COLORADO
Department of Health Care Policy & Financing

Revised: 07172018

3rd PARTY – SYSTEM USER ACCESS REQUEST

This New, Modification, and Revocation Request will be used to create, modify, or terminate access to the systems the Department administers or maintains. "Modification" means current system access privileges are to be modified – access to certain systems can be revoked, and/or access to additional systems can be requested. "Revocation" means ALL system access privileges will be revoked. 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 User IDs will be provided until the User has signed the System User Agreement. **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.** Any questions should be directed to the HCPF Information Security Unit at hcpfsecurity@state.co.us.

Please return completed form to: Your HCPF Contract/Program Manager. Your HCPF Contract/Program Manager will open an OIT Service Desk ticket for processing.

Section 1 – Type of Request

* Type of Request: ☐ New ☐ Modification ☐ Reactivation ☐ Revocation ☐ Transfer

☐ Name Change - Previous Name: _____

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

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: _____

Section 3 – Employer Information

*Employer Name: _____ *Employer Phone Number: _____

*Employer's Primary Address/City/Zip: _____

*Type of Entity: ☐ Fiscal Agent ☐ MA Site ☐ PE Site ☐ State Agency - _____

☐ Case Management Agency Select- _____ ☐ Auditor Select- _____

☐ Other - If other, please describe: _____

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: _____

☐ **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: ☐ PHI or ☐ NOPHI

Select environment: ☐ PROD and/or ☐ UAT

COGNOS

Select access: ☐ COGNOS Consumer (default) and/or ☐ Other: _____

Select role: ☐ De-Identified (No PHI)

☐ Limited Dataset, LDSE (Blinds Provider SSN)

☐ Limited Dataset, LDSI (Shows Provider SSN)

☐ Full PHI (All identifiers)

Select environment: ☐ PROD and/or ☐ UAT

Token for Solutions Center Access (required for both Advantage Suite & COGNOS)

☐ Hard-token (FOB) - default

MOVEit (FTP) ☐ 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: _____

☐ **Long-Term Care Benefit Utilization System (BUS)** - The Long Term Care Benefit Utilization System is used by Single Entry Point and Community Centered Board staff to perform case management for long term care clients.

☐ Local User Access ☐ Administrator Access

☐ Other Access (Specify): _____

County Code: Select- _____ Class: Select- _____

CBMS Existing CBMS User ID, if applicable: _____

☐ **HCPF CBMS Web Portal (MA/PE) (MA Sites, PE Sites and other CBMS HCPF Contractors)** - The Colorado Department of Health Care Policy and Financing CBMS Web Portal provides access to the Colorado Benefits Management system community for Medical Assistance Sites, Presumptive Eligibility Sites and other HCPF contractors determining eligibility for the State medical assistance programs. The Colorado Benefits Management System is used by the counties and Medical Assistance Sites to determine Program eligibility. Default access includes inquiry access to alerts, scanning, traffic log, case comments, client referral, application intake, interactive interview, case assignment, eligibility, authorization, redetermination, eligibility spans, and medical ID card requests. Proof of completion of online and interactive training is required prior to access being granted.

☐ I have attached proof of completion of online and interactive training (required prior to access being granted).

CBMS Environments

☐ TRN (User Training- includes User Practice) ☐ Production

CBMS Special Exception Environments (State Personnel Only)

☐ PROD03 (Test) ☐ UAT (Test) ☐ INT (Tables) ☐ CONV (CBMS prior to Oct 2013)

☐ SIT1 ☐ SIT2 ☐ SIT3 ☐ SIT4

CBMS Special Exceptions Access

☐ Confidential Cases ☐ Statewide Caseload Access Rights ☐ CHP Fee Enrollment (Update)

Override Access - Override Waiver/Agreement required for override access

☐ I have included waiver

☐ EDBC ☐ MA ☐ AwDC WaitList

PEAK Inbox

☐ Portal (Documentation) ☐ PEAK (CBMS) ☐ Inquiry ☐ Update

CBMS Caseload Models

☐ EEMAP Model – Agency Office has four caseloads assigned to a service user ID which acts as the gatekeeper (intake, ongoing, transfer and closed with “carry cases” set to yes, except for the closed caseload)

☐ Medical Assistance Site Model – Each individual eligibility enrollment specialist has their own intake and ongoing caseloads, but the intake “carries cases” is set to no. The gatekeeper will have the intake closed and transfer caseloads set to “carry cases”. This model may vary according to the Medical Assistance Site’s business processes. One other option for this model - Each eligibility enrollment specialists may have their own intake and ongoing caseload and both set to “carry cases”. The gatekeeper in this option will only have the transfer and closed caseloads.

☐ PE Model – Each individual user has an intake caseload only. Each PE office has a closed caseload only.

☐ Healthy Communities/EPSDT – Users do not have a caseload. Users have update access to request medical assistance cards only.

