DEPARTMENT OF HEALTH AND HUMAN SERVICES

CMS CENTERS for MEDICARE & MEDICAID SERVICES

QualityNet Identity Management System (QIMS) Account Form

Account Information — Part A

Specify the type of account that is being requested. If requesting a Security Official Account this form must be signed by a Notary of the Public who has satisfactorily proofed the identity of the individual.

*** Type of Request:**	☐ **Create New User Account**	☐ **Create Security Official Account**
	☐ **Facility** ☐ **Contractor** ☐ **Network** ☐ **CMS** ☐ **Manager** ☐ **Provider** ☐ **QIO**	☐ **SA1 (Top Level) [CMS, IT Contractor]** ☐ **SA2 (Mid-Level, Network or QIO)** ☐ **SA3 (Lowest Level) [Facility, Provider, organizational level]**
*** Date Requested:** (mm/dd/yyyy)	*** QIMS User ID:** (for Change/Disable/Enable)	

Personal Information

(Per NIST 800-63, Table 3, Level 3 the applicant must be seen in person and provide a government issued picture ID such as Drivers License with current address or Passport with nationality)

Prefix:	*** First Name:**	*** Middle Name:**	*** Last Name:**	**Suffix:**
*** Personal Address 1:**		*** City:**	*** State:**	
Personal Address 2:		*** Zip Code 1:**	**Zip Code Extension:**	*** Birth date:** (mm/dd/yyyy)
*** Business Phone:**		*** Cell/2nd Phone:**	***Business E-mail Address** (if none use personal e-mail address)	
Extension:		**Extension:**		
*** Government Identification Used:** (specify type)		*** ID Number:** (specific to the ID)		
*** Issued By:** (state, country)		*** Expiration Date:** (mm/dd/yyyy)		

Business Information

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

Signatures

My statements on this form are true, complete, and correct to the best of my knowledge 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 5 of this form.	***Signature of Applicant**	*** Date:** (mm/dd/yyyy)

QualityNet Identity Management System (QIMS) Account Form

Account Information (continued) — Part A

Authorization: I acknowledge that our organization is responsible for all resources to be used by the Applicant/User identified on Page 1 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 Official and (2) the Help Desk.	*** Signature of Manager:**	*** Date:** (mm/dd/yyyy)
Validation: I am attesting to the fact, that I have vetted the identification of the applicant requesting access to QIMS. The individual has provided the proper credentials as required per "NIST 800-63 Table 3, Level 3" and I have properly identified the credential used in the "Identification Used" section. By doing so, I am attesting to the fact that I properly vetted the identity of the applicant and he/she is in fact, the applicant requesting access. I understand that any change in name, employment status or access needs must be reported immediately to both (1) our designated Security Official and (2) the Help Desk.	*** Signature of Identity Vetting Official:** (Security Official)	*** Date:** (mm/dd/yyyy)
*** Printed Name of Notary** (* Required for Security Official account only)	*** Signature of Notary**	***Date:** (mm/dd/yyyy)
***Notary Seal/Stamp**		

***Application(s) to be accessed once approved**	☐ **QIMS** ☐ **MIS** ☐ **SDPS** ☐ **QIES** ☐ **QMIS** ☐ **QualityNet.org** ☐ **PQRI** ☐ **ESRD/CROWNWeb**		
2nd Factor Credential Required? (to be filled out by the Security Official)	**Yes** ☐ **No** ☐		
Preferred 2nd Factor Contact (select one):	**Primary**	**Secondary**	**Secondary**
(Only select these options if your application requires Multi-Factor Authentication)	☐ **Business Phone** ☐ **Cell/ 2nd Phone**	☐ **Business Phone** ☐ **Cell/2nd Phone**	☐ **Business Phone** ☐ **Cell/2nd Phone**
Reason(s) for CROWNWeb account Activation Denial		☐ **Missing required * information** ☐ **Notarization** ☐ **Roles and/or scope**	

QualityNet Identity Management System (QIMS) Account Form

Part B of this form applies to CROWNWeb only. All Fields marked with an asterisk (*) are required.

CROWNWeb Roles and Scope — Part B

*** 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	☐ Other Roles
CMS Medicare Provider Number (CMS Certification Number):	**ESRD Network #:**	**Office:** **Group:** **Division:**	**Contract(s):** **CMS COTR:**
ESRD Network Affiliation #:			
Select at least one role: ☐ **Facility Viewer** ☐ **Facility Editor** ☐ **Facility Administrator**	**Select at least one role:** ☐ **Network Viewer** ☐ **Network Patient Editor** ☐ **Network Facility Editor** ☐ **Network Administrator**	**Select at least one role:** ☐ **CMS Viewer** ☐ **CMS Editor** ☐ **CMS Administrator**	**Select at least one role:** ☐ **Third Party Submitter for Batch** ☐ **CROWNWeb System Administrator**

Facility Scope

If the Applicant requires and is approved for Roles and Scope over more than ONE dialysis facility, a separate Part B form will be filled out for each facility to which access is required. All requests for additional Facility Scope must follow the SPECIAL ROUTING INSTRUCTIONS FOR ADDITIONAL FACILITY SCOPE on Page 4 of this form.

