



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Armed Forces Billing and Collection Utilization Solution (ABACUS)

US Army Medical Command - DHP Funded System

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. 1095, Health care services incurred on behalf of covered beneficiaries: collection from third-party payers; 10 U.S.C. 1079b, Procedures for charging fees for care provided to civilians; retention and use of fees collected; 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.

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 (MTF) 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 US Treasury uses this information to collect from person(s) or organization(s) with outstanding delinquent debts on behalf of the MTFs.

The types of personal information collected include patient demographic data, employment information, and medical information.

(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. This information will be safeguarded through the use of an Private Cloud Computing environment set up and governed by the Federal Risk and Authorization Management Program (FedRAMP). The specific security measures are outlined in item 3d and 3f below.

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 shared amongst users in the Uniform Business Office (UBO) within the US Army Medical Command MTFs.

Other DoD Components.

Specify. PII will be shared amongst users in the UBO within Navy Bureau of Medicine (BUMED), Air Force Medical Services (AFMS) and the National Capital Region Medical Directorate (NCR MD).

Other Federal Agencies.

Specify. PII will be shared with the billing/claims offices within 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 LLC. Cloud Services Provider (CSP) shall host ABACUS at the CSP's Government-approved Data Center which shall be able to be certified and accredited to Federal Information Security Management Act (FISMA) requirements with a Federal Information Processing Standard (FIPS) 199 categorization of Moderate and comply with the security standards detailed in the FIPS 140-2. At a minimum, ABACUS requires a CON and ATO in a Federal Risk and Authorization Management Process (FedRAMP) approved data center with exemplar secure PHI/PII handling. The CSP is responsible for putting in place the various components of underlying software, infrastructure, and processes in order to attain these requirements. The CSP shall comply the above federal mandates in addition to the requirements of chapters 4.15, 4.16, 4.17, and 4.18 of the ABACUS Performance Work Statement dated 12Jun 2013.

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.

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.

- | | |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input checked="" type="checkbox"/> None |

Describe each applicable format.

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

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.