PRIVACY IMPACT ASSESSMENT (PIA)

For the

Centralized Credentials and Quality Assurance System (CCQAS)
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: 136
- ☐ **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: 007-000000067

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 EDHA 09

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	0720-TBD; 60-day Federal Register Notice re-published on 5/18/2015.
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. 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); DoDM 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); 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.

CCQAS is a Web-based system containing credentialing, privileging, risk management, and adverse actions data on Active Duty, National Guard, Coast Guard, Reserve, Public Health Service, Department of Veterans Administration, Volunteer, Civilian, and Contractor healthcare providers working in Medical Treatment Facilities (MTFs) throughout the world. The system allows 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 who have been given permission to use it. Only those with approved permissions can access CCQAS, so it is not a public system.

The types of personally identifiable information (PII) and protected health information (PHI) collected by CCQAS includes: Name; Other Names Used; Social Security Number (SSN); Driver's License; Other ID Number = National Provider Identifier (NPI) and Electronic Data Interchange Personal Identifier (EDIPN); Citizenship; Gender; Birth Date; Home Telephone Number; Personal Email Address; Mailing/Home Address; Spouse Information; Marital Status; Child Information; Medical Information (may be used in Risk Assessment module for patients involved in a claim); Disability Information; Employment Information; Military Records; Education Information; Professional Certificates; Service; Rank; Sponsor SSN; Military Treatment Facility.

No data is electronically transmitted out of CCQAS via an interface or messaging system because it is protected under 10 U.S.C. 1102, Confidentiality of medical quality assurance records: qualified immunity for participants. However, CCQAS does receive one data element, the NPI, from the Defense Medical Human Resources System-internet (DMHRSi).

CCQAS is currently in both development and sustainment. Current product features include the ability to:

- Capture, store, maintain and report on medical malpractice claims, incidents, disability claims and adverse actions.

- Maintain the credentials records of direct-care providers.

- Automate the provider's application for privileges.

- Potentially Compensable Event (PCE) Capture and Visibility.

- Adverse Action tracking capture and visibility.

CCQAS is managed and resourced by the Solutions Delivery Division (SDD). Physically, CCQAS resides on servers located in Defense Information Systems Agency (DISA) facilities in San Antonio, Texas, with off-site back-up facilities in Oklahoma City, OK. Incremental file backup and archived file storage is where provided by the DISA facility site in San Antonio.

CCQAS is owned and operated by DHA. Users at MTFs and Surgeon General staff (i.e., Army Medical Department (AMEDD), Air Force Medical Operations Agency (AFMOA), and Navy Bureau of Medicine and Surgery (BUMED)) access CCQAS via the Web 24/7, using Internet Explorer as the browser. It is currently Common Access Card (CAC) and Personal Identification Verification (PIV) card enabled, soon to be CAC-enforced-Single sign-on (SSO). It is a networked system that is classified as a Mission Assurance Category (MAC) level III, Sensitive system. CCQAS is currently a role-based system that can be accessed only by individuals with a need to know.

A PIA has been previously submitted for this system with a final signature date of March 29, 2012.

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

All applicable security and privacy processes and regulations have been defined and implemented, reducing privacy risks to the maximum extent possible. However, the privacy of an individual can become compromised if a CCQAS user discloses PII / PHI to someone who does not have the need to know.

To mitigate this risk, all users are required to have a security clearance with a minimum of an IT Level II Position Sensitivity Designation and are trained to protect PII / PHI. All data in CCQAS, whether PII or not, is protected under the 10 U.S.C. 1102, and users are trained and expected to comply with this policy. All users must comply with Privacy Act and HIPAA regulations and as such, take annual training.

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.

☒ **Other DoD Components.**

Specify. Reserve, National Guard, Public Health Service - Healthcare providers at MTFs and/or administrators that may need to review or approve a provider's privilege application.

☒ **Other Federal Agencies.**

Specify. Coast Guard, Department of Veteran's Administration - Healthcare providers at MTFs and/or administrators that may need to review or approve a provider's privilege application.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

Submission of information is voluntary. However, failure to provide information may result in an individual's ineligibility to serve at an MTF or within the MHS. It is necessary to ensure that our health care providers have the credentials and training for the privileges they perform and that all information is documented in claims and adverse actions as necessary. The individual can choose not to furnish their personal data however in order to be allowed to work at the facility, it is mandatory that they provide this information for verification and validation.

(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.

Consent to the specific uses of PII is obtained as necessary, in accordance with DoD 5400.11-R, DoD Privacy Program, C4.1.3.

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

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.	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 logon 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); DoDM 6025.13, Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS); 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 or within the MHS.

ROUTINE USES: Your records may be disclosed outside of DoD in accordance with the DoD Blanket Routine Uses published at http://dpclo.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 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.

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.