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:

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

□ From members of the general public

□ From Federal employees and/or Federal contractors

☒ From both members of the general public and Federal employees and/or Federal contractors

□ 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.

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 an 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://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 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.	
☒	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.	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." 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

☒ Existing DoD Information Systems

☒ Other Federal Information Systems

☐ Databases

☐ Commercial 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

☒ Face-to-Face Contact

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

☒ 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 EDHA 09

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. N1-330-11-3

(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 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.

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.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

☐ Biometrics
☒ Citizenship
☒ Driver's License
☒ Employment Information
☒ Home/Cell Phone
☒ Mailing/Home Address
☒ Military Records
☒ Official Duty Address
☐ Passport Information
☒ Place of Birth
☐ Race/Ethnicity
☐ Records
☒ Work E-mail Address

☒ Birth Date
☒ Disability Information
☒ Education Information
☐ Financial Information
☒ Law Enforcement Information
☒ Marital Status
☐ Mother's Middle/Maiden Name
☒ Official Duty Telephone Phone
☒ Personal E-mail Address
☒ Position/Title
☒ Rank/Grade
☐ Security Information
☒ If Other, enter the information in the box below

☒ Child Information
☒ DoD ID Number
☐ Emergency Contact
☒ Gender/Gender Identification
☐ Legal Status
☒ Medical Information
☒ Name(s)
☒ Other ID Number
☒ Photo
☒ Protected Health Information (PHI)[1]
☐ Religious Preference
☒ Social Security Number (SSN) *(Full or in any form)*

Other PII collected includes: National Provider Identifier (NPI) number; and Electronic Data Interchange Personal Identifier (EDIPN) number pulled from the provider's Common Access Card (CAC).

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Approved 8/31/2017. CCQAS is not required under DoD's current SSN Reduction plan to complete a SSN Justification Memo as directed by the signed 21 November 2012 Memorandum for Tricare Management Activity Privacy Office.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

2. c (2) Law Enforcement, National Security, Credentialing and 2.c (5) Confirmation of Employment Eligibility. Federal statute requires that all persons employed within the United States must provide a SSN or comparable identifier to prove that he or she is eligible to work for or with the government of the United States.

2. c. (8) Computer Matching. CCQAS receives one data element, the National Provider Identifier, from the Defense Medical Human Resources System- internet (DMHRSi). Health care provider information in DMHRSi currently uses SSNs as the personal identifier. Until DMHRSi, from which CCQAS obtains data using SSNs, has been modified/upgraded to replace SSNs with DoD Electronic Data Interchange Personal Identifiers, CCQAS will need to continue using SSNs for verification that an individual's CCQAS records are accurately updated with information obtained from DMHRSi as specified by the DMHRSi Justification for the Use of the Social Security Number Memorandum for Record in the Defense Medical Human Resources System, Internet (DMHRSi); DITPR ID 130, signed by DMHRSi Project Officer, SDD/Clinical Support Program Management Office, Defense Health Agency (DHA).

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

Although the need to continue the use of SSNs with CCQAS is significant, the following steps have been taken to reduce vulnerability of SSN within CCQAS:
1) After the deployment of CCQAS version 2.10, CCQAS and v2.14 now called CCQAS generated forms include only the last four digits of SSN's.
2) CCQAS uses role-based access to control visibility of SSN to a limited subset of "trusted users" such as Credentialing Officers.
3) No data is allowed to leave CCQAS via an interface or messaging system because it is protected medical quality assurance information under 10 U.S.C 1102, Confidentiality of Medical Quality Assurance Records; Qualified Immunity for Participants.
4) CCQAS is not a "public" system accreditation and security profile, and ensures Information Assurance Vulnerability Alerts (IAVAs) are applied in a timely manner.
5) CCQAS is centrally hosted at Defense Information Systems Agency (DISA) facilities to ensure physical access to the system is limited.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☒ No

In order for a health care provider to practice at an MTF, he or she must undergo the credentialing process that entails an extensive verification of the provider's qualifications to perform the requested medical procedures. The SSN is the essential personal identifier to assure that the information for an individual that is obtained from non-DoD agencies and organizations is tied to the correct MHS provider within CCQAS. For example, the SSN must be used when confirming and verifying education with a particular institute (there are over one hundred accredited U.S. medical schools), and/or background checks with the police departments (there are over 10,000 local police departments in the U.S.). As required by DHA-PM 6025.13, Clinical Quality Management in the Military Health System, evidence of qualifying educational degrees must be verified through primary sources. Organizations like the National Student Clearinghouse require SSNs for identification. With regard to background checks with police departments, these are required in accordance with DoD Instruction 1402.5, "Criminal History Background Checks on Individuals in Child Care Services." Therefore, continued use of the SSN within CCQAS is critical to support the credentialing process until such a time when all non-DoD agencies and organizations that need to be contacted for credentials verification purposes cease to use SSNs for identification purposes.

b. What is the PII confidentiality impact level[2]? ☐ Low ☒ Moderate ☐ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

☒ Cipher Locks
☒ Combination Locks
☒ Key Cards
☒ Security Guards
☐ Closed Circuit TV (CCTV)
☒ Identification Badges
☐ Safes
☐ If Other, enter the information in the box below

CCQAS physically resides on servers located in DISA facilities in San Antonio, Texas with off-site back-up facilities in Oklahoma City, Oklahoma. Physical controls are consistent across all facilities in which the system data is used and maintained.

