COLORADO
Department of Health Care Policy & Financing

Department of Health Care Policy & Financing

THIRD PARTY 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 Department's Information Security Officer or Department's Information Security Administrator.

All information provided is used solely for the purpose of providing system access.

User Access Start Date:_____ Access Termination Date: _____
If no date is provided, contract term end date will be used.

Section 1. User Information

First Name:_____ Middle Initial:_____ Last Name: _____

Gender: ☐ Male ☐ Female

Telephone Number_____ Work E-Mail Address: _____

Last four digits of SSN:_____ or any other 4 digit numeric identifier: _____
This information is used solely to verify User's identity for resetting passwords.

Department Type: ☐State Agency ☐Fiscal Agent ☐MA Site ☐PE Site ☐Other _____

If other, please describe: _____

Agency Name:_____ Trading Partner ID # (if applicable): _____

Agency Work Address/City/Zip:_____

Work Telephone: _____ Work Email address: _____

Section 2. User's Manager / Agency Security Administrator Information

Agency Security Administrator Name: _____

Telephone:_____ Email address: _____

Manager Name: _____

Manager Signature: _____ DATE: _____

Telephone:_____ Email address: _____

Please return completed form to: HCPF Information Security Administrator, 1570 Grant Street, Denver, CO 80203-1818

COLORADO
Department of Health Care Policy & Financing

Department of Health Care Policy & Financing

Section 3. System Access Requested

Please indicate what systems you are requesting access to. Upon request and approval, default inquiry-only access will be provided for the following systems, unless a special exception is requested below and authorized. Contact your Supervisor and/or Security Administrator for more information on exceptions if needed.

☐ **MMIS** Do you need installation: ☐Yes ☐No ☐Remote Access (only for specified users)
The Medicaid Management Information System is the claims processing system. Default access is inquiry into claims, provider and client data, prior authorizations, reference (procedure and revenue codes), and rates.

☐ **MMIS-DSS (COGNOS)** ☐ View ☐ Query Studio ☐ Report Studio
The MMIS Decision Support System contains data taken from the MMIS. Default access is inquiry access to claims, provider and client data, and prior authorizations.

☐ **COLD** Do you need installation: ☐Yes ☐No ☐ Remote Access (only for specified users)
The Computer Output to Laser Disk Report Manager is where reports from the MMIS are stored for easy retrieval. Default access is access to reports generated from the Claims system (including the Provider Claim Report), Management and Administrative Reporting (MAR), Managed Care, Client, Provider, and
Third Party.

☐ **PDCS (PDCS Access form also required)**
The Prescription Drug Claim System is the claims processing subsystem of the MMIS that is used for drug claims. Only users with special permission are allowed access to this subsystem.

☐ **CBMS (CBMS Access form also required)**
The Colorado Benefits Management System is used by the counties and Medical Assistance Sites to determine Program eligibility. Default access is inquiry access to alerts, scanning, traffic log, case comments, client referral, application intake, interactive interview, case assignment, eligibility, authorization, predetermination, eligibility spans, and medical ID card requests. Completion of the Computer Based Training is required prior to access being granted.

☐ **CBMS-DSS** ☐ View ☐ Query Studio ☐ Report Studio
The CBMS Decision Support System contains report data taken from the CBMS. Default access is limited to retrieval of designated pre-defined reports.

☐ **Program Eligibility and Application Kit (PEAK) (CBMS Access Form also required)**
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.

☐ **LTC Benefit Utilization System County Code____ Class (SEP, DD, etc) __**
The Long Term Care Benefit Utilization System is used by county and Single Entry Point staff to perform case management for long term care clients.

☐ **COFRS (Vendor Access) Financial Data System Access Form also required**
The Colorado Financial Reporting System is the statewide accounting system used as the official book of entry for accounting activity. Default access is inquiry access to those tables and transactions related to the Department.

☐ **TSO**
The Top Secret program is used to send data between specified entities through the State mainframe system.

☐ **HCPF Secured Sites Portal**
The Colorado Department of Health Care Policy and Financing Secured Sites Portal provides access to the Medical Assistance Program services for Providers and other Third Party users.

☐ **HCPF CBMS WEB PORTAL**
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.

☐ **SAVE (Systematic Alien Verification for Entitlements):** _____
This is the U.S. Department of Homeland Security verification information system.

☐ **Special Exceptions Requested:** _____

☐ **Other Systems Requested:** _____
(May require additional application and approval)

Agency Contract Manager Signature:_____ **Date:** _____
(By signing, Agency Contract Manager attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities.)

HCPF Contract or Program Manager Signature:_____ **Date:** _____
(By signing, Department Contract Manager and or Program Manager attests that information provided is accurate and all access requested is necessary for User to perform authorized responsibilities.)

Please return completed form to: HCPF Information Security Administrator, 1570 Grant Street, Denver, CO 80203-1818

COLORADO
Department of Health Care Policy & Financing

Department of Health Care Policy & Financing

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/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 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.

Department of Health Care Policy & Financing

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.

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.

User Name (First, MI, Last): _____

User Signature:_____ Date: _____

Please return completed form to: HCPF Information Security Administrator, 1570 Grant Street, Denver, CO 80203-1818