

## **Exhibit Q**

### **Clinical Management for Behavioral Health Services (CMBHS) Requirements**

#### **I. CMBHS Background and Overview**

The Department of State Health Services (DSHS) developed the Clinical Management for Behavioral Health Services system (CMBHS), and it began operating in December 2009. The system is used across the state with DSHS and Health and Human Services Commission (HHSC) contracted substance use and mental health treatment service providers and others who qualify.

Some providers use CMBHS as their electronic health record and claims payment system, while others mainly use it to submit data to the state to fulfill contract requirements. The system includes clinical tools that standardize the assessment, diagnosis, and level-of-care determination and treatment processes. Providers also use it to document the services provided and send claims directly to the HHS program that processes and pays that claim type.

CMBHS supports data exchange between:

1. HHSC and local mental health authorities.
2. Contracted substance abuse and mental health service providers (with client consent as required by law).
3. HHSC and other state agencies to coordinate care and help with oversight of services and claim payments.

Service providers with Texas HHSC contracts for delivering mental health services or substance use disorder services are the primary users of CMBHS. The requirements for using CMBHS are defined in their contracts.

Some providers and state agencies don't directly contract with HHSC for service delivery but might qualify for CMBHS and must sign a user agreement. These providers might be Medicaid managed care providers of mental health targeted case management or mental health rehabilitative services that need access to complete assessments. This data must be submitted to HHSC or other state agencies serving the same populations that might need this information to ensure coordination of care.

#### **System Requirements**

1. CMBHS is only compatible with Microsoft Edge (90.x) or higher and Google Chrome version 40 or higher.
2. JavaScript must be enabled to use the application.
3. Adobe Reader is needed to print documents.

#### **II. CMBHS Requirements**

- A. Grantee shall use the CMBHS components/functionality specified in RFAHHS0015355. The required CMBHS components serve as requirements for Treatment services are listed below;

**Exhibit Q**  
**Clinical Management for Behavioral Health Services (CMBHS) Requirements**

1. The local Security Administrator controls and manages access to CMBHS on the local level. They are responsible for security, protecting client health information, and assisting users with CMBHS. In order to do this, the Security Administrator must:
  - a. Be a highly trusted person, as they will have access to confidential and private client, staff, and business information.
  - b. Have above average computer skills to ensure proper user setup and resolution of user problems on the local level.
  - c. Have in depth knowledge of laws and rules regarding protected health information PHI and the business entity's policies and procedures.
  - d. Be able to communicate with the Training and Technical Assistance and Help Line Team and coordinate the resolution of problems with users.
  - e. Be available when staff are using the system and need assistance.
2. **Find/Add Client** gives you a screen to search for an existing client, or to add a new client.
3. **Client Workspace** takes you to a page that summarizes much of a client's protected health information (PHI).
4. **Intake** – Found under the Intake tab are:
  - a. **Screening** is used to determine clinical eligibility for SUD services.
  - b. **Financial Eligibility** is used to determine residency and financial eligibility for state-funded services.
  - c. **Medicaid Eligibility Verification** is used to determine whether the client has Medicaid.
  - d. **Wait List Entry** is used if the client must be placed on a waiting list.
  - e. **Admission** is used to admit a client.
5. **Service Planning** is used to create the following for a client:
  - a. **Treatment/Service Plan or Treatment Plan** is a clinical document where the treatment team documents the client problems identified at admission, and the interventions that a client will receive during an **episode of care**.
  - b. **Treatment/Service Plan Review**  
The Treatment/Service Plan Review is required based on the service type the client is receiving. For Residential services, a treatment plan review is due no less than every 30 Calendar Days for Treatment for Adults, 45 Calendar Days for Treatment for Specialized Female, and 60 Calendar Days for youth or whenever anything significant happens. For outpatient services, a treatment plan review is due halfway through projected length of stay, or when anything significant happens.
6. **Assessment** is used to create:
  - a. **Initial Substance Use Disorder (SUD) Assessment**

**Exhibit Q**  
**Clinical Management for Behavioral Health Services (CMBHS) Requirements**

An assessment, more comprehensive than a screening, is a health professional's review of an individual. The review consists of evaluation of a variety of domains including current and past functioning in the areas of mental health, substance use, risk of harm, physical health, education, employment, family, and socialization.

**b. Update Substance Use Disorder (SUD) Assessment**

Completed when there is a significant change in the client's clinical and/or life situation and as required by law or contract. For substance use disorder services, there is no requirement that an update assessment be completed on a regular basis. An initial assessment completed by your organization can be updated at any time within the same episode of care, regardless of how old it is. An expired assessment can still be updated up to 30 Calendar Days after it expires.

