



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Medication Management Assistant (EMMA) <sup>TM</sup>
---

Department of the Navy - Congressionally Funded Research Grant
--

### **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.**



**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.

System of Record Authorities: 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 1095, Collection from Third Party Payers Act; 10 U.S.C. 5131 (as amended); 10 U.S.C. 5132; 44 U.S.C. 3101; 10 CFR part 20, Standards for Protection Against Radiation; and, E.O. 9397 (SSN)

Medical and dental care in the DoD are authorized by Chapter 55 of Title 10 U.S.C., section 1071 - 1106. The provision of a pharmacy benefit is part of the medical care benefit.

**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.

EMMA consists of medication delivery units and two-way web-based communication software that allows a pharmacist or other licensed practitioner to remotely manage prescriptions stored and released by the patient-operated EMMA system. The system is accessed using web-based software on the healthcare provider's desktop computer and connects to a secure data center using encrypted communications. The EMMA™ system is a web based system that allows pharmacists and physicians to remotely manage and monitor a patient's medication. EMMA assists with the stewardship of controlled substances and, most importantly, assists Wounded Warrior patients to become more independent as they transition from an inpatient to ambulatory setting. EMMA helps Wounded Warrior patients to take the right medication at the right time and provides real time feedback to the Warrior patient's healthcare provider and pharmacist.

The types of PHI/PII collected in the system include name, medication name, prescription number, social security number, date of birth, gender, personal cell phone number, home telephone number, personal email address, disability information and spouse information.

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

All systems are vulnerable to "insider threats." Pharmacy managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. There are defined criteria to identify who should have access to EMMA. These individuals have gone through extensive background and employment investigations. The EMMA® System unit employs security in multiple ways:

- The EMMA® System unit is a sturdy, sealed device secured with a tamper alert system which communicates with our data center in the event that the device is tampered with. The EMMA® System cover is made of steel for the sides, top and rear. A sturdy, casted, plastic molded front cover is snugly fitted to the front of the EMMA® System unit.
- The EMMA® System unit cannot be remotely accessed, for security purposes. Instead, the EMMA® System unit polls our secure data center and retrieves all information that is available.

**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 authorized pharmacy staff will have access to PII as part of their duties. Vendor authorized personnel will have access to the system to perform support and maintenance.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

DEA

**State and Local Agencies.**

Specify.

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

Specify.

Telemedicine and Advanced Technology Research Center (Army). 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 DoDD 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.

The Contractor shall comply with all requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), as implemented by the HIPAA Privacy and Security Rules codified at 45 C.F.R. Parts 160 and 164, and as further implemented within the Military Health System (MHS) by DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003, and DoD 8580.02-R, "DoD Health Information Security Regulation, July 12, 2007. The Contractor shall also comply with all applicable HIPAA-related rules and regulations as they are published and as further defined by later-occurring Government requirements and DoD guidance, including current and forthcoming DoD guidance implementing applicable HIPAA amendments under the American Recovery and Reinvestment Act of 2009 (ARRA). Any rules and regulations that are published, and/or requirements that are defined after the award date of this contract, and that require expenditure of additional Contractor resources for compliance, may be considered "changes" and will be subject to the "changes" clause under the contract.

**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 EMMA® system does not collect PII directly from the patient - it is not the source system.

[Empty box]

**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.

[Empty box]

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

The EMMA® system does not collect PII directly from the patient - it is not the source system.

**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 EMMA systems does not collect PII directly from the patient - it is not the source system.



**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.**