AssureCare

MedCompass User Access Guide

State of Montana MedCompass User Access Guide

Table of Contents

Table of Figures

1.Purpose

The purpose of this user guide is to provide instructions on how to configure MedCompass (the Montana Care Management Solution) security for 0208 Waiver and Part C/FES provider users. When adding a new MedCompass user or changing the access of an existing MedCompass user requires the Provider to identify the new or changed security access for the user and which members that the provider serves the member should have access.

This guide provides instructions for Provider agency designated Security Officer to set up new user accounts, maintain existing user accounts, and managing the end-to-end lifecycle for user access to the MedCompass solution. Access management tasks include creation of the user, assigning security roles, assigning staff roles, and assigning the user to the Provider or one or more of the Provider's sites.

1.1 Overview

The Montana User Access Matrix includes 5 worksheet tabs that collect the required information to enable the appropriate user access to the MedCompass solution. The User Access Matrix includes: Access, Security Role, Staff Team, Staff Role and Provider tab(s)

Each tab definition and detail are included below:

- Access Tab Section 1
- Security Tab Section 2
- Staff Team Tab Section 3
- Staff Role Tab Section 4
- Provider Tab Section 5

1.2 Instructions

1. When entering information into the Montana User Access Matrix, users must complete all required fields. The column headings for required fields have been denoted in the tables below, as well as in the Montana User Access Matrix with a yellow background highlight and a red outline for the cell.
2. It is very important that the Provider Security Officer does not alter the Matrix in any way. This means users must not change any column or worksheet names and not insert any columns or rows. Doing so will break the automated program that reads data from the worksheet and updates MedCompass.
3. Each section below includes field descriptions for some of the fields included in each of the User Access Matrix. The Access Matrix has been updated to include values in each drop down appropriate for your provider organization.
4. When requesting access or updating security roles, the Provider Security Officer MUST use a new sheet for each submission of new users or the changes to existing users. Previously submitted security changes should not be included in subsequent submissions.

5. Please validate the accuracy of all information prior to submission. Errors in the spreadsheet may provide a user incorrect access to system functions or unintended access to members the Provider serves. Additionally, errors in the spreadsheet could delay the processing of the request.
6. If a user has multiple Security Roles or multiple Staff Roles, you should include multiple rows for that user on the respective tabs for each role the user has within the Agency. As noted in the example below, Nicole from @ProviderAgency.org works in human resources but is also the executive director within her Agency.

ID (ICAP Username)	Security Role	Security Profile	Allow
Nicole@ProviderAgency.org	####### - HR	*Provider Agency Name*	Yes
Nicole@ProviderAgency.org	####### - Executive Director	*Provider Agency Name*	Yes

1.3 Invalid Access Requests

DPHHS will perform the initial validation to determine if the right level of access is being requested.

AssureCare will perform basic validations on the worksheet to ensure all required data entered. If any issues are identified or if issues are encountered while loading the data, the Submitter will be contacted via ServiceNow with details on the additional information required/needed to process the request. All communications will be conducted within ServiceNow.

2. Access Tab:

The Access tab identifies the demographic information for the users the Provider Security Officer is requesting to create, modify, activate, deactivate, and/or expire access within the MedCompass System. The Provider Security Officer will need to provide the following information for each user access request:

- the type of request for accessing MedCompass and,
- the necessary user access demographics(s)

The Provider Security Officer will include one row in the Access Tab for any user for which they are either adding, updating, or removing (i.e., expiring) a user's MedCompass access privileges.

The Provider Security Officer must complete the required fields for each user row on the Access Tab. The table below describes the required fields in the Access Tab.

