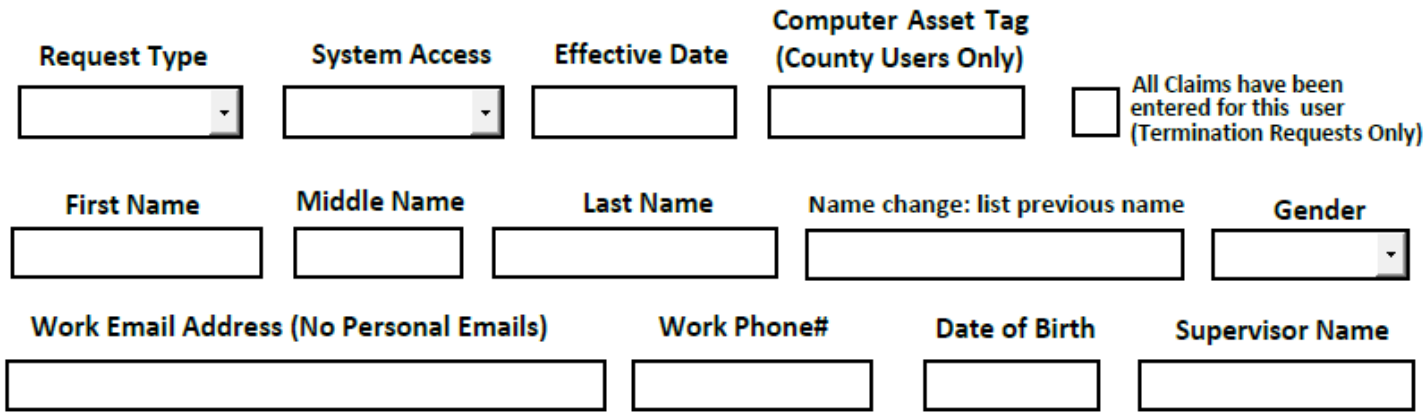
Instructions for Completing Access Request Form (ARF)



Request Type

1. **New User**- select if user has never had a County SmartCare account
2. **Modification**- select if you are requesting a change to the user's account. Be sure to type out your request in the Comments field on the ARF. **Summary of Policies (SOP) and Electronic Signature Agreement (ESA) forms not needed**
3. **Termination**- select if user no longer needs an account. This will terminate user completely. If you are only needing to remove/change your program, use the Modification request type. User signature is not needed for Termination requests. All claims must be entered for terminated staff **(SOP and ESA forms not needed)**
4. **Reactivation-** select if the user's account has been locked due to not logging in for more than 3 months
5. **Name Change-** select if user's legal name has changed. For all Clinical mental health and SUD staff, their ARF, their NPPES account and their license/registration name must match before the form will be processed
   NOTE: For name change requests, newly signed Electronic Signature Agreement (ESA) and Summary of Policies (SOP) forms must be submitted with the ARF
6. **Supervisor Change-** select this if the user's supervisor has changed. Type the current supervisor in the Supervisor Name field in Section I of the ARF
7. **Leave of Absence-** select if the user will be gone for an extended period, but will still need access to SmartCare when they return.

System Access- Select the systems you are requesting access to

Effective Date- This will be the employment date for a new user request or the date you want the changes to take effect

All Claims have been entered- Must be checked to confirm that all claims been entered into SmartCare

First, Middle last Name- User's Legal Name. If the user is an LPHA or Counselor/CPSS, the name on the ARF, their NPPES account and License must match before the form will be processed

- Leave Middle Name blank if user does not have a middle name
- This name must match the name on the user's CalMHSA LMS account for training verification

If Name Change- List user's previous full name so it can be looked up in SmartCare

Gender- choose one of the choices from the drop down

Work Email Address- type the user's work email. Personal emails will not be accepted

Work Phone- Type in the user's work phone# if applicable. Leave blank if user does not have a work phone#

Date of Birth- Enter user's date of birth

Supervisor Name- Enter supervisor's name

Select role below based on your job function

- ☐ Administrative Staff
- ☐ AOD Counselor
- ☐ Billing Staff
- ☐ Certified Peer Specialist
- ☐ Clinical Trainee
- ☐ Community Health Worker
- ☐ LPHA
- ☐ Medical Assistant
- ☐ Medical Records Technician
- ☐ MHRS
- ☐ ParaPro
- ☐ Prescriber
- ☐ Program Manger
- ☐ QA
- ☐ Registered Candidate
- ☐ Rendering Staff (No login for user. For billing only

