

3rd Party System User Access Request Instructions

Section 1 – Type of Request

Identifies what type of application is being submitted

Section 1 – Type of Request	
* Type of Request:	<input type="checkbox"/> New <input type="checkbox"/> Modification <input type="checkbox"/> Reactivation <input type="checkbox"/> Revocation
	<input type="checkbox"/> Name Change - Previous Name: _____
Effective Date (If left blank, it is assumed to be immediate):	_____

Please indicate Type of Request:

- New – User is New at the agency and has not had access at that agency before
- Modification – Used for Name Changes, and Access level changes
 - If name change, please enter Previous Name on line indicated
- Reactivation – If user has not logged into the systems for over 90 days and account is locked
- Revocation – User is no longer needing access, or no longer works for your agency

Section 2 – Individual User Information



Identifies individual whose profile will be set up, modified, reactivated, or revoked

Section 2 – Individual User Information	
*First Name:	_____ *Middle Initial: _____ *Last Name: _____
*List any 4-digit numeric identifier:	_____ *Work Phone: _____
*Individual's Physical Work Address/City/Zip:	_____
*Work Email Address:	_____

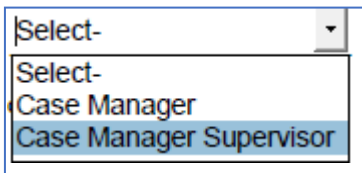
- First Name, Middle Initial, Last Name – Please include middle initial if applicable. This will be incorporated into user's BUS login ID
- 4-digit numeric identifier – Any 4-digit number
- Work Phone – Please include direct number to user. This sometimes is used to reach out to user to assist with issues on the BUS
- Individual's Physical Work Address/City/Zip – Please include. This is also used to set up user's BUS profile.
- Work Email address – This will be used to send out emails generated by the BUS. Please verify for accuracy or user will not receive intended emails.

Section 3 – Employer Information

Information is used to assure user is connected to correct agency

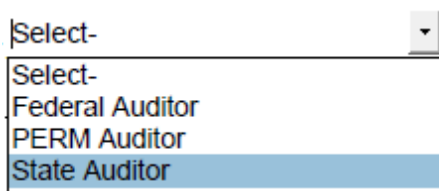
Section 3 – Employer Information	
*Employer Name: _____	*Employer Phone Number: _____
*Employer's Primary Address/City/Zip: _____	
*Type of Entity: <input type="checkbox"/> Fiscal Agent <input type="checkbox"/> MA Site <input type="checkbox"/> PE Site <input type="checkbox"/> State Agency - _____	
<input type="checkbox"/> Case Management Agency <u>Select-</u> 	<input type="checkbox"/> Auditor <u>Select-</u> 
<input type="checkbox"/> Other - If other, please describe: _____	

- Employer Name – This is the agency or vendor the user works for
- Employer Phone Number – Phone number for agency or vendor
- Employer's Primary Address/City/Zip – Address for agency or vendor
- Type of Entity – Please select from the following:
 - Case Management Agency:
 - Case Manager
 - Case Manager Supervisor



A screenshot of a dropdown menu for 'Case Management Agency'. The menu is open, showing three options: 'Select-' (at the top), 'Case Manager', and 'Case Manager Supervisor'. The 'Case Manager Supervisor' option is highlighted with a blue background.

- Auditor:
 - Federal Auditor
 - PERM Auditor
 - State Auditor



A screenshot of a dropdown menu for 'Auditor'. The menu is open, showing four options: 'Select-' (at the top), 'Federal Auditor', 'PERM Auditor', and 'State Auditor'. The 'State Auditor' option is highlighted with a blue background.

Section 4 – System Access Request, Modification, or Revocation(s)

The information to request access to the BUS, interChange (Bridge), and CCM is in this section, highlighted with the RED boxes. You will only need the information on Page 5.

