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:

Defense Health Agency Texting Solution (DHATS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

04/05/24

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.)*

- [x] 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.

Defense Health Agency Texting Solution (DHATS) is a cloud-based application designed to enhance communication within the Defense Health Agency (DHA) by enabling text message transmission to various recipients. This aligns with the broader goal of improving efficiency and responsiveness in the agency's communications. Hosted on the Defense Health Agency (DHA) Amazon Web Services (AWS) GovCloud, DHATS utilizes Application Programming Interface (API) requests to facilitate messaging. External users will not have access to DHATS, with an exclusion for a subscription preferences page; they are limited to receiving Short Message Service (SMS) messages and can transmit a predefined response to opt out of the service. Internal users, comprised of DoD personnel and contractors, will authenticate using Department of Defense Public Key Infrastructure (DoD PKI).

DHATS's internal users can register new system interconnections, review sent messages, update interconnecting system information, and manually review messages flagged for potential inclusion of Personal Identifiable Information (PII) or Protected Health Information (PHI).

DHATS processes and stores the following PII elements: First Name, Last Name, Home/Work Email, Home/Work Phone Number, and PHI. These details of internal users are required to ensure adequate user activity auditing. Phone numbers and potentially first and last names of recipients are used in message templates.

DHATS is engineered to block the transmission of PII or PHI, employing Artificial Intelligence (AI) and Machine Learning (ML) to review each message to ensure that the contents do not include PII or PHI. Any unverified statements are manually investigated, logged, and utilized to train the AI model for future accuracy.

Although the system does not intentionally transmit PHI, it may inadvertently receive PHI from an interconnecting system. All information, including inadvertent PHI, is encrypted in transit and at rest to ensure confidentiality, aligning with relevant regulatory and compliance frameworks. Any accidental submission of sensitive information, such as PHI, is handled with utmost care and in accordance with established protocols, ensuring the integrity and security of the data.

DHATS demonstrates a strong commitment to privacy and security by leveraging cutting-edge technology and adhering to stringent guidelines, fulfilling its core mission of efficient and secure communication within the DHA.

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 personal identifiable information (PII) collected by DHATS, such as the last name, first name, email, and phone number, is primarily used to identify, authenticate, and communicate with users.

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.

DHATS uses information, including PII, provided by the interconnecting systems. The objection to the collection of PII must occur with the interconnecting system, not with DHATS. DHATS cannot prevent the collection of PII of external users by the systems that use DHATS however, DHATS does provide external users with the ability to opt out of receiving its communication.

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.

For DHATS to transmit the initial message, it must utilize the phone number, which is considered PII, of the recipients. DHATS cannot allow external users to consent to the specific use of their PII until after the original line of communication is open. Once the line of communication is available, the user can opt out of communications from DHATS.

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

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.	Defense Health Agency (DHA)
☐ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	U.S. Air Force, Navy, Army, Marine Corps, Coast Guard, and National Guard
☐ 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.	
☐ 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

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 6.1-0330-2022-0006-0002, GRS 6.1-0330-2022-0006-0001

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

(3) Retention Instructions.

As Applicable:

FILE NUMBER: 102-12.1
DISPOSITION: Temporary. Cut off annually upon receipt. Destroy 7 years after cutoff.
NOTE: Non-Capstone Employees must ensure that all email records with dispositions of longer than 7 years be retained external to their email systems.

FILE NUMBER: 212-10
DISPOSITION: Permanent. Cut off annually. Transfer to NARA 25 years after cutoff.

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.

Per DoD 6025.18-R, DoD Health Information Privacy Regulation, paragraph 4.1.b "A DoD covered entity may: (1) Use or disclose PHI for its own treatment, payment, or health care operations. (2) Disclose PHI for treatment activities of a health care provider.". Additional authority is granted per "5 U.S. Code § 552a - Records maintained on individuals".

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).