



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Patient Safety Reporting (PSR)
TRICARE Management Activity (TMA)

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

DoD Clearance and OMB Licensing requirements are currently being reviewed by the TMA Information Collection Management Officer. The PIA will be updated accordingly with their decision.

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. §§1071-1085, 1086, 1097(a) – (b) (Processes for Patient Safety in Military and Veterans Health Care Systems (§1071 Note), Medical and Dental Care, Civilian Health and Medical Program of the Uniformed Services, Contracts for Health Benefits for Certain Members, Former Members, and their Dependents); 10 U.S.C. §1102 (Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants); 42 U.S.C. §201 (Patient Safety and Quality Improvement Act of 2005); 32 C.F.R. Part 199.17 (TRICARE Program); 45 C.F.R. Parts 160 and Subparts A and E of 164 (Health Insurance Portability and Accountability Act Privacy Rule); and, E.O. 9397 (as amended, 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.

The purpose of this system is to provide adverse event reporting, management, and analysis capabilities to the Military Health System (MHS). PSR will establish a uniform MHS automated web-based standardized system that will allow for near-miss reporting, adverse event reporting, provided analysis of medical errors and management improvements that will systemically decrease errors.

The data and reports generated by the PSR system will enable the prompt notification to Military Treatment Facility (MTF) personnel of patient safety events. The aggregation of information provides data for analysis and trending, while MHS gains the ability to share de-identified information across the sites, among the Services, and with the DoD Patient Safety Center (PSC) in order to raise performance. PSR will supply fully de-identified event information as required for compliance with The Joint Commission (TJC) and DoD PSC for data management.

The system will collect the following personally identifiable information (PII): Patient name, date of birth, family member prefix (FMP), Sponsor's social security number (SSN) and details about the safety event involving the patient. Details may include but are not limited to: patient's condition before and after the event, medications, diagnosis, family member's name and contact information if they witnessed the event, and patient's status (inpatient, outpatient).

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

Currently the system is in the development and demonstration phase of acquisition. The privacy risk is that PII/protected health information (PHI) will be viewed/used by people without the need to know. The system has been configured to display the 10 U.S.C. § 1102 privacy statement at the bottom of every screen and will print this on every page. Training will emphasize the requirement to keep PII/PHI out of narrative descriptions. Rules of conduct will be in place and enforced through training and awareness, auditing of user activity, and reminders/warnings concerning proper use.

Records are maintained on optical and magnetic media. Data storage is in fully secure Defense Information System Agency (DISA) spaces. Records may be retrieved by sponsor's Social Security Number, Beneficiary ID (sponsor's ID, patient's name, patient's DOB, and family member prefix), or any combination of the above. Automated records are maintained in controlled areas accessible only to authorized personnel. Entry to these areas is restricted to personnel with a valid requirement and authorization to enter. Physical entry is restricted by the use of a cipher lock. The system will comply with the DoD Information Assurance Certification and Accreditation Process (DIACAP). Access to PSR records is restricted to individuals who require the data in the performance of official duties. Access is controlled through use of passwords. This system is a web-based single instance with fully redundant back-up. Records will be retained and disposed in accordance with the Administrative Instruction (AI) 15.

In addition, SORN amendments are in progress and will be submitted to the Defense Privacy Office for transmittal to the Federal Register upon completion.

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.

MTF personnel with the appropriate level of certification granted as a result of a National Agency Check with Written Inquires (NACI) or DoD-determined equivalent investigation and personnel with a need to know.

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.

Science Applications International Corporation (SAIC) - Tier III System Maintenance and Training Personnel with ADPII or higher security clearance
JACER Corporation - Program Office Personnel with ADPII or higher security clearance.

The contract contains basic safeguards and controls for the protection of PII/PHI. Contract modifications, which will address more specific safeguards and controls, are being requested.

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.

PSR is a system used in the course of health care operations, specifically quality assessment activities. The health care provider with authorization to patient and MTF staff PII will enter and/or view the data. All information in the PSR is protected from discovery by 10 U.S.C. § 1102 and all printable documentation in PSR will be watermarked with that information. PSR will supply fully de-identified event information as required for compliance with The Joint Commission (TJC) and DoD Patient Safety Center (PSC) for data management.

(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.

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

PSR is a system used in the course of health care operations, specifically quality assessment activities, in accordance with DoD 6025.18-R. PSR is used for no other purpose and collection of personally identifiable information from individuals is required for the completion of a patient safety report, objections to the collection of PII/PHI will prevent the completion of the quality assessment activity. Only health care providers with authorization to patient and MTF staff PII/PHI will enter and/or view the data. All information in the PSR is protected from discovery by 10 U.S.C. § 1102 and all printable documentation in PSR will be watermarked with that information. PSR will supply fully de-identified event information as required for compliance with TJC and PSC for data management.

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

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

Describe each applicable format.

In addition to the Privacy Act Statement (PAS) the patient is provided with a copy of The MHS Notice of Privacy Practices (NOPP) which includes use of PII/PHI for health care operation.

The end user will view the DoD warning banner, HIPAA banner and the Privacy Act warning when logging in to the system.