PRIVACY IMPACT ASSESSMENT (PIA)

For the

Full Field Digital Mammography System (FFDM)
US Army Medical Command - DHP Funded Medical Device

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 A0040-66b DASG

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. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

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.

The purpose of the FFDM system is to acquire digital breast images to screen for and diagnose early stages of breast disease. The system will acquire patient information from the hospital information system (Composite Healthcare System / Armed Forces Health Longitudinal Technology Application - CHCS/AHLTA) and associate it with the acquired images.

The Mammography Quality Standards Act (MQSA) requires, as a minimum, that the following information be displayed with the image: name, address, and zip code of facility, first and last name of patient, gender, date of birth, a unique patient identification number, and medical information specific to the system. Military facilities use a combination of a family member prefix (FMP) and the sponsor's social security number to construct the unique patient ID.

This updates the FFDM PIA approved on 3 June 2011.

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

Risks for this system are similar to any other system which requires human data entry or are electronically accessible. These can include inaccurate information entry, unauthorized access, inadvertent data viewing. In addition, there is also a risk that the collected PII would be accessed by unauthorized persons.

Risk is mitigated by strict adherence to security and privacy protocols. The Army takes a "defense in depth" approach to protecting this information. Physical safeguards (e.g., data stored on accredited servers in the Pentagon), technical safeguards (e.g., encryption; common access card, password protection) and procedural safeguards (e.g., physical access to data based on duty position) are employed in series to ensure only those personnel that demonstrate "need to know" can access information contained within the system. The FFDM system is installed in a restricted access area of the radiology department. UserID and password are required in order to log in and gain access to the FFDM application. The user logs off of the FFDM application during hours that the mammography clinic is closed. In response to the risk presented by including inaccurate information in the system, FFDM system correlates information from authoritative sources only. Data is only viewed by authorized users and medical personnel that require access to the information in the performance of their duties. In response to the risk presented by unauthorized disclosure of information contained, administrative procedures require that users receive information assurance awareness, HIPAA and system training in order to mitigate risks involved. This multi-faceted approach to safeguarding PII provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

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. The PII will be shared with health care providers within all US Army medical treatment facilities (MTF).

☒ **Other DoD Components.**

Specify. The PII may be shared with health care providers within Navy and Air Force MTFs.

☒ **Other Federal Agencies.**

Specify. The data may be shared with required and authorized health care providers within other Federal Agencies supporting Army and/or DoD beneficiaries (U.S. Coast Guard, Veterans Administration, Public Health Service, Center for Disease Control).

☒ **State and Local Agencies.**

Specify. Information is provided to State and Local agencies as required by law and DoD guidelines.

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

Specify. The Manufacturer servicing the device may have access to some data. Contracts for Manufacturers supporting this device include a standard Military Health System (MHS) HIPAA Business Associate Agreement, DoD/HIPAA guidelines and Army MEDCOM Information Assurance (IA) guidelines.

The data may be shared with commercial providers under contract with DoD to provide specific health care related patient support. There are clauses in their contracts to protect PII IAW Privacy Act and HIPAA standards.

☐ **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.

Individuals read and sign DD Form 2005, Privacy Act Statement - Health Care Records. A copy of this document is maintained in the medical record. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED.

(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.

Individuals read and sign DD Form 2005, Privacy Act Statement - Health Care Records. A copy of this document is maintained in the medical record. If the individual withholds their consent to specific uses of their PII, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED.

(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.

PRIVACY ACT STATEMENT – HEALTH CARE RECORDS

1. AUTHORITY FOR COLLECTION OF INFORMATION INCLUDING SOCIAL SECURITY NUMBER (SSN)
Sections 133, 1071-87, 3012, 5031 and 8012, title 10, United States Code and Executive Order 9397.

2. PRINCIPAL PURPOSES FOR WHICH INFORMATION IS INTENDED TO BE USED INFORMATION
This form provides you the advice required by The Privacy Act of 1974. The personal information will facilitate and document your health care. The Social Security Number (SSN) of member or sponsor is required to identify and retrieve health care records.

3. ROUTINE USES
The primary use of this information is to provide, plan and coordinate health care. As prior to enactment of the Privacy Act, other possible uses are to: Aid in preventive health and communicable disease control programs and report medical conditions required by law to federal, state and local agencies; compile statistical data; conduct research; teach; determine suitability of persons for service or assignments; adjudicate claims and determine benefits; other lawful purposes, including law enforcement and litigation; conduct authorized investigations; evaluate care rendered; determine professional certification and hospital accreditation; provide physical qualifications of patients to agencies of federal, state, or local government upon request in the pursuit of their official duties.

4. WHETHER DISCLOSURE IS MANDATORY OR VOLUNTARY AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION
In the case of military personnel, the requested information is mandatory because of the need to document all active duty medical incidents in view of future rights and benefits. In the case of all other

personnel/beneficiaries, the requested information is voluntary. If the requested information is not furnished, comprehensive health care may not be possible, but CARE WILL NOT BE DENIED.

This all inclusive Privacy Act Statement will apply to all requests for personal information made by health care treatment personnel or for medical/dental treatment purposes and will 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.