County of San Diego Health and Human Services Agency

SmartCare Access Request Form (ARF) for BHS and Optum Staff

Request a new SmartCare account by submitting the required approval forms. 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.

List Reason(s) for Access Request

Request Type*

Effective Date

* For new user and name change requests, a completed ARF, Summary of Policies and Electronic Signature Agreement must be signed and submitted. For Termination and Modification requests, only a signed and completed ARF is needed.

First Name | **Middle Name** | **Last Name** | **If name change, list previous name**

Phone # | **Gender** | **County Department and Unit Name** | **Date of Birth**

User's Email Address | **Optum Department** | **Program Access**

Please List the Programs User Needs Access To

Substance Use Disorder (SUD)

Mental Health

User's Signature | **Date**

Manager/Supervisor Name | **Title**

Manager/Supervisor Signature | **Date**

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
Manager/Supervisor Name	Manager/Supervisor 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

ELECTRONIC SIGNATURE AGREEMENT

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

Requestor **Signature**: _____ Date: _____

Requestor **Printed Name**: _____

Approver/Supervisor **Signature**: _____ Date: _____

Approver/Supervisor **Printed Name and Title**: _____

County Alcohol and Drug Administrator **Signature**: _____ Date: _____

County Alcohol and Drug Administrator **Printed Name and Title**: _____