Admin- Select for admin, data entry, clerical or front desk staff. May be used by some staff at the corporate office

AOD Counselor- Select if the user is a registered or certified SUD counselor

Billing– Select for any users that are part of your program's billing staff or complete billing related tasks

Certified Peer Support Specialist- Select if the user is a CPSS (must be certified)

Clinical Trainee- Select if the user is an unlicensed graduate student who is enrolled in a post-secondary educational program, that is required for the user to obtain licensure as a LPHA or a Licensed Mental Health Professional. A clinical trainee is also enrolled in a practicum program in agreement with their master's program/school that is part of their degree. Once that practicum placement ends and/or they graduate, they are no longer clinical trainees.

- **NOTE: Please also provide the name of the user's licensed clinical supervisor on the Current Supervisor field in Section I. This will be used as their cosigner for services**

Community Health Worker- Select for any user that is a community health worker Additional info can be found on the DHCS website

LPHA- Select for any user that has a Professional healthcare license. Examples include Physicians, Nurses, Psychologists, Social Workers, Marriage and Family Therapists or Professional Counselors

MHRS- choose if the user is a Mental Health Rehabilitation Specialist

MRT- Select for a user that is a Medical Records Technician. MRT's are admin staff that must view clinical records for the purpose of printing assessments, progress notes, etc

- **NOTE: An MRT form will need to be submitted with the ARF request**

Medical Assistant- choose for medical assistants

- **NOTE: Please also provide the name of the user's licensed clinical supervisor on the Current Supervisor field in Section I. This will be used as their cosigner for services**

ParaPro- Choose if the user is a Para Professional or other qualified provider

Prescriber- Select for users that will use the e-prescribing functions through CalMHSA Rx. Section III of the ARF must be completed and include the user's valid DEA# effective and expiration date

Program Manager- Select for Program Managers (Must provide license information).

QA- Select for users that are part of your programs Quality Assurance Team (QA).

- **NOTE: A QA form will need to be submitted with the ARF request**

Registered Candidate- Users who have completed their practicum placement or graduated from a Master's program and have submitted their application to BBS within 90 days of the date of their degree

Rendering Staff (No Login)- Select for clinical staff who bill for services, but will not need a login to the SmartCare system

Programs to be Added: ▾ **Programs to be Removed:** ▾

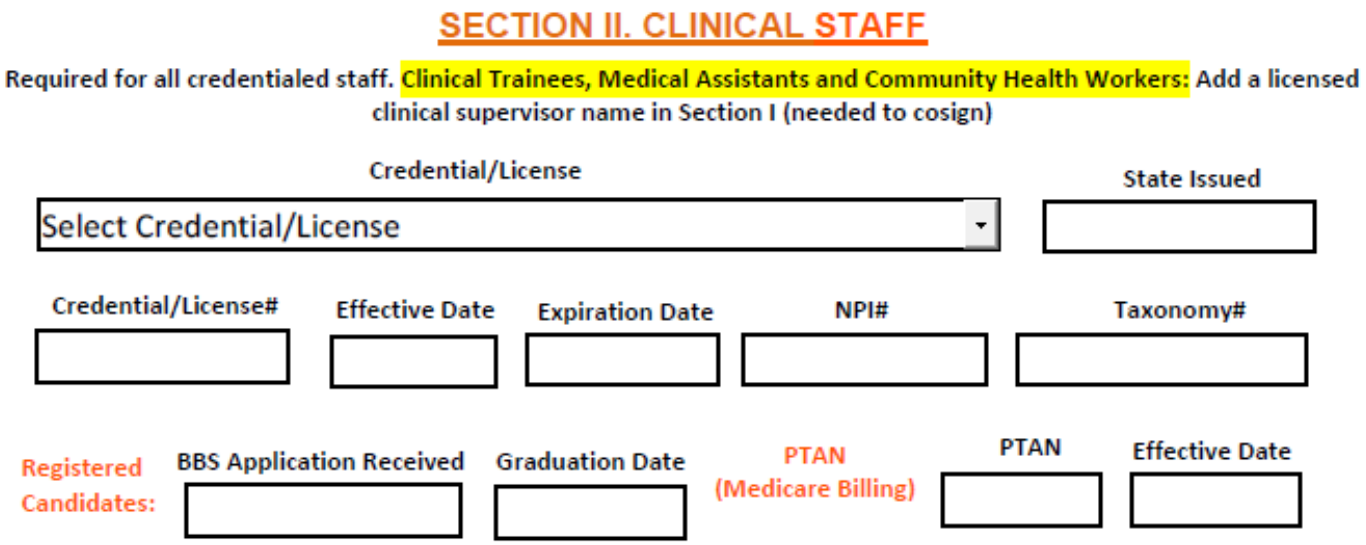
1. Language	Proficiency	2. Language	Proficiency	3. Language	Proficiency
	▾		▾		▾