BUS Existing BUS User ID, if applicable: _____			
<input type="checkbox"/> Long-Term Care Benefit Utilization System (BUS) - BUS is used by Case Management Agencies, Transition Coordination Agencies, Regional Accountable Entities and other contractors to perform case management for long-term care clients.			
<input type="checkbox"/> Local User Access	<input type="checkbox"/> Administrator Access		
County Code: <input type="text" value="Select One-"/>	Class: <input type="text" value="Select One-"/>		
CO interChange Existing CO interChange User ID, if applicable: _____			
<input type="checkbox"/> CO interChange (Production Access to the Bridge) - The Colorado interChange is the Medicaid Management Information System (MMIS) claims processing system. By default, 3 rd Party Users are provisioned with access to view and enter Prior Authorization Reviews based on their user type, organization, and role.			
<input type="checkbox"/> CM User	<input type="checkbox"/> CM Supervisor		
<input type="checkbox"/> Care & Case Management System (MedCompass) –			
select environment(s):			
<input type="checkbox"/> Production	<input type="checkbox"/> Training	<input type="checkbox"/> Other: _____	
select a role:			
<input type="checkbox"/> CMA Supervisor	<input type="checkbox"/> CMA Case Manager	<input type="checkbox"/> Read Only	
<input type="checkbox"/> CIRS- CMA	<input type="checkbox"/> CMA Agency- Billing	<input type="checkbox"/> CMA Agency- Billing Read Only	
<input type="checkbox"/> RAE User	<input type="checkbox"/> Transition Coordinator	<input type="checkbox"/> DOLA	<input type="checkbox"/> Telligen
<input type="checkbox"/> K2 Worklist Access (K2 Worklist access is for Provider Enrollment Application)			
<input type="checkbox"/> Non-HCBS State Reviewer	<input type="checkbox"/> HCBS State Reviewer	<input type="checkbox"/> HCBS & Non-HCBS State Reviewer	
<input type="checkbox"/> Electronic Document Management System (EDMS) <i>*Access is limited to license availability</i>			
Additional DXC System Tools: _____			
PBMS Existing PBMS User ID, if applicable: _____			
<input type="checkbox"/> Magellan's Pharmacy Benefits Management System (PBMS) - <i>*Requires Pharmacy Clinical Supervisor Approval</i>			
<input type="checkbox"/> FirstCI - view only access to the claims system and the pharmacy prior authorizations.			
<input type="checkbox"/> MRx Explore - MRx Explore is Magellan's COGNOS/reporting tool and is for those users who need access to pharmacy reports related to claims and prior authorizations.			
Additional PBMS System Tools: _____			
*** This section to be complete by Pharmacy Clinical Supervisor ONLY for PBMS access***			
Pharmacy Clinical Supervisor Approval: _____ Date: _____			
(Currently Tom Leahey or DeAnn Roecker)			

Updated 11.15.23

For BUS Access, please check:

- If this is a Revocation, please enter existing BUS ID on top line
- Access Level: Local User Access or Administrator Access
- County Code
- Class

****Please note: The BUS is in read-only status and new agencies are not being added.**

For Bridge Access, please check:

- If this is a Modification or Revocation, please enter existing MEUPS ID on top line
- CO interChange
- Access level: CM User or CM Supervisor

For CCM Access, please check:

- Production and/or Training environment
- The role(s) applicable for “minimum access necessary” to perform the job:
 - CMA Administrator – highest level of access
 - CMA Supervisor
 - CMA Case Manager
 - CIRS-CMA – this role is mostly read only through out CCM, but can enter and follow up on CIRS
 - Read Only
 - RAE User
 - Transition Coordinator

****Please note: DOLA access is strictly for state agencies and Telligen access is strictly for Telligen Users.**

Section 5 – Justification

Please use the text box to describe why you are asking for access to the CCM and/or Bridge. If the user has requested Administrator or Supervisor access, this box should explain the reason why the user is needing that level of access.

Section 5 -Justification

REQUIRED - Provide a detailed explanation (in box below) as to why the user needs the access requested.
Access requests **MUST** be tied to a job duty, and only the minimum access necessary to perform job duty, is allowed.
Include reason for Modification/Revocation/Reactivation/Transfer/Name Change (if applicable):

Section 6 – System User Agreement

The User should read the agreement and sign and date below. If this is revocation, the user signature is not needed. The user’s signature must include first and last name.

