (e.g., DIACAP, HIPAA, etc.) required of a DoD system in operation have been defined and implemented, reducing risks

a FORUM FORUM

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. NCR-MD, specifically WRNMMC and FBCH.

MTF personnel with the appropriate level of certification will be granted access as a result of a National Agency Check with Written Inquiries (NACI) or DoD-determined equivalent investigation and personnel on a need to know basis.

☒ **Other DoD Components.**

Specify. To other health care providers utilizing AHLTA and ECIA for the purpose of providing medical care.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Contract with Carl Zeiss SBE, LLC acknowledges it is a Business Associate in accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003. Therefore, a Business Associate Agreement (BAA) is required to comply with HIPAA Privacy and Security regulations. The Contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as required by DoD 6025.18-R and DoDI 8580.02, as amended.

Furthermore, the BAA states: "The Contractor agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the

☐ **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. If an individual chooses not to provide PII/PHI, no penalty may be imposed, but absence of the requested information may result in administrative delays.

(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.

Consent to the specific uses of PII is is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3. 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 restrict the use of their PHI based on the procedures in place at the local facility where the data are collected and maintained, in accordance with DoD 6025.18-R, C10.1. For uses other than treatment, payment and healthcare operations, individuals can authorize the use of their PHI by submitting DD Form 2870. For uses other than treatment, payment and healthcare operations, individuals can request restrictions on the use of the PHI by submitting DD Form 2871.

(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.

1.AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN): 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); and E.O. 9397 (SSN), as amended.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED: Information may be collected from you to provide and document your medical care; determine eligibility for

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.

3. ROUTINE USES: Information in your records may be disclosed to:
-Private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security (with regard to members of the Coast Guard), in connection with your medical care;
-Government agencies to determine your eligibility for benefits and entitlements;
-Government and nongovernment third parties to recover the cost of MHS provided care;
-Public health authorities to document and review occupational and environmental exposure data; and
-Government and nongovernment organizations to perform DoD-approved research.

   Information in your records may be used for other lawful reasons which may include teaching, compiling statistical data, and evaluating the care rendered. Use and disclosure of your records outside of DoD may also occur in accordance with 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, which incorporates the DoD Blanket Routine Uses published at: http://dpcld.defense.gov/privacy/SORNsIndex/BlanketRoutineUses.aspx.

   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 by DoD 6025.18-R. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION: Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

   This all inclusive Privacy Act Statement will apply to all requests for personal information made by MHS health care treatment personnel or for medical/dental treatment purposes and is intended to become a permanent part of your health care record.

   Your signature merely acknowledges that you have been advised of the foregoing. If requested, a copy of this form will be furnished to you.

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.