PRIVACY IMPACT ASSESSMENT (PIA)

For the

Patient Safety Reporting (PSR)
Defense Health Agency (DHA)

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: 166
- ☐ **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 UII: 007-000000111

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.

Pub. Law 106–398 Section 754, Patient Care Reporting and Management System; 10 U.S.C. Chapter 55, Medical and Dental Care; 42 U.S.C. Chapter 6A, Subchapter VII, Part C, Patient Safety Improvement; 32 CFR 199.17, TRICARE Program; DoDI 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); DoD 6025.13-R, Military Health System (MHS) Clinical Quality Assurance (CQA) Program Regulation; 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 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, provide analysis of medical errors and management improvements that will systemically decrease errors. PSR is a Commercial Off-the-shelf Common Access Card access enforced system.

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 Personally Identifiable Information (PII) / Protected Health Information (PHI) about individuals collected in the systems are:

Personal descriptors, ID numbers, health, financial, employment, life, and education.

PSR is owned and operated by the Defense Health Services Systems Program Executive Office (DHSS PEO).

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

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.

Records are maintained on optical and magnetic media. Data storage is in fully secured Defense Information System Agency (DISA) spaces protected by several fire walls. The Patient Safety Reporting System (PSR) does not retrieve data by name or unique personal identifier. Individuals authorized to use PSR are taught to search for events using event number and not patient names or identifiers. 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 to the servers located in the Defense Information System Agency (DISA) spaces are 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 Common Access Card (CAC) including a personalized pin number. This system is a web-based single instance with fully redundant back-up. 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. In addition, this system does not require a system of records notice (SORN) at this time.

Several PII safeguards are integrated into the system.
• Once the Reporter has submitted the event it is no longer viewable by the Reporter
• Role-based security restricts Reviewers/Investigators access to reports within their facility and to those assigned to them in which their role allows
• As a standard business process, users with a need to know (PSM, Reviewer/Investigators) are taught to search for events by event number not patient name or patient identifier
• Once the event report is finalized and the report released to the Service Headquarters and Patient Safety Center, it is de-identified.
• PII is restricted base on role and security settings.

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. DoD Patient Safety Center (PSC)

☐ **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 Personnel with ADPII or higher security clearance

Irving Burton Associates (IBA) - Program Office Personnel with ADPII or higher security clearance.

The contract contains basic safeguards and controls for the protection of PII/PHI.

☐ **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.

PSR is a system used in the course of quality assessment activities and uses de-identified data. Because the health care provider with authorization to patient and MTF staff PII will enter and/or view the data , the notice and ability object occurs at that time.

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 patients and MTF staff 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 PSC for data management.

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