



## QualityNet Identity Provisioning System (QIPS) Account Form

You must apply for a QIPS Account using this form in order to access CROWNWeb; this form can be typed or printed neatly.

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

\* Type of Request:  Create New User Account  Change User Account  Disable User Account  Enable User Account

\* QIPS Role:  QIPS Regular User  Security Administrator  QIPS Support  CROWN Help Desk

\* Date Requested: (mm/dd/yyyy)

QIPS/CROWNWeb User ID: (\* for Change/Disable/Enable)

### 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 4 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: (and extension) 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: (and extension)

### 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 4 of this form.

**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 Help Desk.

### Notarization of Applicant's Identity

Notary must include Date of Notarization and Expiration Date of their term.

\* Date: (mm/dd/yyyy) \* Notary Expiration Date: (mm/dd/yyyy)

\* Notary Public Seal or Stamp: I, a Notary Public, attest that the Identification Information supplied by the Applicant on Page 1 of this QIPS Account Form and presented to me confirms the identity of the Applicant.  
\* Signature of Notary Public:



**QualityNet Identity Provisioning System (QIPS) Account Form**

Page 2 applies to CROWNWeb only and 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

<input type="checkbox"/> <b>Dialysis Facility</b>	<input type="checkbox"/> <b>ESRD Network</b>	<input type="checkbox"/> <b>CMS Employee</b>	<input type="checkbox"/> <b>Other Roles</b>
<b>CMS Medicare Provider Number (CMS Certification Number):</b>	<b>ESRD Network #:</b>	<b>Office:</b> <b>Group:</b> <b>Division:</b>	<b>Contract(s):</b>  <b>CMS PO:</b>
<b>ESRD Network Affiliation #:</b>			
Select at least one role: <input type="checkbox"/> <b>Facility Viewer</b> <input type="checkbox"/> <b>Facility Editor</b> <input type="checkbox"/> <b>Facility Administrator</b>	Select at least one role: <input type="checkbox"/> <b>Network Viewer</b> <input type="checkbox"/> <b>Network Patient Editor</b> <input type="checkbox"/> <b>Network Facility Editor</b> <input type="checkbox"/> <b>Network Administrator</b>	Select at least one role: <input type="checkbox"/> <b>CMS Viewer</b> <input type="checkbox"/> <b>CMS Editor</b> <input type="checkbox"/> <b>CMS Administrator</b>	Select at least one role: <input type="checkbox"/> <b>Third Party Submitter for Batch</b> <input type="checkbox"/> <b>CROWNWeb System Administrator</b>

**Additional Facility Scope**

If the Applicant requires and is approved for Roles and Scope over more than ONE dialysis facility, the following information is required for each of those additional facilities. If space for more than 8 facilities is needed, provide a separate typed sheet with all the required information below. All requests for Additional Facility Scope must follow the SPECIAL ROUTING INSTRUCTIONS FOR ADDITIONAL FACILITY SCOPE on Page 3 of this form.

	<b>CMS Medicare Provider/CCN #</b>	<b>NW #</b>	<b>Facility Name</b>	<b>Name of Facility Contact Person</b>	<b>Contact Phone</b>	<b>Contact Email</b>
1						
2						
3						
4						
5						
6						
7						
8						

<b>Authorization:</b> I acknowledge that my organization is responsible for all resources used by the Applicant/User and that the CROWNWeb Roles and Scope listed above are required to perform his or her duties. I understand that changes to Roles and Scope must be applied timely by the designated Security Administrator.	<b>* Signature of Manager:</b>	<b>* Date:</b> (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 Designated QIPS SA and CROWN Help Desk. All Fields marked with an asterisk (\*) are required.

<b>* QIPS Security Administrator (SA) Name:</b>	<b>* SA Phone Number:</b>	<b>* SA Email Address:</b>	
<b>* Applicant QIPS/CROWNWeb User ID:</b>	<b>* Account Creation Date:</b> (mm/dd/yyyy)	<b>* Account Activation Date:</b> (mm/dd/yyyy)	<input type="checkbox"/> <b>Training</b> <input type="checkbox"/> <b>Production</b>
<b>Help Desk Reason(s) for Account Activation Denial:</b>	<input type="checkbox"/> <b>Missing required * information</b> <input type="checkbox"/> <b>Notarization</b> <input type="checkbox"/> <b>Roles and/or scope</b>	<input type="checkbox"/> <b>Not an original form</b> <input type="checkbox"/> <b>Information Mismatch Between QIPS Form and QIPS Account</b> <input type="checkbox"/> <b>Other: (specify)</b>	



## QualityNet Identity Provisioning System (QIPS) Account 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 QIPS Account 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 QIPS Security Administrator (SA). If you do not know who your SA may be, please contact your Manager. 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 using the SECURE MAILING METHOD below. Only 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 QIPS Security Administrator (SA) will:
  - Create a new QIPS/CROWNWeb account for the Applicant
  - Print and attach the system-generated paperwork tag# to the original QIPS Account Form Pages 1 and 2
  - Complete the applicable fields in the "For Internal Use Only" section on Page 2
  - Within 1 day, mail Pages 1 and 2 with attached paperwork tag to the CROWN Help Desk using SECURE MAILING METHOD below
  - The SA will NOT retain a copy of the form Page 1 for any purpose, but he or she may optionally retain a copy of Page 2
- Upon receipt of Pages 1 and 2 of the original form, the CROWN Help Desk 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 QIPS by the designated SA matches the required information on the original form. If all 4 of these criteria are met, the CROWN Help Desk will activate the Applicant's account, and 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 CROWN Help Desk will advise the user and the SA of the action and the reason via a QIPS system-generated email.

