

I. MANAGEMENT INFORMATION SYSTEM

Cerner Community Behavioral Health (CCBH)

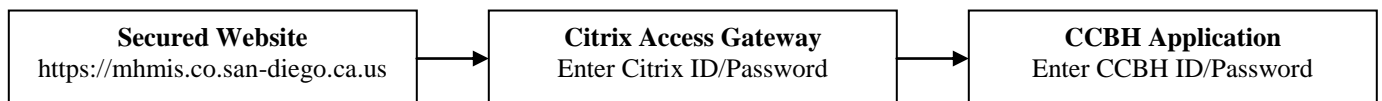
San Diego County Mental Health Services contracted in 2006 with CCBH Software to create a new Mental Health Management Information System (MH MIS). Previously there was one system for client tracking/billing and one for managed care authorizations. The new MH MIS replaces the two systems with one integrated system. All client information, including clinical documentation, is entered into this integrated system, thus allowing each staff responsible for a client's care to access that client's pertinent information.

For the complete **Management Information System: CCBH User Manual**, go to the Optum Health Public Sector Website at <https://www.optumhealthsandiego.com/portal/server.pt> (Note that the "S" in "publicSector" is capitalized. If you do not enter the capital "S", you will not access the website.)

User Account Setup and Access

The Mental Health Management Information System (MH MIS) is used by County and contract operated programs for client tracking, managed care functions, reporting and billing. An electronic health record (EHR) will replace much of what is contained in the paper medical record. Many controls are built into the software and hardware to safeguard the security and privacy of client personal health information.

MH MIS uses CCBH Software which is a web based application that is housed on the County of San Diego Network. Network access to County data systems, including MHMIS, is the responsibility the County Technology Office (CTO). Security and maintenance of the County network is outsourced to the County's Information Technology Outsourcing Contractor (ITOC). Under the direction and oversight of the CTO, the ITOC is responsible for the security of the county network, the Citrix Access Gateway and maintenance of the County's servers which host the CCBH application. In addition, the ITOC is responsible for the set up and maintenance of Citrix user network accounts. The following diagram demonstrates the access to CCBH through the County network secured internet website using the Citrix Access Gateway.



System Administration responsibility for MH MIS is shared between the Administrative Services Organization (ASO) and the County's Mental Health MIS Unit.

- The Mental Health MIS (MH MIS) Unit is responsible for managing access, security, and menu management in CCBH in accordance with County, State and Federal HIPAA

regulations. The MH MIS Unit is also the gatekeeper who ensures that staff is only given access pursuant to contract agreements. In addition, the MH MIS Unit is responsible for coordination among the CTO, ITOC and the ASO.

The ASO is responsible for other system administration activities such as table management, system maintenance, updates to the application, managing the five CCBH environments, producing reports for legal entities, electronic submission of state reporting, coordination with CCBH Software, and providing the User Support Help Desk.

Technical Requirements to Access CCBH

Prior to accessing the CCBH application via the internet, there are some basic technical requirements. For questions about whether an individual user or program site meets the basic technical requirements, it is recommended that the individual or program contact their company's IT department. The ASO may also be able to provide some technical assistance.

In order to access and operate CCBH the following are required:

- Operating System on computer:
 - Windows 2000 (Citrix 10.0 does not supports Windows 95/98)
 - Windows XP Pro
 - Windows XP Home
 - Windows 7
- Internet Explorer version 5.0 or later with a minimum of 24 kbps per concurrent user (high speed internet access)
- A Citrix compatible printer (most newer printers today are Citrix compatible)
- Download Citrix Presentation Server Client file on the user's computer

Staff Set Up and User Account Access

All individuals who provide services or perform some other activity to be recorded in MH MIS as well as those who are authorized to access MH MIS must have a staff account. A "staff" in CCBH is defined as an individual who is employed, contracted or otherwise authorized by his or her designated legal entity or County business group to operate within the County of San Diego public mental health System of Care and whose primary job function may include any one of the following: to provide Mental Health Services, Quality Assurance activities, enter data, view data, or run reports. This includes clinicians, doctors, nurses, office support staff, financial/billing staff, research/analyst staff and program managers/administrative staff. All staff will be assigned a staff ID, which is a numerical ID ranging from 15 numbers. (**Note:** If a person is employed by more than one legal entity, he/she will have a unique staff ID for each legal entity.)

Staff is given access to specific Unit(s)/SubUnit(s) based upon the program(s) where they work. Staff is also given access to specific menus based on their respective job functions. A list and

definition of menus is available on the CCBH Request Form. For additional information regarding staff or program access contact the SDC MHS MIS System Administration.

Staff authorized to access MH MIS will be given login access and a password and are considered “users”.

User Access requires the following steps:

1. Program manager completes the “CCBH Request Form” (ARF) (Appendix I – A.I.1).
2. Contractor employee and employee’s supervisor must read and sign the “Staff Electronic Signature Agreement” (Appendix I – A.I.3).
3. Contractor employee and employee’s supervisor must also read and sign the County’s “Summary of Policies” (SOP) form (Appendix I – A.I.2).
4. Fax all completed forms to the **MH MIS Unit Fax at (858) 467-0411 or SCAN and EMAIL to BHS – AccountRequest.HHSA@sdcounty.ca.gov**
5. MH MIS Unit completes the County’s “Computer Services Registration Form” (CSRF).

