PRIVACY IMPACT ASSESSMENT (PIA)

For the

Fraud and Abuse Correspondence Tracking System (FACTS)
Defense Health Agency (DHA)

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

☐ **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

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.

10 U.S.C. Chapter 55, Medical and Dental Care; 31 U.S.C. 3512, Executive agency accounting and other financial management reports and plans; 32 CFR Part 199, Civilian Health and Medical Program of the Uniformed Services; DoDI 5505.12, Anti-Fraud Program at Military Treatment Facilities (MTFs); E.O. 9397, as amended (SSN).

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.

The DHA Program Integrity (PI) office is the centralized administrative hub for anti-fraud and abuse activities worldwide and will be utilizing the information stored in the FACTS, an electronic collection system, to support this mission. DHA PI is responsible for collecting Personally Identifiable Information (PII)/Personal Health Information(PHI) data, developing policies and procedures regarding prevention, detection, investigation of medical/dental/mental health providers, beneficiaries and others individuals and entities in anti-fraud efforts to control TRICARE fraud, waste and program abuse. Additionally, the PI office monitors contractor program integrity activities, coordination with Department of Defense (DoD) and external investigative agencies and initiating administrative remedies as required. Such collection, investigation, monitoring, and coordination requires both PII and PHI to safeguard the DHA, its provided benefits, and beneficiaries.

The workflow process begins when an allegation of fraud, abuse or waste is reported via sources outside of FACTS. Next, allegations are developed, a case is opened, forwarded to law enforcement for investigation (by secured hardcopy, outside of FACTS), then when litigation is completed by DOJ, final action is completed and case closed. Records are assigned a case, lead, or qui-tam number, unrelated to any PII contained within, when entered into FACTS. Records are then retrieved by a case, lead, or qui-tam number, and not by name or other unique personal identifier.

The PI office is the data owner of the FACTS system. The FACTS application is managed by the Web Strategies & Collaboration (WS&C) office of the Information Delivery Directorate (IDD) of DHA.

FACTS does not collect information directly from individuals. It is an information system used by PI specialists and fraud analysts for correspondence management and tracking.

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

All PII/PHI is evaluated for impact of loss or unauthorized use and protected accordingly. All documents containing PII/PHI are labeled accordingly and handled as sensitive data. All privacy risks have been mitigated in accordance with IA policies and procedures. The system resides behind the firewall on Department of Defense (DoD) network with an annually reviewed Authority To Operate (ATO). The FACTS application was scanned and reviewed against the Security Technical Implementation Guide (STIG) by certified security professionals and passed an Information Assurance (IA) Risk Assessment. The system will be reviewed annually to safeguard against new vulnerabilities.

FACTS has been audited and awarded a Joint Interoperability Test Command (JITC) certification for Records Management compliance.

All data containing PHI will be originating from within the organization and it will not be sourced from external sources.

All PHI stored in FACTS resides in properly labeled and secured documents. There are no reports that can be run in the system that would disclose PHI.

FACTS is a role-based system and only authorized users with a need-to-know and proper training for handling sensitive data will be granted least privilege to the system. All users of the system are required to pass Annual Information Assurance Awareness training and Health Insurance Portability and Accountability (HIPAA) training.

Users requesting access to the system must submit a Remedy ticket to the Help Desk for processing. The successful completion of a sequential series of verification tasks in Remedy is required before any access is granted. This includes identification of the user account, assignment to the appropriate role in the system,

confirmation of all required training and access forms, and finally explicit approval by the Program Integrity Data Owner.

All DoD information system users are required to successfully pass annual training in Information Awareness Security, Information Management & Computer Security, Cyber Awareness, Internal Controls, and Privacy Act & HIPAA. In addition, all DHA PI staff who access FACTS are further trained in safeguarding data through computer-based training (CBT) and presentations by the on-site web Security Manager. All users of the system are required to report suspected data breaches and instructed on handling unintentional information disclosure through Military Health System (MHS) Learn Incident Management training.

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.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

FACTS does not collect PII directly from individuals. Information contained in FACTS is obtained from existing DoD information systems, other Federal information systems, and commercial systems. The opportunity to object is given at the initial point of collection.

Information collected separately is for the identification of fraud and abuse against the Program and is Law Enforcement Sensitive and is maintained on FACTS. The release of such information to individuals or entities would jeopardize attempts to identify criminal activities against the program which could include the individuals whose PHI/PII information is being collected and is exempt under the Health Insurance Portability and Accountability Act (HIPAA), refer to HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, Public Law 104-191.

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.18 Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

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.

No information is collected from individuals. Information is entered by authorized specialists for the correspondence management of fraud and abuse cases against the Program and is Law Enforcement Sensitive. The release of such information to individuals or entities would jeopardize attempts to identify criminal activities against the program which could include the individuals whose PHI/PII information is being collected and is exempt under HIPAA.

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.18 Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

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.	Because FACTS is not a system of records under the Privacy Act, no Privacy Act Statement is required. Further, because FACTS does not collect PII/PHI directly from individuals, no Privacy Advisory is recommended.

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.