Programs to be Added- Do not type in the facility numbers, legal entity numbers or units/subunits. Type in all requested program names the user needs access to. If more than one Legal Entity is being requested, an ARF will be needed for each additional Legal Entity

- **NOTE:** Each Legal Entity must have their own program a manager sign for attestation of information being provided on the ARF

Program to be removed- Do not type in the facility numbers, legal entity numbers or or units/subunits. Type in all requested program names the user needs to be removed from.

Language- Type in the language(s) the user speaks and choose the proficiency from the drop down next to each language field. If the user only speaks English, it should still be entered on the field with the proficiency



Select Credential/License- Select the specific license or counselor credential for the user.

- If the user is a clinical trainee or medical assistant, type the name of their licensed clinical supervisor in the supervisor field on Section I of the ARF
- All waivered staff are required to attach an approved waiver form to the ARF. Please contact QIMatters to start the inquiry process

State Issued- Type the state the credential/license is issued in

Credential/License#- Type the credential/license#

Effective Date- Type the credential/license effective date

Expiration Date- Type the credential/license expiration date

NPI#- Type the users NPI#. This can be found on their NPPES account or NPI registry

Taxonomy#- Type in the user's Taxonomy number. This can also be found on the users NPPES account or NPI registry. The user must have a state approved taxonomy number in relation to their credential/license. More information about this can be found in DHCS's DMC-ODS Billing Manual

Date BBS application Received- The date the BBS cashed the check/money order or the date BBS received the application via the tracking number on the certified mail receipt. Please also submit one of these verifications

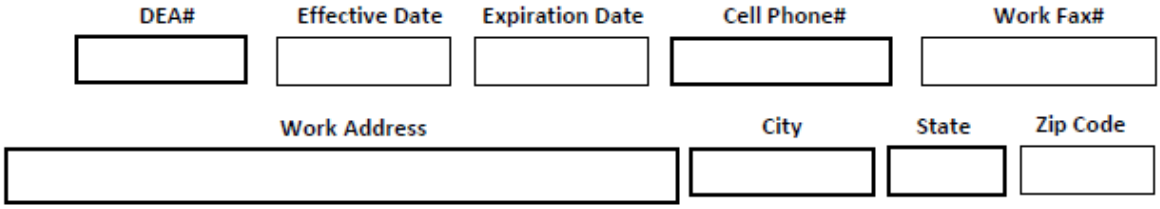
Graduation Date- Enter the graduation date for any users that are registered candidates. Please also submit a copy of the user's diploma or final transcript

PTAN# (Mental Health)- Provider Transaction Access Number. Enter the user's PTAN# which is assigned to healthcare providers by the Centers for Medicare & Medicaid Services (CMS). This number is used to process claims and payments under the Medicare program

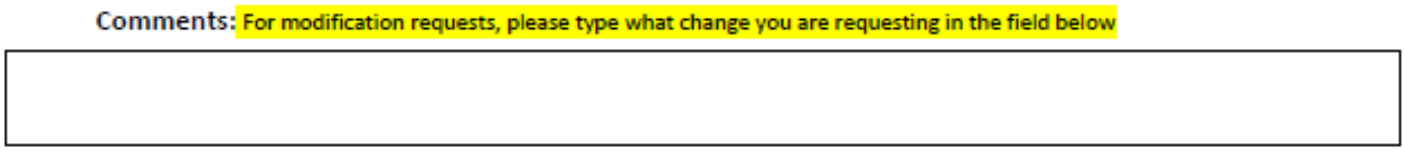
PTAN# Effective Date- Type in the PTAN# effective date

