Third Party User Requests & Modifications/Revocations Introduction

Third Party User Access Requests and Modifications/Revocations are submitted by Case Management Agencies (CMAs) to request access for their employees to the Department of Health Care Policy and Financing’s (DHCPF) and Benefits Utilization System (BUS).

There are two types of this form:

- Third Party User Access Requests – Required for all NEW users.
- Third Party User Access Modification/Revocation – Required to change user details, including level of access, or to revoke access for existing users.

The “Revised: 021317” version of these forms should be used. This version can be completed and signed electronically. Hand-written versions of these forms are acceptable as long as they are clearly legible.

Requests can be received by the Department in hard copy form by mail, and in soft copy form as either a fax or an email.

Send completed access request forms to: (select one method)

- By Mail: HCPF Information Security Administrator
  1570 Grant St. Denver, CO 80203
- By Fax: 303-866-2803
- By Email: Terry.Burnham@state.co.us
Third Party User Access Request Instructions – Page 1

1. All areas marked with a red asterisk * must be completed.
2. If the user has no middle initial, “NMI” may be used.
3. A four digit numeric identifier, must be provided.

---

**3rd PARTY - NEW USER ACCESS REQUEST**

This Request and Agreement will be used to grant access to the systems the Department administers or maintains. The Request must be completed in full, or it cannot be processed. Incomplete applications will be returned for additional information which may delay access. PLEASE PRINT CLEARLY. No Usernames will be provided until the User has signed the System User Agreement. Any questions should be directed to the HCPF Information Security Unit.

All information provided is used solely for the purpose of providing system access or to verify User’s identity for resetting passwords.

*User Access Start Date: [ ]  *Access Termination Date (if no date provided, contract end-date will be used): [ ]

---

**Section 1 – Individual’s Information**

*First Name: [ ]  *Middle Initial: [ ]  *Last Name: [ ]

*Gender: [ ] Male  [ ] Female  *List any 4-digit numeric identifier: [ ]

*Work Phone: [ ]

*Individual’s Physical Work Address/City/Zip: [ ]

*Work Email Address: [ ]

---

**Section 2 – Entity Information**

*Entity Name: [ ]  *Entity Phone Number: [ ]

*Entity Physical Address/City/Zip: [ ]

*Entity Type: [ ] Fiscal Agent  [ ] MA Site  [ ] PE Site  [ ] State Agency - [ ]

[ ] Case Management Agency - [ ] Auditor - [ ]

[ ] Other - if other, please describe: [ ]
Third Party User Access Request Instructions – Page 2

1. LTC Benefit Utilization System (BUS) must be selected.
2. Select the correct county code from the drop down list.
3. Select the correct class of organization from the drop down list.
1. Please enter a detailed explanation for the access requested.
2. Agency Manager must sign and date.
3. Entity Security Administrator or Contract Program Manager must sign and date.
1. Page 4 will be signed by the BUS Analyst.

**3rd PARTY - NEW USER ACCESS REQUEST**

*HCNP Contract/Program Manager Signature:*
(By signing, the signee attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities, and all prior access no longer needed has been listed.)

**Date:**

**Additional Authority Approval:**
(By signing, the signee attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities.) [If this approval is required, the HCNP Information Security Unit will obtain]

**Date:**

**Pharmacy Clinical Supervisor Approval:**
[Required ONLY for Magellan’s PBMS systems access] [If this approval is required, the HCNP contract manager needs to obtain, PRIOR to submitting the form to the OIT Service Desk]

**Date:**

**Health Data Strategy Approval:**
[Required ONLY for BIDM system access] [If this approval is required, the HCNP contract manager needs to obtain, PRIOR to submitting the form to the OIT Service Desk]

**Date:**

---

**Section 6 - System User Agreement**

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 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 (if any) to enter.

System users are responsible for reading and complying with any/all applicable Department Privacy/Safety Policies and Procedures as provided by the Department.

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 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 make unauthorized use/disclosure of, or knowingly permit unauthorized access by others to, records and/or information contained within the system.

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.

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 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 understand that any violation of this Agreement may be cause for sanction including account termination.
1. New User must Print Full name (including middle initial or NMI), Sign and Date.

**3rd PARTY - NEW USER ACCESS REQUEST**

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.

System users who are designated as Security Administrators also have the following responsibilities:

- Authorized Security Administrators shall ensure system users are aware of any/applicable Department Privacy/Security Policies and Procedures and any updates/clarifications provided by the Department.
- 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 incident 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 attacks, unauthorized access, improper use/dissemination of client records and/or information, and any other activity that may be considered a violation, or suspected violation, of this Agreement.

