Managed Care Organizations (MCOs) should use this Instruction Guide to assist users in requesting access to specified DHS systems including eCIS, PROMISe, DocuShare and the HealthChoices Extranet.

Security Access Request Instruction Guide for MCO Business Partner Users

BDCM Security Access Team

Table of Contents

OVERVIEW

The Bureau of Data and Claims Management (BDCM) MCO Monitoring Unit is responsible for facilitating and/or approving Security Access Requests for Physical HealthChoices (PH), Community HealthChoices (CHC), Children's Health Insurance Program (CHIP), and Dual Eligible Special Needs Plan (D-SNP) MCO Business Partners who are requesting access to the following DHS systems**: eCIS, PROMISe Intranet, DocuShare and the HealthChoices Extranet.**

MCO Business Partner users **must** have a b-account user ID and password and have completed a self-registration process for access to eCIS, PROMISe Intranet, and DocuShare.

To access the HealthChoices Extranet, Business Partner users **must** have a Microsoft Account. For access to the HealthChoices forms located within HealthChoices Extranet, users will also need to complete a b-account self-registration (refer to pages 9-10 for Extranet access instructions).

IMPORTANT NOTE: One registration does not automatically give access to all systems. A new user should first register for one system to receive their b-account user ID. Once they receive their b-account user ID, they should then register as an "Existing Business Partner User" when registering for any additional system.

Self-registration links for each system is located on their respective login pages (except for DocuShare which is done through the PROMISe Intranet self-registration process). **If a user already has a b-account user ID, self-registration for DocuShare is not needed.** Additional instruction can be found on pages 8 - 9 under the DocuShare section of this Instruction Guide.

BDCM does not approve Behavioral Health (BH) MCO registrations for eCIS, PROMISe Intranet or DocuShare. BH-MCO users must contact the Office of Mental Health and Substance Abuse Services (OMHSAS) mailbox at RA-PW-BHMCOSecurityR@pa.gov.

CAPS access is managed by the CHIP office. Questions regarding CAPS access should be sent to your respective CHIP contacts.

COMPASS access is managed by the Office of Income Maintenance (OIM). Questions regarding COMPASS access should be directed to RA-PWCOMPASSCP@pa.gov.

Business Partner access for users located outside of the continental United States and Hawaii is not permitted.

MCO DELEGATED ADMINISTRATOR RESPONSIBILITIES

- MCO Delegated Administrators (DAs) are responsible for facilitating MCO Business Partners Security Access Requests. They also act as DHS Points of Contact for any questions or concerns relating to security access. Each MCO may appoint up to 4 (four) Delegated Administrators.

- To become a DA, users must register through the eCIS self-registration process.

- DAs must process the 1st level approval for all eCIS registrations within Identity Manager. After the DA processes the 1st level approval, the request will then come to BDCM to process the 2nd level/final approval.

- Additional information regarding DA registration and eCIS DA 1st level approval can be found in the eCIS Registration Guide located on the DHS Website.

- DAs can revoke user access to eCIS at any time (e.g., if a user is no longer employed by the MCO).

- For PROMISe Intranet and DocuShare security access requests, DAs must email the BDCM Security Access Request Mailbox, RA-PHMCOSecurityReq@pa.gov, stating that the specified MCO user has been approved to request access. This email must be sent to BDCM **prior** to the user requesting access through the self-registration process.

- DAs are required to complete Quarterly PROMISe Intranet Recertifications and Annual eCIS User Recertifications.
    - These are used to verify current users and determine which users should have their access revoked.
    - DHS will also provide MCOs with additional quarterly eCIS user reports to assist the DAs with keeping track of how many of their staff are using eCIS.
    - In order to access the PROMISe Recertifications, DAs must register for the PROMISe role.
    - Additional instruction can be found in the PROMISe Intranet and eCIS sections of this Instruction Guide or DAs can contact the BDCM Security Access Request Mailbox, RA-PHMCOSecurityReq@pa.gov, for further information.

- If there are any staff changes to an MCO's DA contact list, a current DA must send an e-mail to RA-PHMCOSecurityReq@pa.gov listing the information for the new DA **prior** to the new DA registering through the eCIS self-registration process and/or the information of the former DA to be removed from the eCIS system.

- Additional DA responsibilities and clarifications on the bullet points above are listed in each system process outlined in this Instruction Guide.

MCO DELEGATED ADMINISTRATOR CONTACT LIST (PH, CHC, CHIP, D-SNP)

