



Administration &  
Management (J-1)

**DEFENSE HEALTH AGENCY**  
7700 ARLINGTON BOULEVARD, SUITE 5101  
FALLS CHURCH, VIRGINIA 22042-5101

28 January 2025

MEMORANDUM FOR THE DEFENSE PRIVACY, CIVIL LIBERTIES, AND FREEDOM OF  
INFORMATION DIRECTORATE

THROUGH: Defense Health Agency (DHA), Privacy and Civil Liberties Office

SUBJECT: Justification for Use of Social Security Numbers (SSNs) – Centralized Credentials  
and Quality Assurance System (CCQAS), Department of Defense Information Technology  
Portfolio Repository (DITPR) #136

This memorandum is written to satisfy the requirement established by Department of Defense Instruction (DoDI) 1000.30: “Reduction of Social Security Number (SSN) Use Within DoD,” dated August 1, 2012, requiring justification for the collection and use of the SSN in the Centralized Credentials and Quality Assurance System (CCQAS).

CCQAS is a Department of Defense (DoD) DHA Government-Off-the-Shelf (GOTS) web-based application that supports Credentialing, Privileging, and Healthcare Risk Management of Active Duty, Reserve, Guard, Civil Service, contractor, and volunteer direct health care providers within the Military Health System (MHS). The system is accessible to professional medical staff managers and health care providers worldwide as a data repository, reporting, and management tool that consists of the following key functional modules: Credentialing, Privileging, Risk Management, Adverse Actions, and Reporting.

The applicable system of record for CCQAS is EDHA 09, Medical Credentials/Risk Management Analysis System (CCQAS) (November 18, 2013, 78 FR 69076).<sup>1</sup> CCQAS is subject to the Paperwork Reduction Act (PRA) and possesses an active Office of Management and Budget (OMB) Control Number (0720-0071) through 10/31/2025.

Before a health care provider can practice at an MTF, he or she must undergo a credentialing process that entails an extensive verification of the provider’s qualifications to perform the requested medical procedures. Because this credentialing process is dependent upon information obtained via cooperation with thousands of non-DoD agencies and organizations (there are over 10,000 local U.S. police departments and over 100 accredited U.S. medical schools), continued use of an individual’s SSN as the primary personal identifier is essential.

Continued use of SSNs by CCQAS meets the Acceptable Use Cases established by DoDI 1000.30, 2.c.(2) Law Enforcement, National Security, and Credentialing, 2.c.(5) Confirmation of Employment Eligibility, and 2.c.(8) Computer Matching:

---

<sup>1</sup> <https://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570674/edha-09/>

2.c.(2) Law Enforcement, National Security, and Credentialing. Almost every law enforcement application available to Federal, State, and local law enforcement and other criminal justice agencies reports and tracks individuals, and makes application information available to other agencies, through the use of the SSN. This includes, but is not limited to, checks of the National Crime Information Center; State criminal histories; and Federal Bureau of Investigation records checks.

2.c.(5) Confirmation of Employment Eligibility. Federal statute requires that all persons employed within the United States provide an SSN or comparable identifier to prove that they are eligible to work for or with the U.S. Government. Any system that deals with employment eligibility may contain the SSN.

2.c.(8) Computer Matching. Systems, processes, or forms that interact with other Government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information. These applications shall be rigorously scrutinized to determine the availability of some other means for conducting these transactions.

CCQAS employs rigorous physical, administrative, and technical safeguards to protect sensitive data, including personally identifiable information (PII) and SSNs, from unauthorized use and/or disclosure. Any form(s) generated by CCQAS only include the last four digits of an individual's SSN. Additionally, role-based access controls are employed to ensure that visibility of SSN data is limited to a subset of trusted users, such as Credentialing Officers. CCQAS is not available to the general public and only accessible to those individuals who possess a valid Common Access Card (CAC) or Personal Identification Verification (PIV) card and a valid need-to-know. Other layers of security (physical, administrative, and technical) are in place at the Defense Information Systems Agency (DISA) host facility to protect sensitive data collected by CCQAS.

The Clinical Support (CS) Program Office point of contact is Ms. Donna Kays, who may be contacted at (202) 327-0537 and [donna.j.kays.civ@health.mil](mailto:donna.j.kays.civ@health.mil).

---

Ms. Donna Kays  
CCQAS Product Manager  
(202) 327-0537  
[donna.j.kays.civ@health.mil](mailto:donna.j.kays.civ@health.mil)

---