

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:

Public Health Command - Europe (PHCE)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

10/30/23

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.

Public Health Command Europe (PHCE) is a Brigade size component supporting over 54,000 overseas personnel in the Kaiserslautern Community area with services such as Veterinary services for family pets and military working dogs, a multitude of laboratory services to ensure community health, occupational health services, industrial hygienist, and services and many other Public Health Services. The PHCE Enclave consists of End User-Devices (EUDs), switches, appliances, and the data center. PHCE provides the data center all environmental controls such as light, power, heating, ventilation, air conditioning, and physical security. Co-located and managed co-located systems within the data center, include systems and applications that contain Personally Identifiable Information (PII) data. Data Network Connectivity (DNC), Enterprise Management System (EMS), and the Network Protection Suite are services controlled and managed by DHA and are not included in the authorization boundary.

The PII collected contains information about local nationals under General Data Protection Regulation (GDPR), active duty, civilians, and government contractors. PII may include numerous types of PII including citizenship, employment information, home/cell phone, mailing/home address, military records, official duty address, passport information, place of birth, race/ethnicity, records, work/personal email address, birth date, education information, marital status, official duty phone, position/title, rank/grade, security information, child information, DoD ID number, emergency contact, and Protected Health Information (PHI). Commercial-Off-The-Shelf (COTS) applications such as Microsoft Word Excel, PowerPoint, and Outlook are utilized to provide administrative support to the enclave and may process PII.

PII processed on some system components, applications, and documents might utilize specific administrative, physical, and technical security controls to protect PII confidentiality and which may be addressed in separate Privacy Impact Assessments (PIA)s. Such PIAs are available at: <https://dodcio.defense.gov/In-the-News/Privacy-Impact-Assessments.aspx/>.

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 purpose and the intended use of collected PII is specific to a system component and is addressed in the sub-system's PIA.

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.

The MedCOI system does not present any applications for which a user would be required to enter PII. The ability for a user to object to the collection of PII would be presented by the DHA application the user is interacting with. Once a user has agreed to enter PII into the DHA application, then that data becomes subject to the inspection/monitoring functions performed by MedCOI that are not optional. Use of government/DoD Information systems constitutes notice that all communications are subject to inspection.

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.

The MedCOI system does not present any applications for which a user would be required to enter PII. The ability for a user to consent to the specific uses of their PII would be presented by the DHA application the user is interacting with. Once a user has agreed to enter PII into the DHA application, then that data becomes subject to the inspection/monitoring functions performed by MedCOI that are not optional. Use of government/DoD Information systems constitutes notice that all communications are subject to inspection.

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

The MedCOI system does not present any applications for which a user would be required to enter PII. A Privacy Act Statement and/or a Privacy Advisory would be presented by the DHA application the user is interacting with when applicable.

System does not collect PII/PHI directly from individuals. Therefore, no Privacy Act Statement or Advisory is required.

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. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

☐ Other DoD Components (i.e. Army, Navy, Air Force)

Specify. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

☐ Other Federal Agencies (i.e. Veteran's Affairs, Energy, State)

Specify. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

☐ State and Local Agencies

Specify. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

☐ 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. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

☐ Other (e.g., commercial providers, colleges).

Specify. Not applicable for a LAN. The sharing of PII is addressed in the information system's PIA.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

☐ Individuals

☐ Databases

☐ Existing DoD Information Systems

☐ Commercial Systems

☐ Other Federal Information Systems

Not applicable for the MTF MedCOI enclave; the information collection method is specific to the information system component and is addressed in the sub-system's PIA.

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

☐ E-mail

☐ Official Form (Enter Form Number(s) in the box below)

☐ In-Person Contact

☐ Paper

☐ Fax

☐ Telephone Interview

☐ Information Sharing - System to System

☐ Website/E-Form

☐ Other (If Other, enter the information in the box below)

Not applicable for the MTF MedCOI enclave; the information collection method is specific to the information system component and is addressed in the sub-system's PIA.

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

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

The PHCE MedCOI enclave is not a system of records; however, system components, applications, and electronic collections within the enclave might require a SORN. Refer to the specific system component, application, or electronic collection PIA for SORN information

I. 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.

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

(3) Retention Instructions.

The LAN/Enclave itself does not have a NARA approved, pending, or GRS authority and retention instructions applied as a whole. Refer to NARA approved, pending, or GRS authority and retention instruction specific to the systems, applications, electronic collections, file servers, and share drives contained within the LAN/Enclave.

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 statute 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.

Authorities to collect information are specific to the information system component and addressed in the respective sub-system's PIA

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.

The information collected in this system is for the diagnosis and treatment of medical disorders and does not collect PHI/PII directly from individuals. It is not the initial point of collection for any PHI/PII and is not considered a public information collection IAW DoDM 8910.01, V2, Encl 3, paragraph 8b(5).