All forms **must** be typed, and contain all necessary information. Incomplete forms will be returned to the contact person listed on the form. Once completed correctly, the forms must be re-faxed to MH MIS Unit. Please ensure forms are completed correctly to avoid delay in user account setup.

Once all forms have been submitted, the MH MIS Unit will:

1. Complete and process the CSRF for set up of a Citrix User Account with ID/password
2. Set up CCBH User Account with ID/password
3. User will be provided his/her Citrix/CCBH ID/passwords at the CCBH training.

Program managers and other supervisors are responsible to:

1. Register new staff who will be users to attend the “New User CCBH Training”
 2. Contact the QM Unit to confirm CCBH training date/time/location
 3. Confirm that employee has successfully completed CCBH training
- Note:** No user will be granted access to CCBH without successfully completing the CCBH Training.

All forms with instructions are available electronically on the ASO's (OptumHealth) Public Sector website at <https://www.optumhealthsandiego.com/portal/server.pt>

Staff Assignment to Unit(s) and SubUnit(s)

On the ARF, the program manager will be assigning each staff to specific Unit(s) and SubUnit(s) based upon the program(s) where the staff performs work. Staff may be assigned to a single or multiple Unit/Subunits. The Unit/SubUnit number(s) must be reflected on the CCBH Request Form. The MH MIS Unit will monitor staff access to Units/Subunits to ensure that staff has been assigned correctly. Under no circumstances, should a staff person be assigned to a Unit/Subunit if that staff person does not perform work for that program. This would constitute a violation of security and client confidentiality.

User Assignment to a Menu Group

Each user is granted restricted access to MH MIS based on his/her job requirements. One of the ways that access is restricted is through assignment to Units and Subunits described above. In addition, access is further restricted by assignment to a menu group. A menu group defines the screens and reports the user will be able to access and whether the user can add/edit or delete for each of those screens. For example, the user may only be able to view but not change data in one screen but may have rights to add data or edit previously entered data for another screen. Menu groups are created based on multiple criteria such as security, level of access to client information, staff job functions, staff credentials and state and federal privacy regulations.

On the ARF, the program manager or supervisor is responsible for requesting the menu group assignment for each user based on his/her job functions. A user may only be in one menu group at a time. Therefore, it is important for the program manager/supervisor to determine which menu group is the best match for the job functions performed by his/her staff.

For example, there will be menu groups for:

- Data entry staff with full client look up rights
- Data entry staff with limited client look up
- Clinicians
- Program managers and supervisors
- Quality Assurance
- Billing staff
- Billing only (For Billing Purposes Only – It has no views)
- Research and Analysts

Refer to the ARF Instructions for a list and definition of available menus. The MH MIS Unit will review menu group requested by the program manager/supervisor and approve or modify the request.

Limitation of Staff Assignment to “Data Entry – Add New Clients” Menu Group

Program staff will be allowed to view information about a client currently or previously served by their program. Designated program staff will be given access to the “full client look up” in order to add new clients and assign existing clients to their subunit (program). These individuals will be allowed to view all clients in the system, including those not served by their program. Due to security and privacy issues, each program will be limited to two staff that will have this higher level of access. This access allows for data entry, adding new clients, full client lookup; entering demographic, diagnosis, insurance, and financial information (UMDAP); opening assignments; and running reports. Requests for exceptions to the two staff rule must be made in writing directly to and approved by the MH MIS Unit.

Staff Access to Live Production and Training Environment in CCBH

For most users, after logging on to CCBH through the Citrix Access Gateway, two visible CCBH icons will be available for selection. One icon provides access to the Live Production environment used for data entry and reporting. The other icon provides access to the Training environment which is a copy of the set up of the live environment populated with fictitious client data. The training environment is used to train all new and returning users. Access to the training environment will remain available for ongoing training purposes. For example, on occasion, when there are upgrades to the CCBH application, it may be necessary for staff to first practice in the Training environment prior to utilizing new functionality in the Live Production environment. Program managers and staff will be notified of changes to application functionality and will be instructed as to when the training environment should be utilized.

Program Manager/Supervisor Responsibility for Staff Access and Security

The program manager/supervisor shall ensure that staff is in compliance with all County, State and Federal privacy and confidentiality regulations regarding protected health information (PHI). In addition, the program manager shall ensure that his/her staff is aware of the County’s Security Policy regarding the protection of network/application passwords and use of County systems and data as outlined in San Diego County’s “Summary of Policy”. The program manager shall immediately notify the MH MIS Unit whenever there is a change in staff information such as staff demographics, email, job title, credential/licensure, and Unit/Subunit assignment. This includes the initial staff setup, modifying or terminating existing staff accounts. **Under no circumstances shall a staff person who has terminated employment have access to the EHR through CCBH. This would constitute a serious violation of security which may lead to disciplinary actions.**

NOTE !

For system security, providers must notify OptumHealth when staff with access to CCBH move, change jobs, or are terminated.

