PRIVACY IMPACT ASSESSMENT (PIA)

For the

Picture Archive and Communication System (PACS)
Department of the Navy - TMA DHP Funded System - BUMED

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	DoD Registration ID 55, DHP SIRT ID 70
☐	**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 N06150-2

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.

System of Record Authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 1095, Health Care Services Incurred on Behalf of Covered Beneficiaries Collection from Third Party Payers Act;
10 U.S.C. 5131 (as amended), Bureaus: name; location
10 U.S.C. 5132, Bureaus: distribution of business, orders, records, expenses
44 U.S.C. 3101, Records Management by Agency Heads
10 U.S.C. 55 Medical and Dental Care;
42 CFR 290DD Drug and Alcohol Treatment Records;
5 CFR 293.502, Subpart E, Employee Medical File System Records;
29 CFR Part 5, Labor Standards;
5 CFR 339.101-306, Coverage;
DoDD 6485.1 Human Immunodeficiency Virus-1 (HIV-1);
DoD 6025.18-R, Health Information Privacy Regulation
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 Social Security Number (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.

PACS is a commercial off the shelf medical system that collects digital radiological medical images (x-rays, CT, MRI, etc...) for the purpose of display, review and storage. The system is a diagnostic tool for Radiologist interpretation of medical images. PACS collects medical images from various medical modalities such as ultrasound systems, CT scanners, MRI scanners, etc., and patient demographic information from the Composite Health Care System (CHCS). PACS allows medical images to be easily shared across the health care enterprise by storing digital images in a central archive. The PACS system may have clinical area specific applications e.g. Cardiology and Radiology.

DoD purchases PACS' from a Defense Logistics Agency contract titled "DIN-PACS". At present, there are 8 vendors on that contract to include, but not limited to include McKesson, Agfa, Fuji and Carestream. The vendor product is selected based on best value. These products have the same functionality and must meet very specific functional requirements to be on the contract. The PACS functionality varies at each Military Treatment Facility (MTF) based on their clinical capabilities.

Personally identifiable information (PII) collected about individuals include: Patient name, birth date, gender, Patient ID number and medical information: diagnostic images: X-rays, CT scans, MRI scans, Ultrasounds, Mammograms, Nuclear Medicine images, Radiation Oncology images, Angiogram and other Interventional Radiography images.

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

The biggest privacy risk is by user misuse of the system, e. g. not logging off, not "stripping" the PII from images stored in training files, etc. The administrative, technical and physical controls detailed in this PIA are in place because of this possibility to include: periodic security audits, regular monitoring of users' security practices, and annual training for personnel. Additionally contractors have a business associate agreement clause in their contract that details their roles and responsibilities in accordance with the HIPAA Privacy Rule.

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. Diagnostic images are shared throughout the healthcare enterprise for the purpose of diagnosing and treating patients.

☒ **Other DoD Components.**

Specify. Diagnostic Images are shared with Army and Air Force Medical Treatment Facilities worldwide.

☒ **Other Federal Agencies.**

Specify. Diagnostic images are transferred to the VA health system upon a member's separation from Active Duty.

☐ **State and Local Agencies.**

Specify.

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

Specify. There are 8 vendors PACS products that may in use by Navy Medicine to include but not limited to McKesson, Agfa, Fuji and Carestream.

The vendors' contracts contain a business associate agreement clause as well as the standard FAR privacy clauses.

☐ **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.

PACS does not collect PII directly from individuals; it is not the source system.

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.

PACS does not collect PII directly from individuals; it is not the source system.

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.

PACS does not collect PII directly from the patient - it is not the source system.

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☐ Race/Ethnicity	☒ Birth Date	☐ Place of Birth
☐ Personal Cell Telephone Number	☐ Home Telephone Number	☐ Personal Email Address
☐ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☒ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☐ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.

Other ID Number: Patient ID Number

Medical information: diagnostic images: X-rays, CT scans, MRI scans, Ultrasounds, Mammograms, Nuclear Medicine images, Radiation Oncology images, Angiogram and other Interventional Radiography images.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

Existing DoD information system - Composite Health Care System (CHCS)

(3) How will the information be collected? Indicate all that apply.

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☐	**Email**	☐	**Web Site**
☒	**Information Sharing - System to System**		
☐	**Other**		

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Verification. The PII is used to identify medical images pertinent to a particular imaging study in order to ensure results are entered into the correct patient record.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Mission-related (medical care). The information is used to identify diagnostic imaging studies as part of the patient record.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in this DoD information system or electronic collection? Indicate all that apply.