Field	Description	Required	Example Information
Date Sent to AssureCare	The day you are filling out the ticket requesting MedCompass Access	**Y**	MM/DD/YYY (i.e., 10/12/2020)
Request Status	Request Status will always be "Open"	**Y**	Open
Request Type	• **Add –** Select this Value when requesting access for a new user to MedCompass • **Expire -** Select this Value when requesting removal of access to MedCompass for a user • **Update -** Select this Value when requesting an update to a user's access in MedCompass	**Y**	• **Add** Provider – Human Resources • **Expire** Provider – Human Resources • **Update** (you will select this option when a user has a role change such as) Provider – Human Resources > Provider – Executive Director
Request Processing Time	The time it will take to process the request	**Y**	• **Standard** – 1-2 weeks turnaround • **Expedited** – 48-hour turnaround • **Super Expedited** – 24-hour turnaround

Field	Description	Required	Example Information
Date Access/Update Needed By	Will be the day you need Access/Updated Access for the User (MT SLAs) and should match the due date in ServiceNow.	**Y**	10/11/2020
MedCompass Environment	The environment where the MedCompass application is deployed and executed in.	**Y**	Production
ID (ICAP Username)	This is your ICAP Username. (needs to be an exact match) Users will use the email for ICAP of the user you are Requesting Access/Updates for.	**Y**	(Nicole@ProviderAgency.org)
Last Name	This will be the Last Name of the user you are Requesting Access/Updates for.	**Y**	Smith
First Name	This will be the First Name of the user you are Requesting Access/Updates for.	**Y**	Nicole
Email Address Type	This will be the Email Address Type for the User	**Y**	Business Email, Clinical Email, Home Email, Financial Email, Practice Email, Technical Email, Other Email
Time Zone	This will be your time zone (Most users will select Mountain Standard Time)	**Y**	Eastern Standard Time / Central Standard Time / Mountain Standard Time / Pacific Standard Time
Phone Number 1	This is the user's phone number. If a phone number is entered, then columns P and Q are required.	**N**	406) 555-5555
Phone Number Type 1	This will be the user's phone number type. Required if phone number is entered.	**N**	Home Phone, Work Phone, Cell Phone, Message Phone
Preferred Phone Number?	This identifies if the user's phone number is the preferred number. Required if a phone number is entered	**N**	Yes/ No

Access Table 2.0.1

3. Security Role Tab:

The Security Role Tab identifies the security role for each user. The security role controls access to screens, data, and actions within MedCompass. This tab is used to add, modify, or remove the security roles assigned to each user. Each user can have multiple security roles. The Provider Security Officer will need to provide the following information for each user access request:

- The Security Role and,
- The Security Profile

If more than one Security Role is being requested for a user, please enter a separate distinct line for each role provider location combination. By assigning a security role to a user, the Provider Security Officer is granting the user access to specific screens, enabling specific actions, and providing access to information in the system necessary to complete their activities/work/tasks. If you add or remove a Security Role for a user, you should make a corresponding change to the Staff Role tab (i.e., if you remove a Security Role from a user you should also remove the related Staff Role for that user).

The Provider Security Officer will only include a row in the Security Role tab for a user if they are adding a new Security Role for a user (i.e., Allow = "Y" for the username and security role) or if they are removing a Security Role assigned to a user (i.e., Allow = "N" for the username and security role).

The Security Profile field will be populated with the with one of the "Provider Agency" values assigned to the user on the Provider Tab. The number of rows in the "Security_Role" tab for each user should be a multiple of their number of assigned Provider Agency locations from the Provider tab and the number of security roles to be assigned to the user (i.e., if the user requires one security role "####### - GH-SL-W D Manager" for two separate locations [i.e., group homes] assigned to the user on the Provider tab), the user should have two separate rows in the "Security_Role" tab.

The Provider Security Officer must complete the required fields for each user row on the Security Role Tab. The table below describes the required fields in the Security Role Tab.

