

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"/> Transfer
	<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 BUS 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 bus for over 90 days and account is locked
- Revocation – User is no longer needing access to the BUS or no longer works for your agency
- Transfer – Not applicable

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:	_____
Mailing Address for Fob (if different):	_____
Special Instructions for Receipt of Fob:	_____
*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.

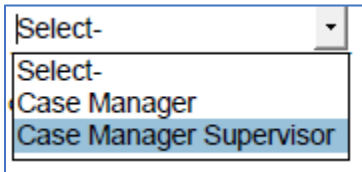
Section 3 – Employer Information

Information is used to assure user is connected to correct agency

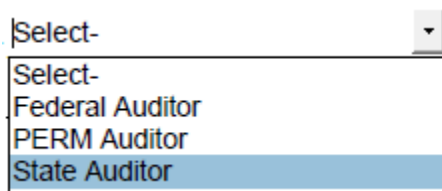
Section 3 – Employer Information	
*Employer Name: _____	*Employer Phone Number: _____
*Employer's Primary Address/City/Zip: _____	
*Type of Entity: <input type="checkbox"/> Fiscal Agent <input type="checkbox"/> MA Site <input type="checkbox"/> PE Site <input type="checkbox"/> State Agency - _____	
<input 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




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



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


The information to request access to the BUS and interChange (Bridge) is in this section, highlighted with the RED boxes. You will only need the information on Page 2 and 5.

Section 4 -System Access Request, Modification, or Revocation(s)	
Please indicate which systems require new access, modification(s), or revocation and current User IDs (if applicable). If modification is being requested, please be specific as to what modification is necessary in the Comments box.	
BIDM	Existing BIDM User ID, if applicable: _____
<input type="checkbox"/> Business Intelligence and Data Management System (BIDM) - The BIDM contains data from the MMIS (Colorado interChange), PBMS, and other data sources. HIPAA requires that persons are limited to the minimum level of protected health information (PHI) necessary to do their jobs (role-based access).	
Advantage Suite Select role: <input type="checkbox"/> PHI or <input type="checkbox"/> NOPHI Select environment: <input type="checkbox"/> PROD and/or <input type="checkbox"/> UAT	
COGNOS Select access: <input type="checkbox"/> COGNOS Consumer (default) and/or <input type="checkbox"/> Other: _____ Select role: <input type="checkbox"/> De-Identified (No PHI) <input type="checkbox"/> Limited Dataset, LDSE (Blinds Provider SSN) <input type="checkbox"/> Limited Dataset, LDSI (Shows Provider SSN) <input type="checkbox"/> Full PHI (All identifiers) Select environment: <input type="checkbox"/> PROD and/or <input type="checkbox"/> UAT	
CMA <input type="checkbox"/> Support <input type="checkbox"/> Consumer <input type="checkbox"/> CMA Group(s): _____	
Token for Solutions Center Access (required for both Advantage Suite & COGNOS) <input type="checkbox"/> Hard-token (FOB) - default	
MOVEit (FTP) <input type="checkbox"/> If checking, please indicate use: _____	
Additional BIDM System Tools: _____	
*** This section to be complete by Health Data Strategy for BIDM-related access***	
	
BIDM Approval: _____ Date: _____ (Approval will be collected after Service Desk submission)	
BUS	Existing BUS User ID, if applicable: _____
<input type="checkbox"/> Long-Term Care Benefit Utilization System (BUS) - The 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	
<input type="checkbox"/> Other Access (Specify): _____	
County Code: Select-	Class: Select-

Updated 2.26.18

For BUS Access, please check:

- If this is a Modification or Revocation, please enter existing BUS ID on top line
- Long-Term Care Benefit Utilization System (BUS)
- Indicate which access level –
 - Local User – for most Case Managers
 - Administrator Access – for Case Management Supervisors or people that will need additional access for their roles
 - Other Access (Specify): - to indicate State Admin Access for vendors
- County Code – Please choose county if applicable
- Class – Select from drop down menu if user is SEP, CCB, or RAE if applicable

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"/> 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 Cathy Traugott and Tom Leahey)			
PEAK Pro	Existing Pro ID, if applicable: _____ Agency ID: _____		
Select only one user type:			
<input type="checkbox"/> Add a Newborn	<input type="checkbox"/> Module Access		
<input type="checkbox"/> Community Based Organization	<input type="checkbox"/> Single Entry Point		
<input type="checkbox"/> Community Centered Board	<input type="checkbox"/> State Authorized Disability Determination Agency		
<input type="checkbox"/> Department of Corrections	<input type="checkbox"/> Veyo – RTD Photo ID		
<input type="checkbox"/> General Pro User			
<input type="checkbox"/> Read Only (check this box if edit access is not appropriate within the user type selected above)			
<input type="checkbox"/> Additional PEAK Pro Access:			
<input type="checkbox"/> Eligibility Check	<input type="checkbox"/> Report My Changes	<input type="checkbox"/> Apply for Benefits	<input type="checkbox"/> RRR
Additional PEAK Pro Access Notes: _____			

For Bridge Access, please check:

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

Section 5 – Justification

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

Section 5 -Justification
<p>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 <u>minimum access necessary to perform job duty</u>, is allowed. Include reason for Modification/Revocation/Reactivation/Transfer/Name Change (if applicable):</p> <div style="border: 1px solid black; height: 180px; width: 100%;"></div>


Section 6 – Authorization

The requesting user’s Manager’s information is needed to complete this section.