CMS Medicare Provider/CCN#	NW #	Facility Name	Name of Facility Contact	Contact Phone	Contact E-mail

Specify States and Territories Within Your Jurisdiction:

I have authorized the CROWNWeb Roles and Scope, including any Additional Facility Scope for the Applicant	*** Signature of Applicant's 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. All Fields marked with an asterisk (*) are required.

*QIMS Security Official (SO) Name:	* SO Phone Number:	* Date: (mm/dd/yyyy)

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

*** Designated Security Official (SO):**

QualityNet Identity Management System (QIMS) Account Form

Instructions and Form Routing

INSTRUCTIONS AND FORM ROUTING for Part A:

For Type of Request = **Create New** User Account: The Applicant will fill in the on line registration form and submit it to the End User Manager (EUM) who will approve the new user for account creation and identity verification hereafter called "identity proofing". The Applicant will take part A of this form to the appointed Security Official (SO) where the Applicant will be required to perform Security Awareness Training and will undergo identity proofing. If the Applicant does not know who the assigned SO is, they can check with their EUM; or call the CROWN Help Desk at 1-888-ESRDHD1(1-888-377-3431) or send an e-mail to support@crownhelpdesk.com

- . The Applicant must provide the registration form to the SO in person so the SO can act as the Identity Proofer. The Applicant may retain a copy of the original request form for his or her personal records.
- Note: the End User Manager will be a pre-designated for the Facility, CROWN Help Desk, network, QIO or CMS activity that the Applicant is closest to.
- Choosing an endpoint for receipt of the 2nd factor PIN is key to accessing any application that works with Protected Healthcare Information (PHI) or Personally Identifiable Information (PII). Please select an option that is close to your computer workstation as you will want easy access to the PIN that is sent via your selected method of receipt.
- Upon receipt of part A of the original form, the designated SO will review the form to ensure it is complete and will then vet the user's identity using a currently valid government picture identification document that lists the applicants current home address, or a passport showing the applicants nationality per NIST 800-63, Table 3, Level 3 E-Authentication recommendations. The SO will enter his/her name, and signature where designated on Part A of the form.
- Once identity vetting is complete, the SO will verify that the person requesting an account has completed the required Security Awareness Training (SAT). The SO will then log into QIMS and ensure the new user account is set up and assign the account holder to the proper QIMS role(s). Once the account has been set up the SO will send a fax copy to the secure fax number at the CROWN Helpdesk and then mail the original form to the CROWN Helpdesk for mandated record keeping. All forms will be mailed in tamper-resistant packaging using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal security regulations to transmit any form(s) electronically; email, the Internet, unsecure transmission media, or any unsecured FAX.
- For Type of Request = **Create Security Official** Account: The Applicant will fill out the registration form, Print it out and take it to a Notary of the Public for Identity proofing.
- After the EUM has signed the form, ensured the SO Applicant has undergone Security Awareness Training and verified the information on the registration form is correct the SO will then log into QIMS and ensure the new user account is set up. The SO will then assign the account holder to the proper QIMS role(s). Once the account has been set up the SO will send a fax copy to the secure fax number at the CROWN Helpdesk and mail the original form to the CROWN Helpdesk for mandated record keeping. All forms will be mailed in tamper-resistant packaging using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal security regulations to transmit any form(s) electronically; email, the Internet, unsecure transmission media, or any unsecured FAX.

INSTRUCTIONS AND FORM ROUTING for Part B:

Upon receipt of the original Part B of this form:

- The EUM will review, approve and sign Part B of the form that is the application role request portion.
- Provisioning of application roles will be accomplished upon completion of any application related training by the SO or assigned local application system administrator following the QIMS User ID being activated.
- Note: the End User Manager will be a pre-designated for the Facility, Help Desk, network, QIO or CMS activity that the Applicant is closest to.
- The CROWN Helpdesk will verify that the each form is; (1) the original, (2) is complete, (3) the required SO information is complete. If all of these criteria are met, the Help Desk will store the original form as required by law. The account cannot be activated if one or more of these criteria are not met; in this case the IMS team will advise the user of the action and the reason via a QIMS system-generated email.

QualityNet Identity Management System (QIMS) Account Form

QUALITYNET DATA SUBMISSION STATEMENT

Every QualityNet 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 QualityNet Identity Management System (QIMS) and the original form will be maintained by the Identity Management Team. 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 QIMS 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 QIMS account User ID and/or Password may have been compromised, you must immediately report that information to your component's designated Security Official (SO) and immediately contact the QualityNet Helpdesk at 1-866-288-8912 (qnetsupport@sdps.org) to report the actual or potential security incident.