



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Medical Evaluation Board (eMEB)
--

US Army Medical Command - Defense Health Program (DHP) Funded Application
---

### **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**

**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.

Statutory Authority: 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. Chapter 55, Medical and Dental Care; 10 U.S.C. Chapter 61, Retirement or Separation for Physical Disability; and Army Regulation 40-3, Medical, Dental, and Veterinary Care; and E.O 9497 (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.

As the Army system of record, the Electronic Medical Evaluation Board (eMEB) allows the electronic processing of Medical Evaluation Board cases. eMEB will ultimately reduce the amount of time required to process a case, as well as, reduce the amount of paperwork needed to input a case file in the system. The required forms are digitized, available on-line, and capable of pulling data from other authoritative data sources. eMEB will reside on the infrastructure currently managed by the Army Publishing Directorate (APD) known as the AFCMP (Army Forms Content Management Portal) which provides the central tools to manage this process. eMEB will be accessible through APD's MyForms environment.

The types of PII collected in the system includes demographic data, military records, financial 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 collection are unauthorized access, inaccurate information in the system/electronic collection, and unauthorized disclosure of PII. There are security measures in place to mitigate these risks. The specific security measures are addressed later in Section 3 of this PIA.

**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.

The PII will be shared within the US Army Medical Command (MEDCOM) organizations using this system and provided to the following systems: Medical Occupational Data System (MODS), MyMEB, Army MEDCOM Systems, Electronic Physical Evaluation Board (ePEB), and Integrated Total Army Personnel Database (ITAPDB). eMEB does not directly interface with any Army Systems with the exception of ePEB. ePEB receives PII from eMEB with a one-time pass of information through an interface to build a case file in ePEB and pass medical documentation for any referred conditions.

**Other DoD Components.**

Specify.

eMEB does not interface with any DoD systems.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

Dynamic Technology Systems (DTS) is the IT Contractor used by APD and is responsible for the sustainment of eMEB. Each contract employee will be required to meet certain security related requirements in order to gain access to certain data and systems as pertains to their roles. The contractor is responsible for safeguarding information of a confidential or sensitive nature. In addition, there are clauses in the contract requiring compliance with the Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA).

**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.

The individual is not present when the PII is collected for eMEB. The PII for eMEB will be collected from other authorized systems and documents to include medical records, MODS, and iTAPDB.

**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 individual is not present when the PII is collected for eMEB. The PII for eMEB will be collected from other authorized systems and documents to include medical records, MODS, and iTAPDB.

**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.

The individual is not present when the PII is collected for eMEB. The PII for eMEB will be collected from other authorized systems and documents to include medical records, MODS, and iTAPDB.

**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.**