PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Patient Safety Reporting-Amazon Web Services (PSR-AWS)

2. DOD COMPONENT NAME:

Defense Health Agency

3. PIA APPROVAL DATE:

01/12/2026

Program Executive Office (PEO) Medical Systems (J6)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☒ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The modernized Patient Safety Reporting (PSR) system, hosted on the Amazon Web Services (AWS) GovCloud (PSR-AWS), is a Public-Key Infrastructure (PKI)/Common Access Card (CAC) and Personal Identify Verification (PIV) compliant automated information system (AIS) for patient safety event reporting, event investigation/management, and data analysis. PSR-AWS is an upgraded version of the RLDatix Cloud IQ (DCIQ) Commercial Off-the-Shelf (COTS) software, acquired to optimize patient safety initiatives focused on eliminating preventable harm for Military Health System (MHS) and Veterans Health Administration (VHA) beneficiaries/patients.

PSR-AWS is implemented throughout the MHS and VHA, permitting authorized personnel to enter patient safety event information (i.e., adverse events, no-harm events, near miss events, or unsafe/hazardous conditions) within Military Treatment Facilities (MTFs) and other applicable healthcare environments. To promote increased reporting, and to protect against retaliation, individuals may choose to withhold their identity when completing a PSR-AWS report. PSR-AWS functionality includes a standardized event taxonomy for user groups to classify medical errors and compile trending reports supporting the overall patient safety mission. PSR-AWS is a key enabler of DHA Clinical Quality Management (CQM) activities governed by Department of Defense Instruction (DoDI) 6025.13, "Medical Quality Assurance and Clinical Quality Management in the Military Health System," DHA Procedures Manual (DHA-PM) 6025.13, "Clinical Quality Management in the Military Health System, Volumes 1-7," and the references therein.

Personally identifiable information (PII) collected by PSR-AWS includes patient personal descriptors, unique identification number(s), and protected health information (PHI) related to a patient safety event; name and contact information of reporting personnel, event reviewer(s), event handler(s), and MTF patient safety manager(s); and name and contact information of medical providers involved in the event.

PII is collected from the following categories of individuals, including Active Duty Service Members, members of the National Guard and/or Reserve Components, Veterans, Retirees, DoD Beneficiaries, Contractors, Foreign Nationals, former spouses, and prisoners of war.

PSR-AWS is owned/managed by the Clinical Support Program Management Office (CSPMO)/Solution Delivery Division (SDD)/Program Executive Office (PEO) Medical Systems (J-6)/Defense Health Agency (DHA).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PSR-AWS collects PII/PHI to support the DHA Patient Safety Center and VHA National Center for Patient Safety (NCPS) mission and to identify the patient, medical providers, or other persons who may have witnessed or been involved in a patient safety event.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Individuals do not have the opportunity to object to the collection of their PII as PSR-AWS is not the initial point of collection.

f. 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.

Individuals do not have the opportunity to consent to the specific uses of their PII as PSR-AWS is not the initial point of collection.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

PSR-AWS does not collect PII directly from individuals. Therefore, no Privacy Act Statement or Privacy Advisory is required.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DHA Military Treatment Facilities (MTFs)
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Departments of the Army, Navy, and Air Force; DoD Combatant Command(s)
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	VHA Medical Centers; VHA NCPS
☐ State and Local Agencies	Specify.	
☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	PSR Tier III System Maintenance Personnel shall establish appropriate administrative, technical, and physical safeguards to protect Government data. The Contractor shall ensure the confidentiality, integrity, and availability of Government data per applicable laws and regulations, including data breach reporting and response requirements, required by DFAR Subpart 224.1 (Protection of Individual Privacy), DoDD 5400.11, "DoD Privacy Program," and DoD 5400.11-R, "DoD Privacy Program. The Contractor shall also comply with federal laws relating to freedom of information and records management.
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☐ Individuals ☐ Databases

☒ Existing DoD Information Systems ☐ Commercial Systems

☒ Other Federal Information Systems

PSR-AWS does not possess automated interfaces with existing DoD clinical or business system - Users manually retrieve and enter information from MHS GENESIS, Defense Medical Human Resources System - internet (DMHRSi), and/or other applicable MTF systems. Other Federal Information Systems: Users manually retrieve and enter information from applicable VHA Medical Center systems.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ In-Person Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☒ Website/E-Form

☐ Other *(If Other, enter the information in the box below)*

PSR-AWS URL: https://jpsr.health.mil.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier EDHA 07

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date.

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 2.7, item 020 (DAA-GRS-2017-0010-0002)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

FILE NUMBER: 204-10.1
DISPOSITION: Temporary. Cut off at the end of the calendar year; destroy 6 years after cut off.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

Pub. Law 106-398 Section 754, Patient Care Reporting and Management System; 10 USC § 1102 Confidentiality of Medical Quality Assurance Record: Qualified Immunity for Participants; 10 USC Section 55, Medical and Dental Care; 42 USC Chapter 6A, Subchapter VII, Part C, Patient Safety Improvement; 32 CFR 199.17, TRICARE Program; DoDI 6025.13 Medical Quality Assurance and Clinical Quality Management in the Military Health System; DHA Procedures Manual 6025.13, Clinical Quality Management in the Military Health System (MHS) Volumes 1-7, and the references therein.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Per DHA's Information Management Control Officer (IMCO), JPSR-AWS does not require an OMB Control Number as the system is not the initial point of collection of information.