DEPARTMENT OF HEALTH AND HUMAN SERVICES

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

CROWNWeb
Consolidated Renal Operations in a Web Enabled Network

Form Approved
OMB No. 0000-0000

CROWNWeb Authentication Service (CAS) Account Form

Page 1 of this form must be NOTARIZED for New User Accounts using the same identification information that you, the Applicant, supplied to your local Security Administrator. All Fields marked with an asterisk (*) are required.

*** Type of Request:**	□ **Create New User Account**	□ **Change User Account**	□ **Disable User Account**

*** Date Requested:** (mm/dd/yyyy)	*** CAS/CROWNWeb User ID:** (for Change/Disable)

Personal Information

Prefix:	*** First Name:**	**Middle Name:**	*** Last Name:**	**Suffix:**

*** Personal Address 1:**	*** City:**	*** State:**
Personal Address 2:	*** Zip Code 1:**	**Zip Code 2:**

*** Birthdate:** (mm/dd/yyyy)	**Home Phone:** **( )**	**Cell Phone:** **( )**	

Identification Information

Applicant must provide **one of the following 4 types** of Photo Identification: Driver's License, State Issued ID Card, Passport, Permanent Resident Card

*** Identification Used:** (specify one of the 5 types)	*** ID Number:** (specific to the ID)	*** Issued By:** (state, country)	*** Expiration Date:** (mm/dd/yyyy)

Business Information

*** Business Name:**	*** Email Address:**	
*** Job Title:**	*** Phone Number:** **( ) Ext:**	**Fax Number:** **( )**
*** Business Address 1:**	*** City:**	*** State:**
Business Address 2:	*** Zip Code 1:**	**Zip Code 2:**
*** Your Manager's Name:**	*** Your Manager's Email Address:**	
*** Your Manager's Job Title:**	*** Your Manager's Phone Number:** **( )**	

Required Signatures

My statements on this form are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of Title 18, United States Code). I agree to the terms and conditions documented on Page 3 of this form.	*** Signature of Applicant:**	*** Date:** (mm/dd/yyyy)
Authorization: I acknowledge that our organization is responsible for all resources to be used by the Applicant/User identified above and that requested accesses are required to perform his or her duties. I have reviewed and verified the information supplied is accurate and appropriate. I understand that any change in employment status or access needs must be reported immediately to both (1) our designated Security Administrator and (2) the Helpdesk.	*** Signature of Manager:**	*** Date:** (mm/dd/yyyy)

Notarization of Applicant's Identity

*** Date:** (mm/dd/yyyy)	*** Notary Expiration Date:** (mm/dd/yyyy)
*** Notary Public Seal or Stamp:**	I attest that the Identification Information supplied by the Applicant on page 1 of this form and presented to me confirms the identity of the Applicant. *** Signature of Notary Public:**

DEPARTMENT OF HEALTH AND HUMAN SERVICES

CMS CENTERS for MEDICARE & MEDICAID SERVICES

CROWNWeb
Consolidated Renal Operations in a Web Enabled Network

Form Approved
OMB No. 0000-0000

CROWNWeb Authentication Service (CAS) Account Form

Page 2 of this form does NOT require notarization. All Fields marked with an asterisk (*) are required.

CROWNWeb Roles and Scope

*** System Access Required for the Applicant's Job Role:** Complete ONE column only with the guidance of your Manager

□ Dialysis Facility	**□ ESRD Network**	**□ CMS Employee**	**□ System Administrator (SA) and Other Roles**
CMS Medicare Provider Number (CMS Certification Number): **Affiliated with ESRD Network #:**	**ESRD Network #:**	**Office:** **Group:** **Division:**	**Contract(s):** **CMS PO:**
Select at least one role: **□ Facility Viewer** **□ Facility Editor** **□ Facility Security Administrator**	Select at least one role: **□ Network Viewer** **□ Network Patient Editor** **□ Network Facility Editor** **□ Network Security Administrator**	Select at least one role: **□ CMS Viewer** **□ CMS Editor** **□ CMS Security Administrator**	Select at least one role: **□ CAS SA** **□ CROWNWeb SA** **□ Helpdesk** **□ Third Party Submitter**
Additional Scope Required Over the Following Facilities: Provide the Medicare Provider Number for each; if more than 8, specify in blocks to the right. 1. 5. 2. 6. 3. 7. 4. 8.			
I have approved the CROWNWeb Roles and Scope for the Applicant:	*** Signature of Manager:**		*** Date:** (mm/dd/yyyy)

For Internal Use Only – Do Not Complete This Section if You are the Applicant or Manager

This section to be completed by the Security Administrator and Helpdesk. All Fields marked with an asterisk (*) are required.

