

## 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:**

Centralized Credentials and Quality Assurance System (CCQAS)

**2. DOD COMPONENT NAME:**

Defense Health Agency

**3. PIA APPROVAL DATE:**

8/12/2020

### SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** (Check one. Note: foreign nationals are included in general public.)

- |  |  |
|--|--|
| <input type="checkbox"/> From members of the general public  | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4)   |

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

- |  |   |
|--|---|
| <input type="checkbox"/> New DoD Information System                    | <input type="checkbox"/> New Electronic Collection      |
| <input checked="" type="checkbox"/> Existing DoD Information System    | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.**

Centralized Credentials and Quality Assurance System (CCQAS) is a web-based system that contains credentialing, privileging, risk management, and adverse actions data on Active Duty, National Guard, Coast Guard, Reserve, Public Health Service, Volunteer, Civilian, and Contractor healthcare providers that work in Medical Treatment Facilities (MTFs) throughout the world.

The system tracks provider training and education through information input and record retention. It also allows healthcare providers to apply for privileges electronically, allows for the electronic review, routing, and approval of provider privileges, and streamlines the credentialing and privileging process. It is accessible 24/7 via the Web to users with role based access permissions.

The types of PII collected by CCQAS include personal descriptors, identification numbers (including Social Security Numbers (SSNs)), education information, health information, employment information, photographs, and information regarding children.

Current product features include the ability to:

- Capture, store, maintain and report on medical malpractice claims, incidents, disability claims and adverse actions. These records include both the provider's documentation of an incident or event in addition to patient data specific to the incident or event.
- Maintain the credential records of direct-care providers, i.e. medical school records, diplomas, certificates, additional training, and experience documentation.
- Share providers above mentioned PII between DoD facilities.
- Automate the provider's application for privileges to provide medical healthcare.
- Potentially Compensable Event (PCE) capture and visibility.
- Adverse Action tracking capture and visibility.

CCQAS is owned and operated by DHA and managed and resourced by the Solutions Delivery Division (SDD).

**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)

The intended use of PII is for verification purposes. Information is used to verify the provider's qualifications to perform the requested medical/dental procedures and to approve the procedures. This requirement is per The Joint Commission and state licensing agencies, which require health care organizations to maintain medical provider qualifications.

**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.

Medical healthcare providers are the primary, individual users of the system. A provider's submission of personal data is voluntary. However, failure to provide information may result in a provider's ineligibility to serve at an MTF or within the Military Health System (MHS). It is necessary to ensure that our healthcare providers have the credentials and training for the privileges they perform and that all information is documented in claims and adverse actions as necessary. Providers may object to PII collection through face-to-face, E-mail, paper, or telephone modes of collection.

Patients do not access the system. However, personal patient data may be found in risk management or adverse action data files. A patient's personal data recorded in the system is not voluntary. Information stored within risk management or adverse action files reflect the details of a malpractice claim, incident, disability claim, or adverse event related to the healthcare provider of record, and thus, patient information is disclosed as part of the known event. There is no process for a patient to object to PII collection as the record is part of a historical, formally documented known event.

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.

Medical healthcare providers are the primary individual users of the system. Upon the completion of system registration, providers must read and verify the CCQAS Privacy Act Statement by selecting the "Yes" radio button. The system does not allow prospective registrants to continue unless they select this radio button. Providers consent to the specific uses of PII in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3.

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

Privacy Act Statements are included on every form completed by an individual provider. Privacy Act, HIPAA, and 10 U.S.C. 1102 statements all appear on the login screen and must be acknowledged before a user can access CCQAS.

AUTHORITY: 10 U.S.C. 1102, Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants; 42 U.S.C. 11112, Encouraging Good Faith Professional Review Activities; DoD Instruction 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); DHA-PM 6025.13, Clinical Quality Management in the Military Health System; and E.O. 9397 (SSN), as amended.

PURPOSE: To obtain information necessary to credential a health care provider and determine whether that individual should have privileges to work or continue working in a military treatment facility (MTF) or within the Military Health System (MHS). Data in the system may contain medical records information including patient care assessments and treatment procedures which may be used to assess malpractice claims and adverse privilege actions filed against a health care provider at an MTF within the MHS.

