PRIVACY IMPACT ASSESSMENT (PIA)

For the

Armed Forces Billing and Collection Utilization Solution (ABACUS)
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 15754

☐ **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 UII: 007-000005781

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 EDHA 12

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. 1079b, Procedures for charging fees for care provided to civilians; Retention and use of fees collected; 10 U.S.C. 1095, Health care services incurred on behalf of covered beneficiaries: Collection from third-party payers; 42 U.S.C. Chapter 32, Third Party Liability For Hospital and Medical Care; 28 CFR Part 43, Recovery of Costs of Hospital and Medical Care and Treatment Furnished by the United States; 32 CFR 199, Civilian Health and Medical Program for the Uniformed Services (CHAMPUS); 32 CFR Part 220, Collection from Third Party Payers of Reasonable Charges for Healthcare Services; DoDI 6015.23, Foreign Military Personnel Care and Uniform Business Offices in Military Treatment Facilities (MTFs); and E.O. 9397 (SSN), as amended.

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 Armed Forces Billing and Collection Utilization Solution (ABACUS) provides a standard patient accounting system for health care billing practices. It assists Department of Defense (DoD) military treatment facilities in the collection, tracking, and reporting of data required for the DoD Third Party Collection Program billing process by the adoption of standard commercial medical billing practices to military treatment facilities. ABACUS will replace three systems - Third Party Outpatient Collection System, and the Medical Services Account (MSA) and Third Party Inpatient billing modules housed in the Composite Health Care System (CHCS). This solution provides data migration, help desk support, training, maintenance, clearing house services and an electronic "Other Health Insurance" discovery. Utilizing data pulled from CHCS and the Central Billing Events Repository, this solution provides electronic clearing house services for the discovery, identification and collection of patient sales revenue for Uniform Business Office. The U.S. Treasury uses this information to collect from person(s) or organization(s) with outstanding delinquent debts on behalf of the military treatment facility.

The types of personal information collected consists of patient demographic data; employment information; and encounter information such as clinical, ambulatory, inpatient and ancillary facility (laboratory, radiology and pharmacy) visits.

Personal information may be collected for active duty DoD, their dependents and former spouses; non-active duty DoD; non-DoD beneficiaries; Reserve, National Guard and other Federal Agency personnel.

The ABACUS program comes under the Defense Health Agency (DHA) and is managed by the Solutions Development Division (SDD) Program Executive Office (PEO); the IT systems that hosts the ABACUS application is managed by the vendor, General Dynamics Information Technology (GDIT).

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

The privacy risks associated with the PII collected includes unauthorized access, incorrect data in the solution, and unauthorized disclosure. To safeguard against these risks, the environment and associated data, ABACUS has been implemented as a Private Cloud Computing environment and has completed the DoD Information Assurance Certification and Accreditation Process (DIACAP) for compliance with Mission Assurance Category (MAC) III and attained an Authority to Operate (ATO). Other physical, technical and administrative controls such as those listed below are also being put in place to the mitigate risks associated with loss and theft of sensitive data such as that being processed in the ABACUS environment.

1. Keyed access to the physical facilities where data is stored, maintained and archived.
2. Secure and encrypted data file transfer capabilities.
3. DoD Issued Common Access Card (CAC) authentication for administrative and end-users.
4. Role-based permissions which grants user access to data that is appropriate/necessary for them to perform their specific job duties.

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. PII is shared amongst users in the Uniform Business Office (UBO) within Army Medical Command (MEDCOM), Navy Bureau of Medicine (BUMED), Air Force Medical Services (AFMS) and the National Capital Region Medical Directorate (NCR MD).

☒ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. PII will be shared with the billing/claims offices within the U.S. Treasury, the Veteran's Administration and US Coast Guard in order to reimburse DoD for medical services provided to their beneficiaries

☐ **State and Local Agencies.**

Specify.

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

Specify. General Dynamics One Source (GDOS) LLC, the Cloud Services Provider (CSP) shall host ABACUS at their Government-approved Data Center which shall undergo DoD Information Assurance Certification and Accreditation Process (DIACAP) compliance for a Mission Assurance Category (MAC) level III sensitive designation and receive a Certificate of Networthiness (CON). The compliance of the GDOS data centers and additional security monitoring will ensure the protection of Personally Identifiable Information/Protected Health Information (PII/PHI) as directed by the regulations and laws of the Federal Government and DoD, which include HIPAA, the Privacy Act of 1974, and DoD Privacy and Security Regulations, Directives and Instructions.

The CSP shall comply the above federal mandates in addition to the requirements stated in chapters 4.15, 4.16, 4.17, and 4.18 of the ABACUS Performance Work Statement dated 12Jun2013.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Health Insurance Payers. Insurance claims are sent to an external clearinghouse which reformats the data for presentation to the insurance companies and sponsors' insurance companies over approved FIPS 140-2 compliant connection via SFTP (CAL approved port 22).

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.

The ABACUS is not the initial point of collection for any PII. PII is obtained from existing systems.

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.

The ABACUS is not the initial point of collection for any PII. PII is obtained from existing systems.

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.

Although ABACUS is a system of records, it is not the initial point of collection for PII. ABACUS collects PII from other systems rather than directly from individuals. Accordingly, a Privacy Act Statement is not required.

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.