(2) Administrative Controls. *(Check all that apply)*

☒ Backups Secured Off-site
☒ Encryption of Backups
☒ Methods to Ensure Only Authorized Personnel Access to PII
☒ Periodic Security Audits
☒ Regular Monitoring of Users' Security Practices
☐ If Other, enter the information in the box below

Because CCQAS is maintained in a secure DISA environment, all controls and fail-safe measures are governed by DISA policies and procedures. DISA performs daily incremental and weekly full backups. The following backup retentions apply: daily incremental backups kept for two weeks, weekly full backups kept for five weeks. Daily incremental backups are intended for local recovery use and will not be stored off-site. Weekly full backups are intended for remote disaster recovery use and will be maintained off-site for the duration of the retention period. Failed backup processing will be reported on a daily basis to the applicable System Administrator for resolution and restarted as required.

CCQAS maintains audit logs of the use of each authorized user for every module used or opened. The audit log maintains the record of access and the dates that the user was in the module, by functional area so that if there were a breach of data, it would be visible to system administrators. Incremental file backup and archived file storage is provided by the DISA facility site in Oklahoma City, OK.

The system maintains a user's manual that will be updated along with each new release. As part of the guidelines for employment within the Defense Health Agency, users must comply with HIPAA regulations and as such, take annual training.

(3) Technical Controls. *(Check all that apply)*

☐ Biometrics ☒ Common Access Card (CAC) ☒ DoD Public Key Infrastructure Certificates

☒ Encryption of Data at Rest
☒ Encryption of Data in Transit
□ External Certificate Authority Certificates
☒ Firewall
☒ Intrusion Detection System (IDS)
☒ Least Privilege Access
☒ Role-Based Access Controls
□ Used Only for Privileged (Elevated Roles)
☒ User Identification and Password
☒ Virtual Private Network (VPN)
□ If Other, enter the information in the box below

All users must have either a Common Access Card (CAC) or Personal Identification Verification (PIV) card to access CCQAS. These access cards are often combined with a Military Identification (ID), Department of Defense ID, or other Federal or state agency ID that is required for access to the facility and/or position.

Data in transit that is transmitted/received between the application servers and the end user is encrypted with SSL/TLS over HTTPS. Data in transit between DMHRSi and CCQAS is inside the DISA facility and is not encrypted.

Although CCQAS hosts a web site at https://ccqas.csd.disa.mil, it is not publicly accessible and is protected within the DISA DMZ and by access control restrictions.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

CCQAS is susceptible to the same privacy risks, inherent in any system collecting, using, and sharing PII/PHI. If this system is not properly protected, then the PII/PHI contained therein could be accessed by unauthorized individuals through various methods, such as data interception, unauthorized access, internal threats, and external threats.

System planning for CCQAS has included threat analysis and vulnerability assessments to support operational telecommunications requirements, and to establish resource allocation priorities and satisfy requirements for countermeasures. Authentication methods are used to defend against imitative communications deception and to authenticate stations, transmissions and communicators.

All PII data has been evaluated with regard to the implications of it being lost, stolen, or disclosed. All data in CCQAS is protected from disclosure by 10 U.S.C. 1102 and is physically protected by strong security safeguards in place at DISA.

The data is considered Moderate Impact and is not released to the public. Moderate Impact PII information can be retrieved from CCQAS via standard and ad hoc reports and saved on mobile computing devices and removable electronic media, but users are cautioned against doing so during CCQAS training, in user manuals, and via other communications. If such data needs to be retrieved for reporting purposes, users know to keep the data protected by using encryption, passwords, and other safeguard practices.

All software development activities for the CCQAS system occur in a closed, secure environment. All personnel who develop, operate, and maintain the system require a Public Trust or Secret Clearance, depending on the activity being performed. Access to the system’s software and hardware is controlled based on an individual’s need to know and job responsibilities.

The data in CCQAS is tightly controlled and strict oversight is in place to assure its integrity, accuracy, currency, and relevance. The Office of the Surgeon General-level personnel oversee what their respective MTF personnel are entering into the system and work with them on a daily basis to ensure that the data is accurate and of high quality. One of the major methods of ensuring the quality of the data is that certain types of information in a provider's credentials record must be primary source verified, meaning that a medical diploma or license will be verified with the issuing university or licensing board. This fact-checking must be done before a provider can report for duty at another facility.

Further, CCQAS follows 10 U.S.C. 1102 which requires Confidentiality of records and prohibits records disclosure and testimony.