Field	Description	Required	Example Information
ID (ICAP Username)	The Username of the user that you are adding or removing the security.	**Y**	Nicole@ProviderAgency.org
Security Role	Provides record level access to specific screens and objects in MedCompass.	**Y**	• ####### - DSP • ####### - Executive Director • ####### - Fiscal • ####### - GH-SL-W D Manager • ####### - HR • ####### - Medical • ####### - Ops Dir-Prog Mgr • ####### - Other Limited • ####### - Self Direct Emplr • ####### - Self Direct FMS * "#######" represents the Provider ID number * See Table 1 for security role definitions
Security Profile	This provides an additional layer of security by linking your Security Role to a Provider agency; limiting the user's view of member's to only those served by the appropriate agency	**Y**	This field will be populated with the with one of the "Provider Agency" values that are assigned to the user from the Provider Tab. ***Only Select a provider in the Staff Profile column that is assigned to that user on the Provider tab. Otherwise, there will be security access issues.***

Field	Description	Required	Example Information
Allow	This value will be either Yes or No	**Y**	Choose "Yes" if you are adding a Security Role to the user. Choose "No" if you are removing the Security Role from the user.

Security Role Table 3.1

3.1. Security Role Definitions and Corresponding Staff Role

Table 1 DDP Provider Security Role Descriptions

Security Roles	Security Role Description	Access Overview	Staff Role
Case Manager	Case Manager for 0208 provides case management services for eligible members; monitors and develops Plan of Care, complete referrals and individual cost plans	Performs tasks such as creating and submitting new members for services. Develops the Plan of Care, initiates the PSP, collects signatures, develops the Cost Plan, monitors the delivery of care. Review quarterly reports submitted by providers. Case Manager is the final approver on the plan of care and the PSP. Send and receive secure messages to care team members and guardians.	Case Manager (for DDP)
CM Supervisor	Case Management Supervisor for 0208 covers Case Loads for Case Managers when needed, may act as CM for members, monitors CM activities and approves case notes	Monitors the completion of work by their case managers to ensure that key tasks and timelines are met. Able to fill in for any case manner on their team and perform required tasks.	CM Supervisor (for DDP)
####### - DSP	Works directly with clients, providing direct care and support, in settings where services are delivered.	read-only access to demographic information, read-only access to Health Summary, ability to enter health metric information, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, Ability to send secure messaging	Provider - DSP
####### - Medical	Works directly with clients to access or provide medical assistance and may take vitals etc. and report on medical issues	read-only access to demographic information, read/write access to health summary info, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, ability to send secure messaging, ability to see provider service authorizations.	Provider - Medical

Security Roles	Security Role Description	Access Overview	Staff Role
####### - GH-SL-W D Manager	Manages a setting where services are provided, generally is responsible for providing backup for staff and ensuring coverage for their site, providing information to meet provider Plan of Care requirements.	read-only access to demographic information, read/write access to health summary info, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, ability to send secure messaging, ability to see provider service authorizations, access to reports	GH Manager/SL Manager/W/ D Manager
####### - Ops Dir-Prog Mgr	Generally, works under Executive Director oversees GH managers and Provider DSP's, will complete PSP documents and assists with scheduling staff, incident management etc.	read-only access to demographic information, read/write access to health summary info, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, ability to send secure messaging, ability to see provider service authorizations, access to reports, ability to view referrals	Operations Director or Program Manager
####### - HR	Oversees provider agency HR issues	ability to enter provider case notes, ability to send secure messaging, ability to see provider service authorizations, access to reports	Provider- HR
####### - Fiscal	Completes or provides oversight of billing in MMIS for services provided by provider agency. Monitors service utilization.	read-only access to demographic information, ability to enter provider case notes, ability to send secure messaging, ability to see provider service authorizations, access to reports	Provider-Fiscal
####### - Executive Director	Oversees provider agency, reports to agency board, and is usually the contact liaison for RM/Central Office for contract or performance issues.	read-only access to demographic information, read/write access to health summary info, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, ability to send secure messaging, ability to see provider service authorizations, access to reports, ability to view referrals	Provider-Executive Director
####### - Other Limited	Provides limited waiver services, doesn't include information on assessments or PSPs typically but would need to view service auths. And billing information	read-only access to demographic information, read/write access to health summary info, ability to enter provider case notes, read only access to PSP, assessments and Care Plan, ability to send secure messaging, ability to see provider service authorizations, access to reports, ability to view referrals	Other (limited provider)