Section 6 - System User Agreement	
Sign Only If Requesting New Access, Modification(s), or Reactivation. No user signature required for Revocation.	
<p>By signing this System User Agreement (the "Agreement"), you consent and agree to be bound by all of the terms and conditions below. You understand that your access to systems owned or operated by the Department of Health Care Policy and Financing (the "Department") or other Colorado State agencies (the "Systems") is conditioned on your compliance with these terms and conditions. You further understand that any failure to comply with the terms and conditions may result in legal action against you, as well as termination of your user account. This Agreement applies to any/all systems you are granted access to by the Department.</p> <p>You acknowledge and agree that the Systems are owned by the Department, either solely or jointly with another State agency, or its licensors, including, but not limited to any copyrights, patents, trademarks or other proprietary rights (collectively, "IP") contained therein. You further acknowledge and agree that the information that may be accessed through the systems (the "Data") is the confidential information of the Department and the State of Colorado that is regulated by State and Federal laws. You understand that your access to the Systems is a privilege granted by the Department and may be revoked at any time. In addition, you agree that your access to the Systems is conditioned upon your compliance with the following acceptable use policy:</p> <p>Acceptable Use Policy. In accessing the Systems, you agree:</p> <ul style="list-style-type: none">a) To comply with all applicable laws and regulations in your use of the Systems or the Data, including, but not limited to any and all data privacy laws that may apply to the Data;b) To comply with any and all privacy and security policies and procedures provided to you by the Department in your use or access to the Systems and any Data;c) Not to use the Systems or Data in any way that infringes on the rights of any individual, including, but not limited to, any privacy rights or other civil liberties;d) Not to engage in any activity intended to harm, disrupt or infiltrate the Systems, including, but not limited to, introducing any malware, virus, "Trojan Horse" or other malicious code designed to disrupt the functionality of the systems or enable the unauthorized access of the Systems or any Data.e) To access, use or disclose Data created, received, maintained or transmitted through the Systems solely as authorized by the Department; and for no other purpose, and limit your use of the Data solely support the administration and delivery of the Colorado Medicaid Assistance Program;f) Not to copy, modify, reverse engineer, decompile, or create derivative works of the Systems or IP contained therein.	
<p>STATE OF COLORADO - THIRD PARTY INDIVIDUAL CERTIFICATION FOR ACCESS TO PII THROUGH A DATABASE OR AUTOMATED NETWORK Pursuant to § 24-74-105, C.R.S., I hereby certify under the penalty of perjury that I have not and will not use or disclose any Personal Identifying Information, as defined by § 24-74-102(1), C.R.S., for the purpose of investigating for, participating in, cooperating with, or assisting Federal Immigration Enforcement, including the enforcement of civil immigration laws, and the Illegal Immigration and Immigrant Responsibility Act, which is codified at 8 U.S.C. §§ 1325 and 1326, unless required to do so to comply with Federal or State law, or to comply with a court-issued subpoena, warrant or order.</p>	
<p>User ID and Passwords. Upon signing this Agreement, the Department shall provide you with a unique User Identification and temporary password for you to access the Systems. You understand that your User ID and Password are unique to you and may not be shared with any other person. In addition, you understand that you are responsible for any activity that occurs under your User ID. In the event that another person knows or has used your User ID and Password, you must notify your Security Administrator immediately. You also understand that masking your identity or assuming the identity of another user is a violation of this Agreement and the Department’s security policies. You acknowledge and agree that you are solely responsible for securing your password and keeping your password confidential.</p> <p>System Administration. The Department may monitor, track, and record all users and uses of the Systems at any time, including your access to email, websites, and the Internet if you are accessing the Internet through a Department connection. The Department has the right to update the Systems at any time without notice to any users. You agree to report violations, or suspected violations of this Agreement immediately to your Security Administrator. If you are a State employee, you also agree not to use state time, property, equipment, or supplies for private profit or gain, or for any other use not in the interest of the State of Colorado.</p> <p>Security Administrator. If you are designated as a Security Administrator, you further agree to the following obligations:</p> <ul style="list-style-type: none">a) You agree to ensure users are aware of any/all applicable Department Privacy/Security Policies and Procedures and any updates/clarifications provided by the Department.b) You shall establish additional appropriate administrative, technical, procedural, and physical safeguards to ensure the confidentiality, integrity, and availability of client/applicant records and other Data.c) You shall ensure all computers used to access the Systems contain appropriate, updated anti-virus software.d) You shall immediately notify the Department Security Administrator to terminate account access for any user no longer authorized to perform required obligations and responsibilities within the System.e) You shall serve as the Department’s contact for any privacy-security issues that require escalation or investigation.f) You shall immediately report alleged or actual privacy/security incidents to the Department Security Administrator. These would include any/all incidents that could affect the Systems such as virus incidents, unauthorized access, improper use/disclosure of client records and/or information, and any other activity that may be considered a violation, or suspected violation, of this Agreement.	
<p>The Department reserves the right to edit/update this Agreement at any time.</p>	
<p>*Individual Name (First, MI, Last): _____</p>	
<p>*Individual Signature: _____ *Date: _____</p>	
<p>Page 7 of 8</p>	

Section 7 – Manager Authorization

The Manager Authorization is required.

Section 7 – Manager Authorization	
ATTENTION – 3rd Party User - These signatures must be collected PRIOR to submitting the form to the HCPF Contract / Program Manager. Requests for access without all required signatures will not be completed.	
By signing, the signees attest that information provided is accurate, all access requested is the minimum access necessary to perform employee's authorized responsibilities, and a request to remove all prior access no longer needed has been submitted.	
* Individual's Manager Name:	_____ *Phone: _____
* Manager Email address:	_____
* Manager Signature:	_____ *Date: _____

Section 8 – Entity Security Administrator & Contract / Program Manager Authorization

The Security Administrator is the contact at the agency who approves the user's computer/software access at the agency. The Manager and Security Administrator can be the same person, but both sections need to be completed.

HCPF Contract / Program information will be obtained by the HCPF approver at the Department. Do not enter information in this section.

Section 8 – Entity Security Administrator & Contract / Program Manager Authorization	
* Security Administrator or Contract/Program Manager Name:	_____ *Phone: _____
* Security Administrator or Contract/Program Manager Email Address:	_____
* Entity Security Administrator or Contract/Program Manager Signature:	_____ *Date: _____
ATTENTION – HCPF Contract / Program Manager - These signatures must be collected (if applicable) PRIOR to submitting the form to the OIT Service Desk. Requests for access without all required signatures will not be completed.	
* HCPF Contract / Program Manager Signature:	_____ *Date: _____
Additional Authority Approval:	_____ Date: _____