ROUTINE USES: Your records may be disclosed outside of DoD in accordance with the DoD Blanket Routine Uses published at <http://dpcllo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx> and as permitted by the Privacy Act of 1974, as amended (5 U.S.C. 552a (b)).

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within the DoD. Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

Collected information may be shared with government boards, agencies, professional societies, civilian medical institutions, or organizations if needed to apply for privileges, licenses, or to monitor professional standards of health care practitioners. Information may also be used to conduct trend analysis for medical quality assurance programs.

DISCLOSURE: Voluntary. However, failure to provide information may result in an individual's ineligibility to serve at an MTF or within the MHS.

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

Within the DoD Component

Specify.

Defense Healthy Agency - Healthcare providers at MTFs and/or administrators may need to review or approve a provider's privilege application at each location a provider will provide medical health services. PII is shared to verify the provider during the credentialing and privileging processes.

Other DoD Components

Specify.

Army Reserve, Navy Reserve, Marine Corps Reserve, Air Force Reserve, Army National Guard, Air Force National Guard, and Public Health Service - Healthcare providers at MTFs and/or administrators may need to review or approve a provider's privilege application at each location a provider will provide medical health services. PII is shared to verify the provider during the credentialing and privileging processes.

Other Federal Agencies

Specify.

Coast Guard, Coast Guard Reserve - Healthcare providers at MTFs and/or administrators may need to review or approve a provider's privilege application at each location a provider will provide medical health services. PII is shared to verify the provider during the credentialing and privileging processes.

State and Local Agencies

Specify.

Code Maintenance Contract - Tier III System Maintenance Personnel with Public Trust or higher security clearance. "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."

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.

DSA #12-884F – for PSI Code Maintenance Contract #HT0015-20-F-0078.  
DSA #18-1971 – for Institute for Defense Analyses (IDA).  
DSA #15-1383 – for TRICARE Pharmacy Program, Fourth Generation (TPharm4) Contract #HT9402-14-D-0002. Renewal request, DSA #15-1383B, is currently being processed by the Data Sharing team supporting the DHA Privacy and Civil Liberties Office as of Dec 2018.  
  
Note: DoDD 5400.11 was reissued as and canceled by DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019.

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

Existing DoD Information System: CCQAS receives the National Provider Identifier (NPI) number from the Defense Medical Human Resources System-internet (DMHRSi).  
Other Federal Information Systems: CCQAS users query the National Practitioner Data Bank (NPDB) web-based repository from the U.S. Department of Health and Human Services (HHS) and manually enter data into CCQAS. CCQAS also receives the List of Excluded Individuals/Entities from HSS-Office of the Inspector General; this data is entered manually by system administrators.

**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)

Face-to-Face Contact

Paper

- Fax  Telephone Interview
- Information Sharing - System to System  Website/E-Form
- Other (If Other, enter the information in the box below)

E-mail, Face-to-Face Contact, Telephone Interview: DoD Service credentialers may collect PII from providers and enter the information into the system as modular users.

Paper: Each DoD Service may maintain an inventory of paper documentation that can be used to collect information about the provider's qualifications.

Information Sharing: DMHRSi interface provides NPI.

Website/E-Form: Information is collected electronically from the individual via a secure Internet or network interconnection. (<https://ccqas.csd.disa.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

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.d.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.

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

(3) Retention Instructions.

TEMPORARY cut off annually Delete/Destroy when 10 years old.

**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 statute 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.

10 U.S.C. 1102, Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants; 42 U.S.C. 11112, Encouraging Good Faith Professional Review Activities; DoDI 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); DHA-PM 6025.13, Clinical Quality Management in the Military Health System; and E.O. 9397 (SSN), as amended.

**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.

CCQAS does not currently have an OMB control number. However, the CCQAS team is currently working with Information Management Control Office (IMCO) to create new OMB package. Anticipated approval is FY21 Q2.