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:

MED365

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

07/15/2025

Program Executive Office (PEO) Medical Systems (J6)

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.

DHA's MED365 tenant is an office automation and collaboration capability for authorized Department of Defense (DoD) Common Access Card (CAC) or Personal Identity Verification (PIV) users to fulfill content management, document creation and management, account creation and management, file management, enterprise class search, and collaboration space(s) needs. MED365 delivers multiple capabilities to meet the diverse Defense Health Agency (DHA) mission needs across DHA sub-components and Military Treatment Facilities (MTFs); its applications cover Information Technology Infrastructure Library (ITIL) & Development, Security and Operations (DevSecOps) processes and are natively integrated in a single platform providing cloud intuitiveness and process automation. To satisfy DoD-specific requirements, the MED365 tenant implements configurations in accordance with the DoD Cross-Tenant Collaboration, Tenant Configuration Guide (TCG) to provide the following core services: Identity Access, Teams, Exchange Online, and SharePoint Online\OneDrive for Business.

Personally Identifiable Information (PII) collected includes: demographic and employment information, users are provided the opportunity to collect and/or store PII in performance of their official duties. Categories of individuals from which PII is collected includes Active Duty Service Members, Federal employees, and Federal contractors.

MED365 is managed by DHA's PEO Medical Systems/CIO (J-6).

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)*

PII is provided to MED365 for authentication, mission-related, and administrative purposes. The intended use of the collected PII is to establish an individual's MED365 account, engage in content management, document creation and management, file management, and utilize collaboration spaces.

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.

MED365 does not serve as the initial point of collection for any PII and/or PHI introduced to the environment by its individual users.

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.

MED365 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

MED365 does not solicit information 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 Health Agency (DHA) sub-components and Military Treatment Facilities (MTFs)
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Army, Navy, and Air Force
☐ 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.	Microsoft is contracted to provide software support and sustainment services and therefore has full access to MED365. Contractual language that safeguards PII and/or PHI includes: "The Contractor shall comply with DoD Directive 8500.1, "Information Assurance (IA)," DoD Instruction 8500.2, "Information Assurance (IA) Implementation," DoD Directive 5400.11, "DoD Privacy Program," DoD Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs" dated March 13, 2019, and DoD 5200.2-R, "Personnel Security Program Requirements."
☐ 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: milConnect (Defense Manpower Data Center (DMDC)); enterprise records feeding from the enterprise user directory (Global Federated User Domain (GFUD))

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)*

E-mail; Website/E-Form; Other: As part of its collaboration and content management offerings, MED365 users are provided the opportunity to collect and/or store PII and/or PHI within the MED365 environment in performance of their official duties.

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.

MED365 does not retrieve records on U.S. citizens or lawful U.S. residents by name or other unique identifier.

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 6.1, item 010 (DAA-GRS-2022-0006-0001)
GRS 6.1, item 011 (DAA-GRS-2022-0006-0002)
GRS 5.2, item 020 (DAA-GRS-2022-0009-0002)
GRS 5.1, Item 020 (DAA-GRS-2016-0016-0002)

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

(3) Retention Instructions.

Email: Future (All Non-Capstone Users) - In addition to the 180-day Purge for Deleted items, emails older than 10 years will be automatically deleted. Members of the DISA organization will have mail deleted after 7 years./Future (Capstone/HLO) - 26-Year Retain Adaptive Scopes Retention Policy. Email is held for 26 years after the sent/received date. If an email is 10 years old, it will be retained for 16 more years. (All email is retained, even deleted) with Auto Expanding archives.

Teams 1-1 Chat: Future (All Non-Capstone Users) - Deleted items will purge at 180 days after the item is moved to the deleted items or a soon after as technically practicable/Future (Capstone/HLO) - 26 years(All chats stored in Exchange, even deleted chats)

Teams Group Chat: Future (All Non-Capstone Users) - Delete after 7 years (If user does not delete - True Culling allowed)/Future (Capstone/HLO) - 26 Years (All email retained, even deleted)

Microsoft Groups: Delete after 7 years(If user does not delete - True Culling allowed)

Teams Recordings (Channel): No Default Retention (Subject to 180-day Team inactivity expiration)

Teams Recordings (Non-Channel): Delete after 7 years(If user does not delete - True Culling allowed)
Teams Chat Files: Delete after 7 years(If user does not delete - True Culling allowed)

Teams Channel Files: Delete after 7 years(If user does not delete - True Culling Allowed) (Subject to 180-day Team inactivity expiration) (Back end SPO site can be configured according to organizational prepopulated Record Disposition Schedules [RDS])

OneDrive: Delete after 7 years (If user does not delete - True Culling allowed)

SharePoint Online (SPO) Files: No Default Retention. Site owners configure according organizational prepopulated RDS

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 USC 301, Departmental Regulations; 10 USC 142, Chief Information Officer; 40 USC 11315, Agency Chief Information Officer; 44 USC 3506, Federal Agency Responsibilities; 44 USC § 3554, Federal Agency Responsibilities; Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 10 USC, Ch. 55, Medical and Dental Care; 10 USC 1073c, Administration of Defense Health Agency and

Military Medical Treatment Facilities; and 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.

MED365 is exempt from Paperwork Reduction Act (PRA) requirements per DoDM 8910.01, Volume 2, Enclosure 3, Section 8(b11): "Collections of information from DoD civilian employees within the scope of their employment (includes all the tasks performed to accomplish the job they perform for the Office of the Secretary of Defense (OSD) or DoD Component), unless the results are to be used for general statistical purposes."