☒ Users ☐ Developers ☒ System Administrators ☒ Contractors

☐ Other

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☐	Security Guards	☒	Cipher Locks
☒	Identification Badges	☐	Combination Locks
☒	Key Cards	☐	Closed Circuit TV (CCTV)
☐	Safes	☐	Other

(2) Technical Controls. Indicate all that apply.

☒	User Identification	☐	Biometrics
☒	Password	☒	Firewall
☒	Intrusion Detection System (IDS)	☒	Virtual Private Network (VPN)
☒	Encryption	☒	DoD Public Key Infrastructure Certificates
☐	External Certificate Authority (CA) Certificate	☒	Common Access Card (CAC)
☐	Other		

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☐ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☒ **Yes. Indicate the certification and accreditation status:**

☐	**Authorization to Operate (ATO)**	**Date Granted:**	pending - each vendor's PACs products may be
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection: PACS obtains the PII from CHCS through a secured transmission and the name of the patient is associated with the digital radiological medical images.
Use, Retention, and Processing: Only personnel with the "need to know" can access a member's PII information.
Disclosure: No other personnel other than those with a "need to know" can access a member's PII information unless permission is granted from the individual in writing to release the information.
Destruction: Data is destroyed in accordance with the Navy's Records Management Manual.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

The perceived threats are primarily from computer hackers, disgruntled employees, and acts of nature (e.g. fire, flood, etc.)

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that PACS, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

All systems are vulnerable to "insider threats". PACS Managers/System Administrators are vigilant to this threat by limiting system access to those individuals who have a specific need to access the information. There are defined criteria to identify who should have access to the PACS. These individuals have met the personnel security requirements in accordance with SECNAV M-5510.30.

The following controls are used to mitigate the risks:

a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.
b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.
c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.
d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.
e) Training. Personnel are required to complete annual training (Cyber Awareness, Privacy Act and HIPAA) to keep users alert to the security requirements.
f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. The PACS servers and workstations are physically located in locked spaces and outside of high traffic areas per HIPAA privacy requirements.

Servers are located at MTF.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	DOORN.EDWIN.ALLEN.1021385200 Digitally signed by DOORN.EDWIN.ALLEN.1021385200 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=DOORN.EDWIN.ALLEN.1021385200 Date: 2014.04.22 07:39:21 -04'00'
Name:	Edwin A. Doorn
Title:	PACS Program Manager
Organization:	Naval Medical Logistics Command
Work Telephone Number:	301-619-8055
DSN:	343-8055
Email Address:	edwin.doorn@med.navy.mil
Date of Review:	22 Apr 2014
Other Official Signature (to be used at Component discretion)	KEMPER.MICHAEL.J.1069046025 Digitally signed by KEMPER.MICHAEL.J.1069046025 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=KEMPER.MICHAEL.J.1069046025 Date: 2014.04.24 15:28:50 -04'00'
Name:	CDR Michael J. Kemper
Title:	Director, Medical Equipment and Logistics Solutions (Code 03)
Organization:	Naval Medical Logistics Command
Work Telephone Number:	301-619-3384
DSN:	343-3384
Email Address:	michael.kemper@med.navy.mil
Date of Review:	22 Apr 2014

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	THORNTON.CAYETANO.SEELOS.1164922142 Digitally signed by THORNTON.CAYETANO.SEELOS.1164922142 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=THORNTON.CAYETANO.SEELOS.1164922142 Date: 2014.06.13 17:04:28 -04'00'
Name:	CDR Cayetano S. Thornton
Title:	Deputy Chief IM/IT and Chief Information Officer
Organization:	Bureau of Medicine and Surgery
Work Telephone Number:	202-762-3180
DSN:	
Email Address:	cayetano.thornton@med.navy.mil
Date of Review:	Endorsement for Approval
Component Privacy Officer Signature	PATTERSON.ROBIN.W.1229323403 Digitally signed by PATTERSON.ROBIN.W.1229323403 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=PATTERSON.ROBIN.W.1229323403 Date: 2014.09.09 19:06:44 -04'00'
Name:	Robin Patterson
Title:	Head, Department of the Navy FOIA/Privacy Act Program Office (DNS-36)
Organization:	Office of the Chief of Naval Operations
Work Telephone Number:	202-685-6545
DSN:	
Email Address:	robin.patterson@navy.mil
Date of Review:	

Component CIO Signature (Reviewing Official)	MUCK.STEVEN.ROBERT.1179488597 Digitally signed by MUCK.STEVEN.ROBERT.1179488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597 Date: 2014.09.10 12:39:24 -04'00'
Name:	For Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer
Work Telephone Number:	703-601-0116
DSN:	
Email Address:	barbara.hoffman@navy.mil
Date of Review:	10 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.