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:

Armed Forces Billing And Collection Utilization Solution - Amazon Web Services (ABACUS-AWS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

02/16/22

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 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 (MTFs) 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 MTFs. ABACUS replaced the Third Party Outpatient Collection System (TPOCS), as well as the Medical Services Account (MSA) and Third Party Inpatient billing modules housed in the Composite Health Care System (CHCS). This solution included the migration of current and historical data from both TPOCS and CHCS; help desk support for end users, end user training, maintenance, clearing house services and an electronic "Other Health Insurance" discovery. ABACUS is now the single source of financial information for the accounting of Services Uniform Business Office (UBO) receivables.

Utilizing data from CHCS and Military Health System (MHS) Genesis, ABACUS develops claims and invoices to aid the UBOs in the recovery of revenue for services rendered at MTFs from third party payers and other federal agencies. In addition, the United States (U.S.) Treasury uses information maintained in ABACUS to collect from person(s) or organization(s) with outstanding delinquent debts on behalf of MTFs.

The types of personal information collected consists of patient demographic data, Social Security Numbers (SSNs,) employment information, and encounter information such as clinical, ambulatory, inpatient, laboratory, radiology, and pharmacy visits.

Personal information is collected for active duty DoD, their dependents and former spouses, non-active duty DoD, non-DoD beneficiaries (such as member of the legislative and executive branches), Reservists, National Guard, Public Health Services, as well as civilian or Federal agency personnel treated at DoD MTFs.

ABACUS is owned by Defense Health Management Systems (DHMS).

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 used for administrative and mission-related purposes primarily to identify beneficiaries and authenticate eligibility in support of the Third Party Collection (TPC), Medical Services Account (MSA), and the Medical Affirmative Claims (MAC) Programs.

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.

ABACUS is not the initial point of collection for PII. PII is obtained from existing systems, and therefore the opportunity to object is only available at the source systems.

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.

ABACUS is not the initial point of collection for PII. PII is obtained from existing systems, and therefore the opportunity to consent to use is only available at the source systems.

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

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.	DHA Uniform Business Office (UBO) Program Office personnel
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Army (MEDCOM) Navy (BUMED) Air Force Medical Operations Agency (AFMOA) National Capital Region (NCR MD)
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	U.S. Treasury Veteran's Administration(VA) Centers for Medicare and Medicaid (CMS) Homeland Security (for Coast Guard)
☐ 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.	General Dynamics One Source (GDOS) LLC (a subsidiary of GDIT), the Cloud Services Provider (CSP) is providing ABACUS to the Government as a cloud-based Software-as-a-Service (SaaS) offering, hosted in the Amazon Web Services (AWS) GovCloud environment. AWS GovCloud is FedRAMP certified for Infrastructure-as-a-Service (Iaas) and Platform-as-a-Service (PaaS) cloud services at level 4. The CSP is responsible for all operations, support and maintenance of ABACUS. The ABACUS contract includes the appropriate FAR clause language to ensure compliance with the Privacy Act of 1974 (5 U.S.C. 552a), the Health Insurance Portability and Accountability Act of 1996, and the Freedom of Information Act (5 U.S.C. 552). Additionally, the contract includes the requirement for Assessment and Authorization (A&A) as specified in DoDI 8510.01 for compliance with Risk Management Framework (RMF) Authority to Operate (ATO) at the moderate level. The following language is included in the contract performance work statement: 1.11.7 PII/PHI, and Federal Information Requirements; The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Health Insurance Portability and Accountability Act (HIPAA): 1.11.7.1 Health Insurance Portability and Accountability Act (HIPAA) The Contractor shall ensure that all staff, including sub-Contractors and consultants, complies with the training requirements of the Privacy Act of 1974 (5 U.S.C. 552a) and Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191). The training requirements are mandated by Office of the Secretary of Defense (OSD) Memorandum 15041-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information": DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003; and the TMA Workforce Training Policy Memorandum, dated May 28, 2008, on the subject, "Workforce Training Policy Pursuant to the Department of Defense Privacy Act Regulations and the Department of Defense Health Insurance Portability and Accountability Act Privacy and Security Regulations."
☐ 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

Composite Health Care System (CHCS) and 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.

ABACUS-AWS will not collect any personally identifiable information (PII) from individuals to be stored in a system of records and retrieved by a personal identifier. Therefore, no SORN is necessary.

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. Unscheduled

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

(3) Retention Instructions.

Unscheduled - Permanent. Treat system and/or records maintained in the system as permanent until a NARA approved schedule and disposition authority has been applied.

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.

The authority for maintenance of the system is as follows:
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; 45 CFR Parts 160 and 164, Health and Human Services, General Administrative Requirements and Security & Privacy; 32 CFR Part 220, Collection from Third Party Payers of Reasonable Charges for Healthcare Services; DoD 6010.15-M, Chapter 3, Medical Services Account; and E.O. 9397 (SSN), as amended.

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.

OMB # 0720-0055 - Third Party Collection Program (Insurance Information) expires 10-31-2022