Security Role Definition Table 3.2.1

4. Staff Team Tab:

The Staff Team identifies the Provider Agency work queue assignment for the user. The Provider Security Officer should only assign their Provider Agency Staff Team to their users that should have access to the tasks assigned to the Provider Agency. The most common tasks that will be sent to the Provider Agency work queue are referrals. This tab is not required for every user but if information is entered in Column A then Columns B and C are required.

Field	Description	Required	Example Information
ID (ICAP Username)	This will be the ICAP Username of the User you are Requesting Access/Updates for.	**Y**	**Provider** – (Nicole@ProviderAgency.org)
Staff Team	Specific team or group of individuals within your organization.	**Y**	Team Name or Role Designation ”DDP Region 1”
Allow	This value will be either Yes or No	**Y**	Choose “Yes” if you are adding a ‘Staff Team’ to the user. Choose “No” if you are removing the ‘Staff Team’ from the user.

Staff Team Table 4.1.

5. Staff Role Tab:

The Staff Role represents the job title, role, job function of the user in the system. For example, the staff role is what shows up as the user's title when they sign an assessment. It is the users title that displays when the user is added to a member's care team. It is also used to populate the user "Case Load" on the user's dashboard.

For Montana, Staff Roles map one-to-one to each Security Role (meaning if you have Security Role "X" you will always have Staff Role "Y"). For each row in the Security Role Tab for a user there should be a corresponding role in the Staff Role Tab. If a user requires multiple Staff Role, please add a distinct line for each role.

Field	Description	Required.	Example Information
ID (ICAP Username)	This will be the ICAP Username of the User you are Requesting Access/Updates for.	**Y**	**Provider** – (Nicole@ProviderAgency.org)
Staff Role	This will be your role in MedCompass. This should match your Security Role.	**Y**	• Provider - DSP • Provider - Medical • GH Manager/SL Manager/W/D Manager • Operations Dir or Program Mgr • Provider - HR • Provider - Fiscal • Provider - Executive Director • Other (limited provider) • Self Direct (EO)-Employer • Self Direct- FMS staff
Allow	This value will be either Yes or No	**Y**	Choose "Yes" if you are adding a 'Staff Role' to the user. Choose "No" if you are removing the 'Staff Role' from the user.

Staff Role Table 5.1.0

6. Provider Tab:

The Provider Tab identifies the Provider Agency assigned to each user. Each Provider Agency user MUST be assigned at least one Provider on the Provider Tab. The key function of the Provider Tab is that it limits the members a user can access. If a user is given access to your Provider Agency with the "(82)" designation, the user will have access to all members that your agency serves. Otherwise, the user will only have access to members where their assigned Provider Site is assigned to the member's care team.

The Provider Security Officer must complete the required fields for each user row on the Provider Tab. The table below describes the required fields in the Provider Tab.

Field	Description	Required.	Example Information
ID (ICAP Username)	This will be the ICAP Username of the User you are Requesting Access/Updates for.	**Y**	**Provider Agency User** – (Nicole@ProviderAgency.org)
Provider Name	This field includes a pick list of the valid provider ID's for your Provider Agency.	**Y**	See the Options Tab column K for the list of your Provider Agency names to choose. These include your primary Provider ID (82) and your sites.
Provider ID	This field will automatically populate when a Provider Name is selected. This field should not be changed	**Y**	See the Options Tab column M for the list of your Provider ID's that will populate when a Provider Name is chosen. ID's that start with "998" are provider sites which will allow you to limit the members that can be accessed by your users.
Allow	This value will be either Yes or No	**Y**	Choose "Yes" if you are adding a 'Provider' to the user. Choose "No" if you are removing the 'Provider' from the user.

Provider Table 6.1.0