SECTION III. PRESCRIBER INFORMATION

Complete all fields for users who will be utilizing the e-prescribing function in CalMHSA Rx will need to provide the following information



DEA#, Effective Date, Expiration Date- Enter the user's DEA information
Cell Phone#- Enter the user's cell phone. This cannot be a work# or landline. It is for E-prescribing verification purposes (REQUIRED Field)
Work Fax#- Enter the work's fax# (REQUIRED Field)
Work Address, City State Zip Code- Enter the main work address the user works at

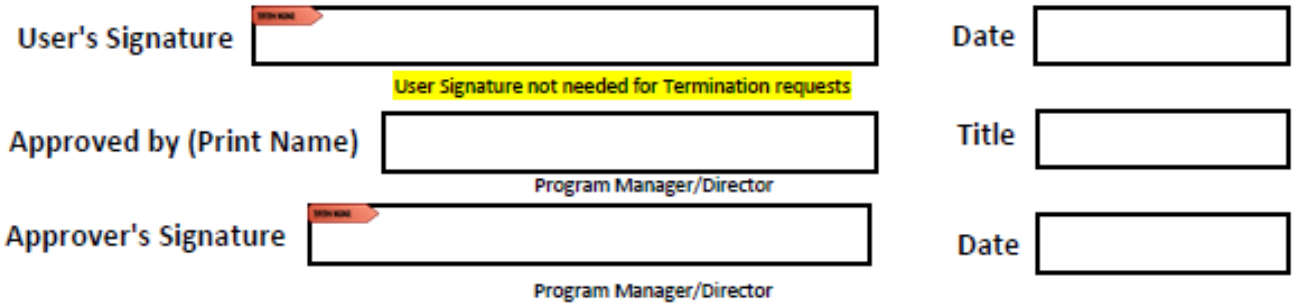


Comments- Please use this box to include the following information:

- What modifications are being requested to the user's SmartCare Account
- Add any additional information not collected on the form

SECTION IV. USER ACCESS AUTHORIZATION

Pursuant to the contractual agreement on file with the County of San Diego and as designated by my corporate office, I am authorizing access as noted above and affirm that I have personally reviewed the County's Summary of Policies with the above User:



Users and Approver's Signature- Signatures can be written or digitally signed

- The User's signature/date must be signed on or before the Approver's signature/date
- If digitally signed, the time stamp on the User's signature must be before the time stamp on the Approver's Signature
- This rule is the same for the Electronic Signature Agreement (ESA) and the Summary of Policies (SOP) forms attached to the ARF

HHSA Behavioral Health Services Management Information Systems

Access Request Form (ARF)

All forms must be TYPED and complete or will be returned.

Request a new Smart Care account by submitting the required approval forms to MIS help desk and BHSCredentialing. All new users must successfully complete the required SmartCare training modules after creating a CalMHSA LMS account. Once the training is finished, please notify the MIS help desk. Upon confirmation, the user's login credentials will be provided.

Per California Department of Health Care Services (DHCS) BHIN 22-032, County Behavioral Health Plans (which include Mental Health Plans and DMC-ODS Plans) are required to report data on its network providers using the "274" standard which is an Electronic Data Interchange selected by DHCS to ensure provider network data submitted to DHCS is consistent, uniform, and aligns with national standards. This information is used by DHCS to monitor whether our provider network is adequate to support the estimated need and demand for behavioral health services. Required provider information, inclusive of identifying information, is sent to DHCS on a monthly basis for these purposes.

