3rd PARTY – SYSTEM USER ACCESS REQUEST

This request is used to create, modify, or terminate access to systems the Department administers or maintains.

- "Modification" means changes to access roles within systems the user has already been granted access to.
- "Revocation" means ALL system access privileges indicated will be revoked. Managers must immediately submit a revocation request form to terminate account access for any user no longer authorized to perform responsibilities within the system(s).
- Both "Revocation" and "New" request forms should be submitted when transferring from one agency to another.

The Request must be completed in full.

- Incomplete applications will be rejected and require re-submission which may delay access.
- No User IDs will be provisioned until the User has signed the System User Agreement.

Applications are valid for 30 days from the signature date.

- If you are a Case Manager requesting access to interChange, Care & Case Management System (MedCompass), and/or PEAKPro, submit your application to HCPF_OCLSystemApplications@state.co.us for Contract / Program Manager approval and final submission.
- Otherwise, please return the completed form directly to your HCPF Contract / Program Manager to be completed.
- Any questions related to this form can be directed to HCPF_Security@state.co.us.

Upon completion, the HCPF contact should submit the application to ServiceHub > Request a Service > *HCPF 3rd Party Access Request* for processing by the *Access Control HCPF* group.

Section 1 – Type of Request

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

☐ 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: _____

*Work Email Address: _____ *****Work Phone: _____

*Individual's Physical Work Address/City/Zip: _____

Section 3 – Employer Information

*Employer Name: _____ *****Employer Phone Number: _____

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

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

☐ BHA   ☐ Fiscal Agent   ☐ LCA   ☐ Managed Care Entity / RAE   ☐ PCMP / Provider   ☐ TC   ☐ PCC Optum

☐ Case Management Agency _____   ☐ Auditor _____

☐ 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 provide any current User IDs (if applicable). If a modification is requested, please be specific as to what modification is necessary in the Comments box.

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).

☐ Fax Number Required for Access: _____

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

☐ **Medical Assistance (MA) 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.

☐ Intake / Carries Cases: ☐ Yes   ☐ No

☐ Ongoing / Carries Cases: ☐ Yes   ☐ No

☐ **Presumptive Eligible (PE) Model** – Each individual user has an intake caseload only. Each PE office has a closed caseload only.

☐ Intake / Carries Cases: ☐ Yes   ☐ No

☐ Ongoing / Carries Cases: ☐ Yes   ☐ No

List of Caseload Parameters/Special Indicators: _____

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

☐ **Hospital Presumptive Eligibility -** This user access role should be assigned to hospital presumptive eligibility contractors.

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

☐ Other/Additions/Exceptions: _____

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

☐ View   ☐ Query   ☐ Report

☐ **County Dashboard** – This tool provides information for all high-level program groups currently operating within CBMS to monitor program workflow and guide decisions about how to manage workload.

☐ **MAP Dashboard** – This Tableau tool is provisioned by OIT DATA. A ticket will be entered to ServiceHub for OIT DATA to manage access requests.

Soft Token for CBMS Access (required for CBMS Web Portal & COGNOS – select only one)

☐ Desktop, select one: ☐ Windows, Version: _____ or   ☐ Mac OS

☐ Phone, cell number _____ and select type: ☐ Android or ☐ iOS (Apple)

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.

☐ **CO interChange** (Production Access to the Bridge) **-** The Colorado interChange is the Medicaid Management Information System (MMIS) claims processing system. By default, 3rd Party Users are provisioned with access to view and enter Prior Authorization Reviews based on their user type, organization, and role.

  select environment(s):

   ☐ Production   ☐ Training   ☐ Other: _____

  select role(s):

   ☐ CM User   ☐ CM Supervisor   ☐ Transition Coordinator (TCA)   ☐ MMIS_IC_EDMS_OPTUM

☐ **Care & Case Management System (MedCompass)**

  select environment(s):

   ☐ Production   ☐ Training   ☐ Other: _____

  select a role:

   ☐ CMA Supervisor   ☐ CMA Case Manager   ☐ CES_SLS Exception Review

   ☐ CIRS- CMA   ☐ DOLA   ☐ PASRR   ☐ RAE User

   ☐ Read Only   ☐ Telligen   ☐ Transition Coordinator (TCA)

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

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

Additional Gainwell Tools: _____

☐ **Enterprise Data Warehouse (EDW)** - The EDW database 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).

