



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Medical Communications for Combat Casualty Care (MC4)

Department of the Army / Program Executive Office Enterprise Information Systems (PEO EIS)

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. 3013, Secretary of the Army; 10 U.S.C. 1071-1085, Medical and Dental Care; 50 U.S.C. Supplement IV, Appendix 454, as amended, Persons liable for training and service; 42 U.S.C. Chapter 117, Sections 11131-11152, Reporting of Information; 10 U.S.C. 1097a and 1097b TRICARE Prime and TRICARE Program; 10 U.S.C. 1079, Contracts for Medical Care for Spouses and Children; 10 U.S.C. 1079a, CHAMPUS; 10 U.S.C. 1086, Contracts for Health Benefits for Certain Members, Former Members, and Their Dependents; E.O. 9397 (SSN); DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs); DoD Directive 6040.37, Confidentiality of Medical Quality Assurance (QA) Records; DoD 6010.8-R, Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); Army Regulation 40-66, Medical Record Administration and Health Care Documentation.

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 MC4 systems are required for Army compliance with the Title 10, section 1074f (1997 and 2008) US Code Statutory Requirement to establish a longitudinal electronic medical record for deployed forces / service members. MC4 is medical information management system for Army deployed medical forces enabling collection of a comprehensive life-long electronic medical record for service members and enhance medical situational awareness to operational commanders.

The MC4 System provides the Army's single medical Information Management/ Information Technology System for automation and digitization efforts for deployable medical forces. It integrates and links tactical medical automation information management solutions vertically throughout the levels of health care and horizontally into Army Battle Command, Combat Service Support and communications architectures. Information collected are patient demographics, medical information, military information, and disability information.

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

Risk of exposure of an individual's SSN is mitigated in the system. All personnel accessing MC4 systems are required to undergo a background investigation and receive a favorable adjudication (IT 1, IT 2 or IT 3). Approved personnel receive a CAC (Common Access Card), which authenticates their credentials before being authorized to access the MC4 systems. In addition to the CAC card, each user requires a MC4 User Account in order to access/process/change data on the MC4 systems. This MC4 User Account defines specific MC4 application access privileges according to the user's job responsibilities and security roles. Accesses to PII data are available only to specific restricted job responsibilities and security roles. The PII is hidden to all other job responsibilities and security roles.

Furthermore, the MC4 system is DIACAP accredited. There is daily monitoring of network intrusion detection, firewall and regular adherence to Information Assurance Vulnerability Alerts (IAVA's) and Security Technical Implementation Guides (STIG's). Files transferred across the NIPRNET using a secure Virtual Private Network (VPN) tunnel or Secured File Transfer Protocol (SFTP). MC4 does not create new data about individuals through aggregation. Appropriate safeguards are in place for the collection, use and sharing of information. Security measures are adequate and risk is minimal.

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. All Army health care providers and personnel staff within various levels of commands.

Other DoD Components.

Specify. All DOD components health care providers and personnel staff within various levels of commands.

Other Federal Agencies.

Specify. All Federal Agencies health care providers and personnel staff within various levels of commands.

State and Local Agencies.

Specify.

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

Specify. MC4 systems are maintained IAW current DOD and Army IA security policies by a worldwide system administrator network of contractor support personnel. Each are subject to the 5 U.S.C. 552a, as amended, the Privacy Act of 1974 and DoD 5400.11-R, "Department of Defense Privacy Program." Personally Identifiable Information contained in this system may be used only by authorized persons in the conduct of official business and HIPAA warning, that applies to any system accessed by this connection which contains data related to the health of an individual, Protected Health Information in this system is subject to Public Law 104-191, the Health Insurance Portability and Accountability Act of 1996 and the Final Privacy Rule and Final Security Rule codified in 45 C.F.R. § 160 and 164, DoD 6025.18-R, "DoD Health Information Privacy Regulation" and DoD 8580.02-R, "DoD Health Information Security Regulation." Information in this system may only be used and/or disclosed in strict conformance with these authorities. All contractors are required to take initial and annual refresher training for HIPAA Operations and Privacy Act.

Other (e.g., commercial providers, colleges).

Specify. The MC4 system only allows healthcare providers with an account and appropriate privileges to access the needed medical data. Once an encounter is signed by the Doctor, it is automatically sent (encrypted) to the CDR. In order for healthcare providers to enter data, they must enter their appropriate information.

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.

If the soldier is conscious at the time of treatment, he or she can object. Personal information is provided by the individual at the creation of the medical record.

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

If the soldier is unconscious at the time of treatment, he or she cannot object. Personal information is provided by the individual at the creation of the medical record.

[Empty rectangular 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.

If the soldier is conscious at the time of treatment, he or she can object. Personal information is provided by the individual at the creation of the medical record.

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

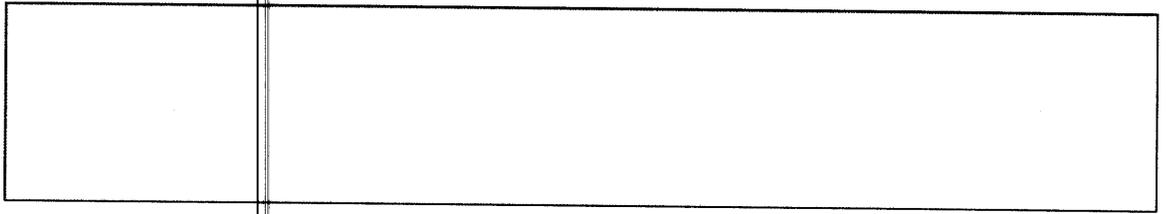
If the soldier is unconscious at the time of treatment, he or she cannot object. Personal information is provided by the individual at the creation of the medical record.

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.

Electronic and paper



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.