PRIVACY IMPACT ASSESSMENT (PIA)

For the

KARL STORZ Integrated Operating Room System with LiveData
Defense Health Agency

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.

5 U.S.C. 301, Departmental regulations; 10 U.S.C. Chapter 55, Medical and Dental Care; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); DODI 6015.23, Delivery of Healthcare at Military Treatment Facilities: Foreign Service Care; Third-Party Collection; Beneficiary Counseling and Assistance Coordinators (BCACs); 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.

KARL STORZ integrated Operating Room (KS i-OR) is an OR system that offers centralized control of the entire OR to improve patient safety and operational efficiency to better manage endoscopic and peripheral devices and to view, display, document and communicate information from video and other data sources such as AGFA PACS, AHLTA, CHCS, Essentris and S3. Patient records are accessed and are updated during the OR procedures. Personally identifiable information (PII) and protected health information (PHI) are collected using the other data sources such as AGFA PACS, AHLTA, CHCS, Essentris and S3 to determine eligibility and administer health care delivery services. User data, which contains some PII and PHI, is collected to support administration and clinical practice authorization and access. Clinical patient data is documented and stored in the patient files in the original data sources such as AGFA PACS, AHLTA, CHCS, Essentris and S3 and are not managed or stored permanently in the i-OR system. Data is strictly used for patient care management.

The personal information collected from the other data sources such as AGFA PACS, AHLTA, CHCS, Essentris and S3 and is used by KS i-OR system is as follows:

Name
Social security number (SSN)
Gender
Birth date
Medical information

The individuals whose information that is being used in this system include active duty military (all services + Coast Guard and Reserve), veterans, dependents, retirees and/or their dependents, active-duty, contractors, foreign nationals, former spouses, reservist, national guard personnel, and prisoners of war.

The system does not host a Web site accessible by the public.

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

All PII is contained on secured ISs located in a secured MTF site. KS i-OR data is 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 clearance and a "need to know" in order to access data. User and system authentication is addressed by verifying need to know and clearance. There are defined user and administrator roles that provide access to the KS i-OR solution via CAC authentication. This allows for thorough control and auditing of solution access.

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 to the maximum extent possible and to the point that any remaining risk has been accepted by the KS i-OR Designated Approving Authority (DAA).

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. DoD Medical Treatment Facility (MTF)

☐ **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. Data Exchange occurs between Karl Stortz i-OR and individual Service readiness applications, contractor systems providing system maintenance and help desk support.

☐ **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.

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

KS i-OR is not the initial point of collection of PII from individuals; therefore, individuals do not have the opportunity to object to the collection of their PII.

KS i-OR receives data from AGFA PACS, AHLTA, CHCS, Essentris, and S3, all of which collect PII directly from individuals and provide individuals the opportunity to object at the point of collection.

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.

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

KS i-OR is not the initial point of collection of PII from individuals; therefore, individuals do not have the opportunity to consent to the collection of their PII.

KS i-OR receives data from AGFA PACS, AHLTA, CHCS, Essentris, and S3, all of which collect PII directly from individuals and provide individuals the opportunity to consent at the point of collection.

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.

KS i-OR is not the initial point of collection of PII; therefore no Privacy Act Statement is required. This statement is given only at the initial point of collection.

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.