The Department reserves the right to edit/update this Agreement at any time.

* Individual Name's (First, MI, Last):

* Individual's Signature: ____________________________  * Date: _____________

Please return completed form to:
Your Entity Security Administrator or Contract/Program Manager for approval.
Contract manager will open an OIT Service Desk ticket for processing.
Third Party User Modification/Revocation Request Instructions – Page 1

1. All areas marked with a red asterisk * must be completed.
2. The type of user modification must be indicated.
3. The reason for the change must be indicated.
4. If the user has no middle initial, “NMI” may be used.
5. A four digit numeric identifier, must be provided.

2

3

4

5

3rd PARTY – USER ACCESS MODIFICATION / REVOCATION

This Modification / Revocation Request will be used to modify or terminate access to the systems the Department administers or maintains. This request can only be used for those workforce members who already have access to Department systems. “Revocation” means ALL system access privileges will be revoked. “Modification” means current system access privileges are to be modified – access to certain systems can be revoked, access to additional systems can be requested. The request must be completed in full and signed by the User’s Manager. Managers must immediately notify the HCPF Information Security Unit to terminate account access for any user no longer authorized to perform required obligations and responsibilities within the system.

*Type of Request: [ ] Additional [ ] Modification [ ] Reactivation [ ] Revocation [ ] Transfer

*Name Change - Previous Name:

*Effective Date (If left blank, it is assumed to be immediate):

*Reason for Addition/Modification/Revocation/Reactivation/Transfer/Name Change

Section 1 – Individual’s Information

*First Name: [ ] *Middle Initial: [ ] *Last Name: [ ]

*Gender: [ ] Male [ ] female *List any 4-digit numeric identifier:

*Individual’s Physical Work Address/City/Zip:

*Work Email Address:

Section 2 – Entity Information

*Entity Name: *Entity Phone Number:

*Entity Physical Address/City/Zip:

*Entity Type: [ ] Fiscal Agent [ ] MA Site [ ] PE Site [ ] State Agency -

[ ] Other - If other, please describe:

[ ] Case Management Agency - [ ] Auditor - [ ]
1. Manager and Security Administrator information must be filled in.
2. LTC Benefit Utilization System (BUS) must be selected.
3. Select the correct county code from the drop down list.
4. Select the correct class of organization from the drop down list.
Third Party User Modification/Revocation Request Instructions – Page 3

1. Page 3 must have a detailed explanation for the change requested
2. The form must be signed and dated by the Agency Manager and Security Administrator.

---

**Section 5 - Authorization**

**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. Good Example: “Access to Colorado interChange required to research provider information, for program integrity job function.” Bad Example: “Trackwise access required just in case.” Or “Access needed to do my job.”

---

*Manager Signature:*
*Date:*

(By signing, the signee attests that information provided is accurate, any additional 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 listed.)

*Entity Security Administrator or Contract/Program Manager Signature:*
*Date:*

(By signing, the signee attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities and all access no longer needed has been listed.)
1. Page 4 Will be signed by the BUS Analyst

**HCPF Contract/Program Manager Signature:**
(By signing, the signee attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities and all prior access no longer needed has been listed.)

**Date:**

**Additional Authority Approval:**
(By signing, the signee attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities; if this approval is required, the HCPF Information Security Unit will obtain)

**Pharmacy Clinical Supervisor Approval:**
(Required ONLY for Magellan’s PBMS systems access; if this approval is required, the HCPF contract manager needs to obtain, PRIOR to submitting the form to the OIT Service Desk.)

**Date:**

**Health Data Strategy Approval:**
(Required ONLY for BIDM system access; if this approval is required, the HCPF contract manager needs to obtain, PRIOR to submitting the form to the OIT Service Desk.)

**Date:**

---

**Section 6 - System User Agreement**

*(Sign Agreement Only If Requesting Additional, Modification, or Reactivation)*

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 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 (if any) to enter.

System users are responsible for reading and complying with any/all applicable Department Privacy/Security Policies and Procedures as provided by the Department.

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 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 make unauthorized use/disclosure of, or knowingly permit unauthorized access by others to, records and/or information contained within the system.

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
1. The User must Print their full name (including middle initial), Sign and Date. If this is a revocation and the User is no longer available to sign, please make a note to that effect in the signature entry box.

The Department reserves the right to edit/update this Agreement at any time.

*Individual Name (First, MI, Last):

*Individual Signature:  

*Date: 

Please return completed form to:  
Your Entity Security Administrator or Contract/Program Manager for approval.  
Contract manager will open an OIT Service Desk ticket for processing.