Section 6 – Manager Authorization
<p>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.</p> <p>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.</p> <p>*Individual’s Manager Name: _____ *Phone: _____</p> <p>*Manager Email address: _____</p> <p>* Manager Signature: _____ *Date: _____</p> <p style="text-align: center;">Page 6 of 8</p>

Section 7 – System User Agreement

The User should read the agreement and sign and date below. If this is revocation, the user signature is not needed.

Section 7 - System User Agreement	
Sign Only If Requesting New Access, Modification(s), or Reactivation. No user signature required for Revocation.	
<p>By signing this Agreement, you consent and agree to be bound by all of the terms and conditions below, and you understand that any failure to comply with the terms and conditions may result in sanction, which can include termination of your user account. This Agreement applies to any/all systems you are granted access to by the Department of Health Care Policy and Financing. Completion of this Agreement is required before access will be granted. System users are responsible for reading and complying with any/all applicable Department Privacy/Security Policies and Procedures as provided by the Department.</p> <p>System users understand that the Colorado Department of Health Care Policy and Financing (Department) owns, either solely or jointly with another State agency, the system application and all information that can be accessed through the system. Access to the system is restricted to those who have been authorized by the Department and their Security Administrator to enter.</p> <p>System users shall only use/disclose records and/or information that is created, received, maintained, or transmitted within the system as authorized by the Department, and/or as required to perform authorized obligations and responsibilities. System users shall limit use/disclosure of records and/or information concerning Colorado Medical Assistance Program clients or applicants to the purposes directly connected with the administration, operation, or oversight of the Colorado Medical Assistance Program. System users shall not make unauthorized use/disclosure of, or knowingly permit unauthorized access by others to, records and/or information contained within the system.</p> <p>System users shall maintain an assigned, unique User ID. Users understand that they are responsible for any activity that occurs under their individual User ID. In the event that a User suspects that another person knows and/or has used his/her User ID and Password, the User must notify his/her Security Administrator immediately. Additionally, it is a security violation for a User to mask his/her identity or assume the identity of another User. System users shall practice adequate Password management by keeping Passwords confidential. Users shall not share their Passwords with anyone else for any reason, and are discouraged from writing down their Passwords and posting in view of others.</p> <p>System users understand that the Department may monitor, track, and record all Users and uses of the system at any time. (This includes all Internet usage and email, when Department connection is utilized.) System users shall not knowingly cause or allow the addition, modification, destruction or deletion of any records and/or information accessible through the system, except solely in the course of performing their authorized work. System users shall not attempt to alter, exploit, or otherwise interfere with the system application. The State/Department has the right to update the system at any time. System users shall report any violations, or suspected violations of this Agreement immediately to their Supervisor and/or Security Administrator. System users who are also State employees shall not 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>System users who are designated as Security Administrators also have the following responsibilities:</p> <ul style="list-style-type: none"> Authorized Security Administrators shall ensure system users are aware of any/all applicable Department Privacy/Security Policies and Procedures and any updates/clarifications provided by the Department. Authorized Security Administrators shall establish additional appropriate administrative, technical, procedural, and physical safeguards to ensure the confidentiality, integrity, and availability of client/applicant records and/or information created, received, maintained, or transmitted within the system. Authorized Security Administrators shall ensure all computers used to access the system contain appropriate, updated anti-virus software. Authorized Security Administrators 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. Authorized Security Administrators shall serve as the Department's contact for any privacy/security issue that requires escalation or investigation. Authorized Security Administrators shall immediately report alleged or actual privacy/security incidents to the Department Security Administrator. These would include any/all incidents that could affect the system 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 style="text-align: center;"></p> <p>*Individual Signature: _____ *Date: _____</p> <p style="text-align: center;">If requesting access to BUS, interChange for PAR entry, and/or you are a CCB or SEP requesting PEAK Pro access, submit your application to HCPF_OCLSystemApplications@state.co.us for Contract / Program Manger approval. Otherwise, please return completed form to your HCPF Contract/Program Manager. Your HCPF Contract/Program Manager will open an OIT Service Desk ticket for processing.</p> <p style="text-align: center;">Page 7 of 8</p>	

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: _____