  ☐ **COGNOS**

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

   Select role: ☐ De-Identified (No PHI)   ☐ Limited Dataset, LDSE (Blinds Provider SSN)

                   ☐ Full PHI (All identifiers) ☐ Limited Dataset, LDSI (Shows Provider SSN)

  ☐ **CMA**

   Select access: ☐ Consumer (default) ☐ Query Author ☐ CMA Group: _____

  ☐ **MOVEit (FTP)** *Specify folder(s) in justification box later in form; for each folder requested, specify R / W / D / N access for each*

   Select environment: ☐ PROD   and/or   ☐ UAT

   Select access point: ☐ Web Portal and/or   ☐ FTP Client Application

   Select access*: ☐ Read   ☐ Write   ☐ Delete   ☐ Notifications

┌──┐
│   ***** This section to be completed by Decision Support for EDW-related access*****   │
│   │
│   **EDW Approval:** _____ **Date:** _____   │
│   (Currently Deepika Amarachinta)   │
└──┘

PBMS (Magellan – PT)   Existing PBMS User ID, if applicable: _____

☐ **Magellan's Pharmacy Benefits Management System (PBMS)** - *Requires Pharmacy 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.

> ***** This section to be complete by Pharmacy Clinical Supervisor ONLY for PBMS access*****
>
> **Pharmacy Clinical Supervisor Approval: _____ Date: _____**
> <div align="center">(Currently Tom Leahey or DeAnn Roecker)</div>

PBMS (MedImpact)   Existing PBMS User ID, if applicable: _____

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

    ☐ **MedCommand** – access to PBM applications including MedOptimize®, MedAccess®, and MedResponse to monitor and manage pharmacy benefits. Required to be able to access all other applications.

        ☐ **MedAccess** Administrative User- read only access to the claims system and the pharmacy prior authorizations.

        ☐ **MedOptimize** Report Query Builder - reporting tool that allows users to create ad-hoc reports containing member, claim, prior authorization, and drug information.

> ***** This section to be complete by Pharmacy Clinical Supervisor ONLY for PBMS access*****
>
> **Pharmacy Clinical Supervisor Approval: _____ Date: _____**
> <div align="center">(Currently Tom Leahey or DeAnn Roecker)</div>

PEAK Pro   Existing Pro ID, if applicable:_____   Agency ID:_____

☐ **PEAK Pro**

Select *only one* user type:

☐ **ADAP (ADP)**	☐ **Department of Corrections (DOC)**
☐ **Add a Newborn (ANB)**	☐ **LTSS Case Management Agency**
☐ **Behavioral Health Administration (BHA)**	☐ **Women, Infants and Children (WIC)**
☐ **Community Based Organization (CBO)**	

Note: *Organization must be created in Peak Pro prior to access request for individual user(s)*

Indicate Affiliated Organization: _____

Additional PEAK Pro Access Notes: _____

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 <u>minimum access necessary to perform job duty</u>, is allowed.

Include reason for Modification/Revocation/Reactivation/Transfer/Name Change (if applicable):

Section 6 – 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 be rejected.

If you are a Case Manager requesting access to interChange, Care & Case Management System (MedCompass), and/or PEAKPro, submit your application to HCPF_OCLSystemApplications@state.co.us for Contract / Program Manager approval and final submission.

Otherwise, please return the completed form to your HCPF Contract / Program Manager.
Your HCPF Contract / Program Manager will submit the completed form to ServiceHub to create a ticket for processing.

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:** _____

If your organization has identified an Entity Security Administrator, please complete this section:

Entity Security Administrator Name: _____Phone: _____

Security Administrator Email Address: _____

Entity Security Administrator Signature: _____ **Date:** _____

Section 7 – HCPF Contract / Program Manager Authorization

ATTENTION – HCPF Contract / Program Manager - These signatures must be collected (if applicable) PRIOR to submitting the form to ServiceHub. Requests for access without all required signatures will be rejected.

* HCPF Contract /
Program Manager Signature: _____ ***Date:** _____

Additional Authority Approval: _____ **Date:** _____

Section 8 - System User Agreement

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

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.

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:

Acceptable Use Policy. In accessing the Systems, you agree:
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.

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.

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.

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.

Security Administrator. If you are designated as a Security Administrator, you further agree to the following obligations:
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.

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

*Individual Name (First, MI, Last): _____

*Individual Signature: _____ ***Date:** _____