#### **FOR TYPE OF REQUEST = CHANGE USER ACCOUNT**

- Complete Date Requested, Applicant QIPS/CROWNWeb User ID, Applicant's Name, all Manager items (Manager Name, Manager Job Title, Manager Email, Manager Phone Number) in the **Business Information** section, complete any other information on Page 1 which require change, then obtain Applicant and Manager Signatures with Dates on Page 1 only. Notarization is NOT required. If changes apply to Page 1 only, the QIPS SA will enter the changes into the QIPS application, print and attach the system-generated paperwork tag#, then mail with Page 1 of the original form to the CROWN Help Desk using the SECURE MAILING METHOD below.
- If the changes only apply to CROWNWeb Roles and Scope on Page 2, the QIPS SA will enter the changes into the CROWNWeb application; no QIPS Account Form shall be mailed to the CROWN Help Desk because no system-generated paperwork tag# is created.

#### **FOR TYPE OF REQUEST = DISABLE OR ENABLE USER ACCOUNT**

- Complete Date Requested, Applicant QIPS/CROWNWeb User ID, Applicant's Name, all Manager items (Manager Name, Manager Job Title, Manager Email, Manager Phone Number), then obtain the Manager's Signature with Date on Page 1 only. The Manager's Signature can be initially waived if a disable request involves a time-sensitive employee termination, but must be subsequently obtained within one business day. Notarization is not required. The QIPS SA will enable or disable the account in the QIPS application, print and attach the system-generated paperwork tag#, then mail with Page 1 of the original form to the CROWN Help Desk using the SECURE MAILING METHOD below.

#### **SPECIAL ROUTING INSTRUCTIONS FOR ADDITIONAL FACILITY SCOPE**

- If the Applicant is approved for Roles and Scope over more than ONE dialysis facility in the same ESRD Network as the first facility he or she was granted Roles and Scope over, Pages 1 and 2 of the original signed QIPS Account Form must be mailed to the QIPS Security Administrator (SA) at the Network level using the SECURE MAILING METHOD below. The Network level SA will then process the form and route as usual.
- If the Applicant is approved for Roles and Scope over ONE OR MORE dialysis facilities in different ESRD Network(s) as the first facility he or she was granted Roles and Scope over, Pages 1 and 2 of the original signed QIPS Account Form must be mailed to the CMS Security Administrator for approval and processing. Using the SECURE MAILING METHOD below, send QIPS Account Forms which span multiple Networks to: The Centers for Medicare and Medicaid Services, ISG CROWNWeb Team, Mail Stop S3-02-01, 7500 Security Blvd., Baltimore, MD 21244-1850.

#### **SECURE MAILING METHOD FOR ALL QIPS ACCOUNT FORMS**

- All QIPS Account Forms must be mailed in a tamper-proof envelope/package using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal Systems Security to transmit this form electronically by any electronic means using, but not limited to, any form of email, the Internet, or facsimile/FAX. Tamper-proof refers to any envelope/package which cannot be opened by unauthorized persons after being sealed, without exhibiting signs of such tampering.
- QIPS Account Forms which require the Applicant to mail the form to their designated QIPS Security Administrator (SA) (in order to create a new or change a current QIPS account) should be mailed as described directly above; this only applies if the QIPS SA is not co-located with the Applicant. Incomplete forms should NOT be mailed directly to the CROWN Help Desk because the form is invalid without processing by the Applicant's QIPS SA Applicant. All incomplete forms received by the CROWN Help Desk will be destroyed and the Applicant must start over.

#### **MAILING ADDRESS FOR COMPLETED QIPS ACCOUNT FORMS**

- After account creation or change in the QIPS application, the QIPS SA will mail original completed individual and/or batched QIPS Account Forms with corresponding paperwork tag #s in a timely manner using the SECURE MAILING METHOD described above to: CROWN QIPS Processing/CSC, P.O. Box 12238, Durham, NC 27709



## QualityNet Identity Provisioning System (QIPS) 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 the Centers for Medicare and Medicaid Service's (CMS) computerized information and resources. The Privacy Act prohibits disclosure of information from records protected by this statute, except in limited circumstances.

The information you furnish on Page 1 of this form will be maintained by CMS in the QualityNet Identity Provisioning System (QIPS), previously known as the CROWNWeb Authentication Service (CAS), and the original QIPS Account Form will be securely maintained by the CROWN Help Desk. 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 QIPS/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.

Any violation of these security requirements could result in the termination of your 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 QIPS/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 CROWN Help Desk at 1-888-ESRDHD1 (ESRDHD1@esrd.net) to report the actual or potential security incident.**

According to the Paperwork Reduction Act (PRA) 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 0938-1050. 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 time for 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 (CMS), Attention: PRA Reports Clearance Officer, 7500 Security Boulevard, Baltimore, Maryland 21244-1850.

**Please DO NOT MAIL QIPS Account Forms to this address.**