Staff Termination Process

- **Routine User Termination** – In most cases, staff employment is terminated in a routine manner in which the employee gives an advanced notice. Within one business day of employee termination notice, the program manager shall fax to the MH MIS Unit (858) 467-0411 or scan and email to BHS-AccountRequest.HHSA@sdcounty.ca.gov a completed ARF with the termination date (*will be a future date*). The MH MIS Unit will enter the staff expiration date in CCBH which will inactivate the staff account at the time of termination and process the CSRF to delete the County network Citrix account.
- **Quick User Termination** – In some situations, a staff person’s employment may be terminated immediately. In this case, the program manager must immediately call the MH MIS Unit at (619) 584-5090 to request the staff account be inactivated immediately. Within one business day, the program manager shall fax a completed ARF to the MH MIS Unit (858) 467-0411 or scan and email to BHS-AccountRequests.HHSA@sdcounty.ca.gov.

The MH MIS Unit is responsible for inactivating both the CCBH and Citrix staff accounts.

Application Training

Prior to staff obtaining access to CCBH, he/she shall successfully complete the CCBH training. Program managers are responsible for registering new and returning CCBH users for training on the CCBH application. The Quality Management (QM) Unit provides training on a regularly scheduled basis. Previous CCBH users returning to employment (including maternity leave) after more than 90 days of absence will be required to resubmit new paperwork including an updated ARF and be evaluated for a skills assessment or retraining.

User Manuals

Users should be familiar with the MH MIS User Manual and the Financial Eligibility and Billing Procedures Manual, which contain detailed information about program workflow requirements using the MH MIS. These manuals are available on line at www.optumhealthsandiego.com.

Security and Confidentiality

The County of San Diego is responsible for the protection of County technology and data and to monitor through its own policies and procedures user compliance with state and federal privacy and confidentiality regulations.

The County’s Security mandates state that access will be given to a user at the least minimum level required by the user to execute the duties or job functions and that only those individuals with a “need to know” will be given access. Protection of County data and systems is also

achieved via the use of unique user identification and passwords as well as other tracking methods.

Passwords

The sharing of passwords or allowing unauthorized individuals access into the system is strictly prohibited. A user's password is his/her electronic signature that is not to be shared or made available to anyone. Programs must ensure that the County's Policy and Procedures regarding security and confidentiality as stated in the Summary of Policies is complied with at all times. Failure to comply with these polices and procedures can result in the temporary or permanent denial of access privileges and/or disciplinary action.

MH MIS passwords:

- Must be changed every 90 days
- Must have a minimum of 7 characters
- Must contain a mix of letters & numbers
- May NOT be reused
- Are case sensitive
- Will be rejected if common words or acronyms are used

Unauthorized Viewing of County Data

All terminals and computer screens must be protected from the view of unauthorized persons. All confidential client information, electronic or printed, shall be protected at all times.

User Support

Users can obtain support through the OptumHealth Support Desk. The OptumHealth Support Desk can assist a user with the MH MIS application (technical assistance), MH MIS password issues, connectivity/access problems, printer problems, data entry questions, special requests, such as reports and Citrix access issues for contractors. For Citrix access issues (i.e. password reset), County employees must contact the County IT vendor.

In some cases, the OptumHealth Support Desk may refer the caller for second level user support, i.e. to the Mental Health Quality Management Unit for clinical issues and to the Mental Health Billing Unit for financial eligibility and billing issues.

The OptumHealth Support Desk may be contacted as follows:

Phone: 1-800-834-3792

Fax: (619) 641-6975

Emails: sdhelpdesk@optumhealth.com

- OptumHealth Support Desk hours: Monday through Friday, from 6:00 am to 6:00 pm except on holidays.

The OptumHealth Support Desk will provide after-hour cell phone emergency support for urgent Citrix and CCBH issues. Urgent issues affecting multiple users include:

- When logging into CCBH, the system does not respond or appears to be frozen, and/or no data can be entered or viewed
- For after-hour support use cell (800) 834-3792 on weekdays 4:30 am – 6:00 am and 6:00 pm – 11:00 pm and on weekends 4:30 am – 11:00 pm

For an operating system failure, contact your company's IT department. The IT department will determine the need for OptumHealth Support Desk involvement.

NOTE: Printing issues, password resets technical and CCBH application questions are not considered an emergency and will be handled the next business day.

QUICK RESOURCE GUIDE

1. MH MIS Unit Phone: 619-584-5090
2. MH MIS Unit Email: MH_MIS_SystemAdmin.hhsa@sdcounty.ca.gov
3. MH MIS FAX (ARFs and SOPs): 858-467-0411
4. MH MIS Email (ARFs and SOPs): BHS-AccountRequest.HHSA@sdcounty.ca.gov
5. OptumHealth Support Desk Phone: 1800-834-3792
6. OptumHealth Support Desk 24 Hour Pager: 619-893-4839
7. OptumHealth Support Desk email: sdhelpdesk@optumhealth.com
8. Web address to access CCBH: <https://mhmis.co.sandiego.ca.us>
9. OptumHealth Public Sector Website: www.optumhealthsandiego.com