SECTION I. USER INFORMATION

Request Type	System Access	Effective Date	Computer Asset Tag (County Users Only)	☐ All Claims have been entered for this user (Termination Requests Only)

First Name	Middle Name	Last Name	Name change: list previous name	Gender

Work Email Address (No Personal Emails)	Work Phone#	Date of Birth	Supervisor Name

Select role below based on your job function

- ☐ Administrative Staff
- ☐ AOD Counselor
- ☐ Billing Staff
- ☐ Certified Peer Specialist
- ☐ Clinical Trainee
- ☐ Community Health Worker
- ☐ LPHA
- ☐ Medical Assistant
- ☐ Medical Records Technician
- ☐ MHRS
- ☐ ParaPro
- ☐ Prescriber
- ☐ Program Manger
- ☐ QA
- ☐ Registered Candidate
- ☐ Rendering Staff (No login for user. For billing only

Programs to be Added:

Programs to be Removed:

1. Language	Proficiency	2. Language	Proficiency	3. Language	Proficiency

SECTION II. CLINICAL STAFF

Required for all credentialed staff. Clinical Trainees, Medical Assistants and Community Health Workers: Add a licensed clinical supervisor name in Section I (needed to cosign)

Credential/License	State Issued

Credential/License#	Effective Date	Expiration Date	NPI#	Taxonomy#

Registered Candidates:	BBS Application Received	Graduation Date	PTAN (Medicare Billing)	PTAN	Effective Date

SECTION III. PRESCRIBER INFORMATION

Complete all fields for users who will be utilizing the e-prescribing function in CalMHSA Rx will need to provide the following information

DEA#	Effective Date	Expiration Date	Cell Phone#	Work Fax#

Work Address	City	State	Zip Code

Comments: For modification requests, please type what change you are requesting in the field below

SECTION IV. USER ACCESS AUTHORIZATION

Pursuant to the contractual agreement on file with the County of San Diego and as designated by my corporate office, I am authorizing access as noted above and affirm that I have personally reviewed the County's Summary of Policies with the above User:

User's Signature _____ **Date** _____

User Signature not needed for Termination requests

Approved by (Print Name) _____ **Title** _____

Program Manager/Director

Approver's Signature _____ **Date** _____

Program Manager/Director

COUNTY OF SAN DIEGO

Summary of Policies
Regarding County Data/Information and Information Systems

To aid in the performance of their regular job assignments and duties, County employees, volunteers, agents and contractors are provided access to many County tools and resources. In the electronic age, these tools and resources include County "data/information" in various formats (e.g. on electronic media, paper, microfiche) and County "information systems" (e.g. computers, servers, networks, Internet access, fax, telephones and voice mail), whether owned, provided or maintained by or on behalf of the County.

The County has established policies and procedures based on best business practices to support the performance of the County's business and to protect the integrity, security and confidentiality of the County's data/information and information systems. Users[1] of these resources play a critical role. By carrying out their regular assignments and duties in compliance with all applicable County's policies and procedures, best practices are maintained.

This summary helps users know their responsibilities by highlighting important aspects of policies that govern access to and use of County data/information and information systems. The policies themselves provide further detailed information governing the use of County data/information and information systems and should be reviewed. Most notably, the County Chief Administrative Officer (CAO) Policy *Acceptable Use of County Data/Information* provides additional guidance on protecting County data/information; the CAO Policy *County Information Systems – Management and Use* provides guidance in controlling and using County information systems; and the CAO Policy *Telecommunications – Management and Use* provides guidance in using desktop and cellular telephones.

Access to County data/information or information systems is necessary to the performance of regular assignments and duties. Failure to comply with these policies and procedures may constitute a failure in the performance of regular assignments/duties. Such failure can result in the temporary or permanent denial of access privileges and/or in discipline, up to and including termination, in accordance with Civil Service Rules.

1. County data/information in all formats and information systems are for authorized County use only. Personal use of County information systems is prohibited unless specifically authorized by the Appointing Authority.
2. As part of their regular assignments and duties, users are responsible for protecting any data / information and information systems provided or accessible to them in connection with County business or programs.
3. Users cannot share data/information with others outside of their regular duties and responsibilities unless specifically authorized to do so.
4. Users have no expectation of privacy regarding any data/information created, stored, received, viewed, accessed, deleted or input via County information systems. The County retains the right to monitor, access, retrieve, restore, delete or disclose such data/information.