☐ OCC Model - Agency Office has four caseloads assigned to a service user ID which acts as the gatekeeper (intake, ongoing, transfer and closed with “carry cases” set to yes, except for the closed caseload)

CBMS Access User Roles

☐ **Auditor -** This user access role should be assigned to State Auditors and other specified auditors. Users do not have caseloads. Users will have management inquiry a*ccess*.

☐ **Management -** This user access role should be assigned to managers, supervisors, quality assurance, trainers, lead workers, or those serving as liaison between the Department and the contract agency. Users generally do not have caseloads. Users will have *supervisory update access*.

☐ **Eligibility Enrollment Specialist (EES) -** This user access role should be assigned to Department and contracted Eligibility/Enrollment Staff. Users have caseloads. Users will have *update access* in all relevant windows.

☐ **Eligibility Enrollment Support (ES) (Specify Update Access Needed) –** _____

This user access role should be assigned to users who provide general eligibility/enrollment support. Users do not have caseloads. Users will have specified update access according to business need and approval.

☐ **Customer Service -** This user access role should be assigned to users who provide customer service. Users do not have caseloads. Users will have inquiry access only.

☐ **Gatekeeper (Each agency will designate a Gatekeeper)** - This user access role should be assigned to a user(s) tasked with managing agency cases. Responsible for ensuring cases of departing workers are transferred to other workers.

☐ Transfer Cases ☐ Closed Cases ☐ Intake ☐ Ongoing

☐ **Healthy Communities Outreach Worker/EPSDT -** This user access role should be assigned to Healthy Communities personnel. Users do not have a caseload. Update access only in reissuance of Medical Identification Cards.

☐ **Presumptive Eligibility -** This user access role should be assigned to presumptive eligibility contractors. Users have an intake caseload. Users have specified update access.

☐ **TPL Worker (Designated TPL and Fiscal Agent staff only) -** This user access role should be assigned to State and HCPF Fiscal Agent Personnel only. Users do not have caseloads. Users have limited update access.

☐ Other/Additions/Exceptions: _____

High Level Program Groups / Caseload - Please indicate High Level Program Group and Caseload access rights. Any questions should be directed to your supervisor and/or security administrator.

High Level Program Groups	**Intake**	**Caseload? Carries Cases**	**Ongoing**	**Carries Cases**	**List of Caseload Parameters/Special Indicators** (Including: languages, alpha assignment, etc)
☐ **Medical Assistance Programs**	☐	☐ yes ☐ no	☐	☐ yes ☐ no	_____
☐ **Presumptive Eligible Medical**	☐	☐ yes ☐ no	☐	☐ yes ☐ no	_____

☐ **Program Eligibility and Application Kit** (CBMS PEAK Interface) - The PEAK application is a self-service online tool used by individuals to screen for potential eligibility for assistance programs and check current eligibility status. Access is granted to designated users only.

☐ Portal (Documentation) ☐ PEAK (CBMS) ☐ Inquiry ☐ Update

☐ **CBMS-DSS (COGNOS)** - The CBMS Decision Support System contains report data taken from the CBMS. Default access is limited to retrieval of designated pre-defined reports. Proof if interactive training is required prior to access being granted. Query and Report access is limited to license availability.

☐ View ☐ Query ☐ Report

CO interChange

Existing CO interChange User ID, if applicable: _____

☐ **CO interChange** (Production Access) **-** The Colorado interChange is the Medicaid Management Information System (MMIS) claims processing system.

☐ **K2 Worklist Access** (K2 Worklist access is for Provider Enrollment Application)

☐ Non-HCBS State Reviewer ☐ HCBS State Reviewer ☐ HCBS & Non-HCBS State Reviewer

☐ **Electronic Document Management System (EDMS)** **Access is limited to license availability*

Additional DXC System Tools: _____

PBMS

Existing PBMS User ID, if applicable: _____

☐ **Magellan's Pharmacy Benefits Management System (PBMS)** - **Requires Pharmacy Clinical Supervisor Approval*

☐ FirstCI - view only access to the claims system and the pharmacy prior authorizations.

☐ 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)

SAVE

Existing SAVE User ID, if applicable: _____

☐ **Systematic Alien Verification for Entitlements** (SAVE) - The application provides access to the SAVE system for determining immigration status, which is required for determining a non- citizen applicant's eligibility for many public benefits.

OTHER SYSTEMS

☐ **Other Systems** (Please Specify) - _____

☐ **Special Exemptions Requested:** _____

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 - 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: _____**

* 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: _____

Section 7 - System User Agreement

Sign Only If Requesting New Access, Modification(s), or Reactivation. No signature required for Revocation.

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.

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.

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.

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 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.

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

- 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.

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 HCPF Contract/Program Manager. HCPF Contract/Program Manager will open an OIT Service Desk ticket for processing.