*** Designated Security Administrator (SA):**	*** SA Phone Number:** ( )	*** SA Email Address:**

*** Applicant CAS/CROWNWeb User ID:**	*** Account Creation Date:** (mm/dd/yyyy)	*** Account Activation Date:** (mm/dd/yyyy)	**□ Training** **□ Production**

Helpdesk Reason(s) for Account Activation Denial:	**□ Missing required * information** **□ Roles and/or scope** **□ Other:** (specify here)	**□ Notarization** **□ Information Mismatch Between CAS Form and CAS Account**	**□ Not an original form**

INSTRUCTIONS AND FORM ROUTING:

- For Type of Request = **Create New** User Account: The Applicant and Manager must complete all required information on pages 1 and 2 of the form. The Applicant must have page 1 of the original form notarized, and then provide original pages 1 and 2 to his or her designated Security Administrator (SA). If you do not know who your SA may be, please check with your Manager; or call the QualityNet Help Desk on 1-866-288-8912. If the SA is not co-located with the Applicant, the Applicant will mail pages 1 and 2 of the original form (and only their form) to the SA in a tamper-proof package by United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal Systems Security to transmit this form electronically using email, the Internet, or unsecured FAX. The Applicant may retain a copy of the original form for his or her personal records.
- Upon receipt of pages 1 and 2 of the original form, the designated Security Administrator (SA) will create a new CAS/CROWNWeb account for the Applicant. The SA will mail pages 1 and 2 of the original form to the Helpdesk. All forms will be mailed in tamper-proof packaging using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal Systems Security to transmit any form(s) electronically using email, the Internet, or unsecured FAX. The SA shall NOT retain a copy of this form for any purpose.
- Upon receipt of pages 1 and 2 of the original form, the Helpdesk will verify that the form (1) is original, (2) is complete, (3) contains either the raised Notary seal or the Notary stamp with Notary license number, and (4) the required information entered into CAS by the designated SA matches the required information on the original form. If all 4 of these criteria are met, the Helpdesk will activate the Applicant's account, then store the original form as required by law. The account cannot be activated if one or more of the 4 criteria are not met; in this case the Helpdesk will advise the user and the SA of the action and the reason via a CAS system-generated email.
- For Type of Request = **Change** User Account: Specify CAS/CROWNWeb User ID and Name, complete all areas on pages 1 and 2 which require changes, obtain Applicant signature/date on page 1, and Manager signatures/dates on both pages 1 and 2. Notarization is not required except for a change in the user's name (any name field).
- For Type of Request = **Disable** User Account: Specify CAS/CROWNWeb User ID and name, obtain Manager signature/date on page 1 (Manager signature can be initially waived if the request involves a time-sensitive employee termination, but must subsequently be obtained within one business day). Notarization is not required.

DEPARTMENT OF HEALTH AND HUMAN SERVICES

CENTERS for MEDICARE & MEDICAID SERVICES

CROWNWeb

Consolidated Renal Operations in a Web Enabled Network

Form Approved
OMB No. 0000-0000

CROWNWeb Authentication Service (CAS) Account Form

CROWNWEB DATA SUBMISSION STATEMENT

Every CROWNWeb system user agrees, based on his or her best knowledge, information, and belief, that the data they submit to CMS is accurate, complete, and truthful.

PRIVACY ACT STATEMENT

The information on pages 1 and 2 of this form is collected and maintained under the authority of Title 5 U.S. Code, Section 552a(e)(10) (The Privacy Act of 1974). This information is used for assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by the statute, except in limited circumstances.

The information you furnish on page 1 of this form will be maintained by CMS in the CROWNWeb Authentication Service (CAS) application and the original form will be maintained by the QualityNet Helpdesk. The data may be disclosed as a routine use disclosure under the routine uses established for this system as published at 59 FED.REG.41329 (08-11-94) and as CMS may establish in the future by publication in the Federal Register.

Furnishing the information on this form is voluntary. However, if you do not provide this information, you may not be granted access to CMS computer systems.

SECURITY REQUIREMENTS FOR USERS OF CMS COMPUTER SYSTEMS

CMS uses computer systems that contain sensitive information to carry out its mission. Sensitive information is any information which the loss, misuse, or unauthorized access to, or modification of could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. To ensure the security and privacy of sensitive information in Federal computer systems, the Computer Security Act of 1987 requires Federal agencies to identify sensitive computer systems, conduct computer security training, and develop computer security plans. CMS maintains a system of records for use in assigning, controlling, tracking, and reporting authorized access to and use of CMS's computerized information and resources. CMS records all access to its computer systems and conducts routine reviews for unauthorized access to and/or illegal activity.

Anyone with access to CMS Computer Systems containing sensitive information must abide by the following:

- Do not disclose or lend your CAS/CROWNWeb ACCOUNT USER ID and/or PASSWORD to someone else. They are for your use only and serve as your "electronic signature". This means that you may be held responsible for the consequences of unauthorized or illegal transactions executed under your account.
- Do not browse or use CMS data files for unauthorized or illegal purposes.
- Do not use CMS data files for private gain or to misrepresent yourself or CMS.
- Do not make any disclosure of CMS data that is not specifically authorized.
- Do not duplicate CMS data files, create extract files of such records, remove or transmit data unless you have been specifically authorized to do so.
- Do not change, delete, or otherwise alter CMS data files unless you have been specifically authorized to do so.
- Do not make copies of data files, with personal identifiable data, or data that would allow individual identities to be deduced unless you have been specifically authorized to do so.
- Do not intentionally cause corruption or disruption of CMS data files.

A violation of these security requirements could result in termination of CMS systems access privileges. In addition, Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system for illegal activities.

If you become aware of any violation of the above security requirements or suspect that your CAS/CROWNWeb account User ID and/or Password may have been compromised, you must immediately report that information to your component's designated Security Administrator (SA) and immediately contact the QualityNet Helpdesk at 1-866-288-8912 (qnetsupport@ifmc.sdps.org) to report the actual or potential security incident.

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information is 0000-0000. The time required to complete this information collection is estimated to average 20 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, complete the form, and review the information collection (this does not include the Notarization activity for new user accounts as required on page 1). If you have any comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: The Centers for Medicare and Medicaid Services, Attention: PRA Reports Clearance Officer, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.