[1] *For purposes of this summary, the term "user" shall refer to any person authorized to use County data/information and information systems to perform work in support of the business, programs or projects in which the County is engaged. It also applies to users accessing other networks, including the Internet, through County information systems.*

5. Attempts by users to access any data or programs contained on County information systems for which they do not have authorization will be considered a misuse.
6. Users shall not share their County account(s) or account password(s) with anyone, use another's account to masquerade as that person, or falsely identify themselves during the use of County information systems.
7. The integrity and security of County data/information depends on the observation of proper business practices by all authorized users. Users are requested to report any weaknesses in County information system security and any incidents of possible misuse or violation of County IT policies to the appropriate County representative.
8. Users shall not divulge Dial-up or Dial-back modem phone numbers to anyone.
9. Users shall not make copies of system configuration files (e.g. password files) for their own unauthorized use or to provide to other people/users for unauthorized uses.
10. Users shall not make copies of copyrighted software or information, except as permitted by law or by the owner of the copyright.
11. Users shall not engage in any activity that harasses, defames or threatens others, degrades the performance of information systems, deprives an authorized County user access to a County resource, or circumvents County security measures.
12. Users shall not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a County information system. For example, County users shall not run password cracking or network scanning programs on County information systems.

Misuse of workplace tools and resources, including County data/information and/or County information systems, will be reported to a user's management. Misuse may constitute a failure to perform regular duties and assignments. Such failure may result in short-term or permanent loss of access to County data/information or information systems and/or disciplinary action in accordance with Civil Service Rules, up to and including termination. For non County employees, including volunteers and employees of County contractors, misuse may result in a suspension or withdrawal of your access rights, termination of your participation in County programs, or appropriate against the contractor under the contract's terms, or any combination of all or some of the above consequences.

Acknowledgement:
I have received and read the County of San Diego's Summary of Policies Regarding County Data/Information and Information Systems.

User Name	**User Signature**	**Date**
Program Manager/ Director Name	**Program Manager/ Director Signature**	**Date**

ALL SIGNERS: Keep a copy of this summary for your reference
COUNTY SIGNERS: Department Personnel Representative --- file the original of this form in the authorized user's agency or department personnel file.
NON-COUNTY SIGNERS: Contract administrator --- file the original form along with the contract

SAN DIEGO COUNTY BEHAVIORAL HEALTH SERVICES

Management Information Systems (MIS)

ELECTRONIC SIGNATURE AGREEMENT

This Agreement governs the rights, duties, and responsibilities associated with the use of an electronic signature within the San Diego County MIS.

The undersigned (I) understands that this Agreement describes my obligations to protect my electronic signature, and to notify appropriate authorities if it is stolen, lost, compromised, unaccounted for, or destroyed. I agree to the following terms and conditions:

I agree that my electronic signature will be valid for one year from date of issuance or earlier if it is revoked or terminated per the terms of this agreement. I will be notified and given the opportunity to renew my electronic signature each year prior to its expiration. The terms of this Agreement shall apply to each such renewal.

I agree to keep my electronic signature secret and secure by taking reasonable security measures to prevent it from being lost, modified or otherwise compromised, and to prevent unauthorized disclosure of, access to, or use of it or of any media on which information about it is stored. I understand I may not share it with anyone under any circumstances. I agree that access to my electronic signature may be revoked or terminated per the terms of this agreement.

I will use my electronic signature to establish my identity and sign electronic documents and forms completed in the course of carrying out my assigned job duties. I am solely responsible for protecting my electronic signature. If I suspect or discover that my electronic signature has been stolen, lost, used by an unauthorized party, or otherwise compromised, then I will immediately notify the County MIS Unit and request that my electronic signature be revoked. I will then immediately cease all use of my electronic signature. I will immediately request that my electronic signature be revoked if I discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. I understand that I may also request revocation at any time for any other reason.

If I have requested that my electronic signature be revoked, or I am notified that someone has requested that my electronic signature be suspended or revoked, and I suspect or discover that it has been or may be compromised or subjected to unauthorized use in any way, I will immediately cease using my electronic signature. I will also immediately cease using my electronic signature upon termination of employment or termination of this Agreement.

I further agree that, for the purposes of authorizing and authenticating electronic health records, my electronic signature has the full force and effect of a signature affixed by hand to a paper document.

User **Signature** _____ Date _____

User **Printed Name and Title** _____

Program Manager/Director **Signature** _____ Date _____

Program Manager/Director **Printed Name and Title** _____