**c. Detoxification - Initial**

In the General Tab, the user gathers information about why the client is presenting for services and documents that information in the General section. The data fields and questions under the General tab are the same for all clients receiving all service types and of any age.

**7. Service Management** is used to create:

- a. Case Management
- b. Open Case
- c. Close Case
- d. Service Authorization Request
- e. Service Begin
- f. Service End

**8. Service Documentation** is used to create:

- a. Progress Notes
- b. Psychoeducational Notes
- c. Administrative Notes
- d. Lab/Test Results
- e. Medication – Found under this tab are:
  - i. Medication Order
  - ii. Medication List
  - iii. Medication Service (Single Client)

**9. Consents & Referrals** – Found under this tab are:

- a. Consent
  - i. Create Consent
  - ii. Revoke Consent
- b. Referral

**10. Discharge** – Under this tab are:

- a. Discharge Client
- b. Discharge Summary

**Exhibit Q**  
**Clinical Management for Behavioral Health Services (CMBHS) Requirements**

- c. Discharge Follow-up
- B. Grantee may use additional components/functionality that is available.
  - 1. Request/maintain user access for appropriate staff (including access control and credential maintenance);
  - 2. Grantee details;
  - 3. Utilize the CMBHS Reports to review: Performance Measures, Client level data, Dashboards, Demographic, Management, Curriculum and CMBHS Grantee's Capacity Reports.
  - 4. Invoices and/or Claims;
  - 5. Financial Status Report (FSR);
  - 6. Deliverable Submission.
- C. Grantee shall designate a Security Administrator and a back-up Security Administrator. The Security Administrator is required to manage locations, manage user accounts and Grantee's organization setup information. implement and maintain a system for management of user accounts/user roles to ensure that all the CMBHS user accounts are current. The Security Administrator controls and manages access to CMBHS on the local level. They are responsible for security, protecting client health information, and assisting users with CMBHS.
- D. In accordance with the HHS Data Use Agreement v 8.5, establish and maintain a security policy that ensures adequate system security and protection of confidential information.
- E. Attend HHSC training for the CMBHS functionality.
- F. Each Fiscal Year, Grantee shall complete the HHSC approved Cybersecurity training, required per the Texas Government Code, Section 2054.5192.

**III. CMBHS ACCESS and Forms**

When the grant agreement with Grantee is executed; Grantee shall comply with the following requirements regarding CMBHS access and management of users:

- A. Grantee shall select the organizations CMBHS Security Administrator and back-up Security Administrator and complete the HHSC Form: **CMBHS Security Administrator Application.** Grantee shall contact the CMBHS Helpline to request the form, as follows:
  - 1. Phone Number: (866) 806-7806
  - 2. Email Address: [CMBHSTrainingTeam@hhs.texas.gov](mailto:CMBHSTrainingTeam@hhs.texas.gov)

*Note: The CMBHS Helpline hours of operation are Monday through Friday, 8:00 a.m. to 4:30 p.m. Central Standard Time.*

**Exhibit Q**  
**Clinical Management for Behavioral Health Services (CMBHS) Requirements**

- B. Grantee shall submit the completed **CMBHS Security Administrator Application** forms to the CMBHS helpline email address, [CMBHSTrainingTeam@hhs.texas.gov](mailto:CMBHSTrainingTeam@hhs.texas.gov).
- C. Grantee shall submit updated/revised **CMBHS Security Administrator Application** forms within ten (10) Business Days of changes to the Grantee's designated Security Administrator or the back-up Security Administrator.
- D. Grantee's CMBHS Security Administrator is responsible to ensure that access to CMBHS *is* restricted to only authorized users, in accordance with HHSC Data Use Agreement.
- E. Grantee's CMBHS Security Administrator is responsible for disabling authorized users who are no longer authorized to access CMBHS secure data within one (1) business day of identifying the authorized user needs to be removed.
- F. Grantee's CMBHS Security Administrator shall complete and submit a signed CMBHS Security Attestation Form and a list of Grantee's employees, contracted laborers, and sub-Grantees authorized to have access to secure data.
- G. Grantee shall ensure that Grantee's employees have appropriate Internet access and an adequate number of computers of sufficient capabilities to use the CMBHS. Equipment purchased with HHSC funds must be inventoried, maintained in working order, and secured.
- H. HHSC reserves the right to limit or deny access to CMBHS at any time for any reason deemed appropriate by HHSC. Grantee access to CMBHS will be placed in inactive status when the Grantee ceases to have an executed grant agreement with HHSC.