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:

ICU Medical MedNet System_V6_AA Enterprise PIA

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/05/24

CyberLOG

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
- [x] 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
- [x] 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.

The ICU MedNet is a server-based safety software product intended for use in healthcare facilities by trained healthcare professionals to provide valuable bedside guidance by managing infusion information with compatible ICU Medical infusion systems. ICU Medical MedNet™ Integrated System consist of the ICU Medical MedNet software, ICU Medical MedNet Meds, the LifeCare patient-controlled analgesia (PCA) infuser, and the Plum 360 infuser. The ICU Medical MedNet™ suite of software also includes a separate application which is ICU Medical MedNet™ Meds™. The LifeCare patient-controlled analgesia (PCA) infuser allows patients to self-administer analgesics with defined parameters using a push-button pendant attached to the device. The Plum 360 infuser is a larger volume infuser capable of delivering fluids for a variety of therapies such as parenteral, enteral, or epidural infusions. This system is network and wireless capable. ICU Medical MedNet System does process Personal Identifiable Information (PII)/Protected Health Information (PHI) when interfaced with Cerner and Military Health Services (MHS) Genesis.

The ICU Medical MedNet Integrated System consist of the following hardware: DHA provided server with Windows Server 2019, Microsoft SQL 2019, DHA provided Windows 10 client workstation, a LifeCare PCA infuser, and a Plum 360 infuser. The software consist of DHA virtualized imaged Windows Server 2019, Microsoft SQL 2019 Database, ICU Medical MedNet, and ICU MedNet Meds. The LifeCare PCA and the Plum 360 use a propriety kernels. This server and workstation can be scanned, patched, and placed under Configuration Control. The LifeCare PCA and Plum 360 can only be scanned or patched by a licensed ICU Medical personnel. The local Military Treatment Facility (MTF)/clinic sites are responsible for day-to-day operations, maintenance, and management of the ICU Medical MedNet System_V6_AA Enterprise PIA.

PII collected includes military records and PHI. The categories of people in which PII is collected includes: All Active Duty Service Members, Retirees, Veterans, and their families. In addition, PII is collected from both members of the general public and Federal. The baseline site is Madigan Army Medical Center in Joint Base Lewis-McChord, Washington. This system is deployed to Ft. Sill, Oklahoma and Ft. Hood, Texas. This system is owned by Defense Health Agency's Cyber Logistics and operated by deployed Military Treatment Facility (MTF).

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 PII collected is to match patient with the medical device. The intended use of this PII is to enhance patient care.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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.

Individuals do not have the opportunity to object to the collection of their PII because ICU Medical MedNet™ System is not the initial point of collection.

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.

Individuals do not have the opportunity to consent to the specific uses of their PII because ICU Medical MedNet™ System is not the initial point of collection.

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

ICU Medical MedNet System does not collect PII directly from individuals, therefore; no Privacy Act Statement or Privacy 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.	Defense Heath Agency's Military Treatment Facilities
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	
☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	
☐ State and Local Agencies	Specify.	
☒ 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.	The military treatment facilities (MTF) may utilize contractor services to support this product. DoD's policy requires such contracts include language to safeguard PII including FAR clauses: 52.224-1, Privacy Act Notification; 52.224-2, Privacy Act; and FAR 39.105, Privacy. When the contractor has access to PHI, a HIPAA Business Associate Agreement is also required.
☐ Other *(e.g., commercial providers, colleges)*.	Specify.	

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

Existing DoD Information Systems:

Cerner
Military Health Service (MHS) Genesis

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)*

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://dpcld.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.

l. 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. GRS 5.2, item 020 (DAA-GRS-2017-0003-0002)

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

(3) Retention Instructions.

FILE NUMBER: 103-14
DISPOSITION: Temporary. Delete no more than 7 years from the date last modified. (See DoD DTM 22-001 on default disposition policies and OSD Records Manager guidance which file number to associate).

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 statue 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.

5 U.S.C. 301, Department Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C., Chapter 55, Medical and Dental Care; DoD Instruction 6430.02, Defense Medical Logistics Program; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 45 CFR 164, Security and Privacy; DoD Manual 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs.

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.

This system does not require OMB approval since it does not collect information directly from members of the public and the information collected is for the diagnosis and treatment of medical disorders and is not considered a public information collection in accordance with DoDM 8910.01, V2, Encl 3 8b(5).