



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Palmetto Government Benefits Administrator (PGBA)
---

TRICARE Management Activity (TMA)/Managed Care Support Contractor (MCSC)
--

### **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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

**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**

MHS Beneficiaries

**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; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary, and Medical Care; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; 32 CFR 199.17, TRICARE Program; 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 Palmetto Government Benefits Administrator (PGBA) Information System's (IS) purpose is to provide enrollment, claims processing, and customer service to individuals eligible for TRICARE benefits. The system is a proprietary IS owned by PGBA, LLC (PGBA). As a subcontractor to the Health Net Federal Services (HNFS - North contract) and Humana Military Healthcare Services (HMHS - South contract), PGBA operates the system out of the BlueCross BlueShield of South Carolina data center located in Columbia, South Carolina.

The PGBA IS is connected to Department of Defense (DoD) systems that provide eligibility, enrollment, deductible and catastrophic cap, TRICARE Encounter Data (TED), and benefits information through the Defense Enrollment Eligibility Reporting System (DEERS) Online Enrollment System (DOES). The PGBA IS is also interfaced with certain systems owned and operated by HNFS - North contract and HMHS - South contract.

The PGBA IS is classified as MAC III Sensitive. The PGBA IS is accessed from the PGBA service centers located in Surfside Beach, Florence, and Columbia, South Carolina. The system is also accessed from multiple HNFS and HMHS TRICARE service centers.

PGBA has developed and hosts a secured web site (i.e., [www.myTRICARE.com](http://www.myTRICARE.com)) used by beneficiaries, providers, government agents, and Prime contractors (i.e., HNFS and HMHS). PGBA provides a backup and recovery plan to TRICARE Management Activity (TMA). The plan is executed annually through a hot site disaster recovery test with connections to DEERS/DOES, TED, HNFS, and HMHS.

The personally identifiable information (PII)/protected health information (PHI) collected is: name, Social Security Numbers (SSN), DEERS identifiers, mailing/home address, marital status, emergency contact, medical information, disability information, gender, date of birth, and home telephone number, credit card numbers, claims information, and enrollment information. The PII/PHI is collected from or about individuals that include active duty personnel, dependents, former spouses, Reservist, and National Guard personnel.

Data is collected, used, and maintained in accordance with the requirements set forth in the TRICARE Next Generation of Contracts (T-NEX) and TRICARE Third Generation (T-3) Managed Care Support Services Contracts.

System contact information:  
Vice President of PGBA Systems  
I-20 @ Alpine Road, mail code AA-225  
Columbia, South Carolina 29219

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

Privacy risks are associated with access to areas where operations personnel provide enrollment services, adjudicate claims, review claims information, and provide customer support.

Privacy risks specific to our system include the risk of exposure of demographic data (name, address, phone number, e-mail address, family member data, etc.), medical data (medical procedures performed, dates of medical procedures, and physician information), and credit card data (member credit card information used to pay enrollment fees).

Physical card access, security cameras, and guards protect the buildings and areas used by operations personnel who view PII/PHI. "Piggybacking" is monitored and employees are disciplined if they allow others to "piggyback" their access.

There are corporate and PGBA TRICARE policies, business rules, and internal instructions written to address the handling of PII/PHI. Our PGBA TRICARE Compliance department issues privacy Warning Notices. PGBA TRICARE management must approve documented access to any PII/PHI related to the T-NEX and T-3 contracts.

Any privacy breach or suspected privacy breach is immediately reported to management and/or the PGBA TRICARE Compliance department. In addition, a "hotline" can be used for employees to report privacy breaches without going through the management chain. Management personnel are encouraged to pursue all potential privacy issues and to call the PGBA TRICARE Compliance department. PGBA TRICARE Compliance department investigates and reports all potential privacy breaches.

With regard to incidental disclosures, Chapter 1, Section 5, Subsection 4.4.1 of the TRICARE Operation Manual directives require that PGBA (as a subcontractor) report to Health Affairs (HA)/TMA through our Prime contractors. The Prime contractors report any disclosure or potential disclosure of personal information, whether PHI or PII, within 60 minutes of determination that a disclosure occurred.

**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.

"HMHS/HNFS discloses certain information ("Information") to Business Associate pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), as that term is defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"). HMHS/HNFS and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to the Agreement in compliance with HIPAA and the regulations promulgated thereunder by the U.S. Department of Health and Human Services, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations ("CFR"), as the same may be amended from time to time and other applicable state and federal laws, rules and regulations."

All contracts contain language which requires the contractor to comply with the HIPAA Privacy Rule and HIPAA Security Rule. In addition to the responsibilities to comply with the HIPAA Privacy Rule and the HIPAA Security Rule, the contractor is required to comply with the Privacy Act of 1974, as amended (Privacy Act).

**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.

Individuals have the ability to object to the collection of their PII by declining interaction with the system. All interaction with the system is voluntary; if an individual refuses to submit claims for payment, the system will not query DEERS for information or store medical or demographic information on an individual. If an individual does not have to pay enrollment fees or refuses to be enrolled, the system will not store any demographic and/or credit card information for an individual. If an individual does not call the Service Center, the system will not collect or store any information for that individual. There are many individuals who are eligible for TRICARE that have never interacted with the system in any way.

(2) If "No," state the reason why individuals cannot object.

**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.

Individuals can verbally or in writing consent or authorize secondary uses of their PII/PHI in accordance with the Privacy Act and Health Insurance Portability and Accountability Act (HIPAA).

As a T-NEX and T-3 subcontractor and claims processor, PGBA is fully compliant with HIPAA regarding the restriction and disclosure of certain information at the request of the individual and regarding the information provided in system-to-system interfaces (DOES/DEERS) with DoD.

Individuals are able to authorize to specific uses and disclosures of their PHI particularly in certain contexts (custody agreements, as permitted by the HIPAA Privacy Rule, personal representative authorizations, and etc.) .

(2) If "No," state the reason why individuals cannot give or withhold their consent.

**k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

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

Describe each applicable format.

<p>The following PAS will appear at or before the point of collection of PII:</p> <p><b>AUTHORITY:</b> 10 U.S.C. Chapter 55, Medical and Dental Care; 38 U.S.C. Chapter 17, Hospital, Nursing Home, Domiciliary, and Medical Care; 45 CFR Parts 160 and 164, Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules; 32 CFR 199.17, TRICARE Program; and E.O. 9397 (SSN), as amended.</p> <p><b>PURPOSE:</b> To provide eligibility, enrollment, deductibles, catastrophic caps, claims processing, and customer service to individuals eligible for TRICARE benefits.</p> <p><b>ROUTINE USES:</b> In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records may specifically be disclosed outside the Department of Defense as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: to the Department of Veterans Affairs, the Department of Health and Human Services, the Department of Homeland Security, and to other federal, state, local, or foreign government agencies, and to private business entities, including entities under contract with the Department of Defense and individual providers of care, on matters relating to eligibility, claims pricing and payment, fraud, program abuse, utilization review, quality assurance, peer review, program integrity, third-party liability, coordination of benefits, and civil or criminal litigation.</p> <p><b>DISCLOSURE:</b> Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.</p>
--

**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.**