MCO NAME	DA CONTACT INFORMATION
Aetna Better Health (CHIP)	Sosi Hovagimian - HovagimianS@aetna.com Mindy Dunlap – mdunlap@aetna.com
Aetna Health Inc. (D-SNP)	Lori Chestnut – lxchestnut@aetna.com Rose Hellwarth – hellwarthr@aetna.com Stephanie Bruce – bruces2@aetna.com Leah Hoffman - lmsendi@cvshealth.com
AmeriHealth Caritas/Keystone First (PH, CHC, CHIP, D-SNP)	Shirleyah Roane - sroane@amerihealthcaritas.com Nicole Smith – nlsmith@keystonefirstpa.com Tyeisha McNeil - tmcneil@amerihealthcaritas.com Ellan Baumgartner - ebaumgartner@amerihealthcaritas.com
Bravo Health Pennsylvania, Inc. (D-SNP)	Catherine Powers - catherine.powers@cigna.com Lara Walden - lara.walden@cigna.com Ryan Saxon - ryan.saxon@cigna.com Tammie Christie - tamatha.christie@cigna.com
Capital Blue Cross (CHIP)	Tara Whitcomb - Tara.Whitcomb@capbluecross.com Brook King - Brook.King@capbluecross.com Glenda Crimmel - Glenda.Crimmel@capbluecross.com
Geisinger Health Plan (PH & CHIP)	Andrew Centrone - amcentrone@thehealthplan.com Susan Leitzell - stleitzell@thehealthplan.com
Health Partners Plans (PH, CHIP, D-SNP)	Tosha Fleming - TFleming@jeffersonhealthplans.com Michelle Fogg -MFogg@jeffersonhealthplans.com Chava Kintisch – ckintisch@jeffersonhealthplans.com Jeanine Datts – jdatts@jeffersonhealthplans.com
Highmark Choice Co. - Highmark Healthy Kids (CHIP)	Stacey Bloom - stacey.bloom@highmark.com Diana Kobus - diana.kobus@highmark.com Connie Thomas - connie.thomas@highmark.com Rich Linn - richard.linn@highmark.com
Highmark Wholecare (formerly Gateway) (PH, D-SNP)	Rebecca McDaniels - rmcdaniels@highmarkwholecare.com Cherri Samuel-Chitwood - csamuel-chitwood@highmarkwholecare.com Christopher Santoro – csantoro@highmarkwholecare.com
Humana Insurance Company (D-SNP)	Rebecca Harbison - rjohnson55@humana.com Heather Woloch - hwoloch@humana.com Misty Tudor - mtudor1@humana.com
Keystone Health Plan East - aka Independence Blue Cross (CHIP)	Joanne Fifield - joanne.fifield@ibx.com Eileen Santos-Galarza - e.santos-galarza@ibx.com
PA Health & Wellness (CHC, D-SNP)	Joshua Leh - Joshua.Leh@pahealthwellness.com Samuella Williams - Samuella.Williams@pahealthwellness.com Christina Lennon – Christina.Lennon@pahealthwellness.com
United HealthCare (PH, CHIP, D-SNP)	Julie Bilbrey – Julie_s_bilbrey@uhc.com Michael Dick - Michael.Dick@uhc.com Benjamin Hughes – Benjamin.c.hughes@uhc.com
UPMC (PH, CHC, CHIP, D-SNP)	Jason Rabbitt - rabbittj@upmc.edu Qudsia Saleem – saleemq@upmc.edu Kathleen Pulkowski - pulkowskik@upmc.edu Susan Zimmerman - zimmse@upmc.edu

SECURITY ACCESS REQUEST PROCEDURES

To request access to eCIS, PROMISe Intranet, DocuShare, HealthChoices Extranet, or HealthChoices Forms, please follow the appropriate procedures, per system type, within this Instruction Guide. Existing Business Partner users will log in to do the applicable self-registrations. If a user does not know their password, they should contact the DHS Helpdesk, 1-800-281-5340, to have it reset.

New Users (who do not have a b-account user ID) – Please contact your MCO Delegated Administrator for the MCO Tax ID you must use when registering for DHS systems.

If a user is registering as a new user and receives an error that the email address is already used, it means that either they already have a b-account user ID associated with that email address **or** their email address was recycled from a previous user. **Do not try to register using another email address**. Users should contact their DA who will contact BDCM to determine the issue.

Be aware of the following when going through the Self-Registration process:

- ✓ Users create their own password.
- ✓ The security questions are case sensitive.
- ✓ The b-account user ID is sent through email; therefore, users must make sure to correctly enter their work email address**. Personal email addresses are not permitted.**

eCIS ACCESS (PH, CHC, CHIP, D-SNP MCOs)

eCIS allows users to look up recipient/participant information (e.g., medical assistance and managed care eligibility, TPL, address, household member composition, facility code and waiver code information, etc.).

eCIS Inquiry Only Access is 24 hours a day, 7 days a week except when the system is down for maintenance.

eCIS can only be accessed via Google Chrome or Microsoft Edge browsers. Internet Explorer cannot be used.

User Responsibility to Request Access:

- Navigate to the eCIS Registration Link via the eCIS Login Page.
  - Click on *Business Partner Login*.
  - Click on *Register for eCIS* under *Self-service for Business Partner.*

- **Existing b-account ID Users:**
  - Click on *Existing Business Partner Account – CLICK HERE* (located beneath the Welcome paragraph).
  - Users should log in using their b-account user ID and password.
  - Follow the instructions for registering.
  - On the Organization Information page, users **must** select the Option for:
    - Program Office: Office of Medical Assistance Programs (OMAP)
    - Business Category: MA Managed Care Organization – Physical Health
  - On the Organization Role page, users **must** select "I am a non-Administrative Business Partner user".
  - When entering the Electronic Signature, the user's name **must** match what is listed in their profile. There should be a single space between the first and last name and no spaces before or after.

- **New Users (who do not have a b-account user ID):**
  - Click NEXT and follow the instructions for registering.

- Users **must** enter the correct **Organization Tax ID** with no dashes. The DA will provide this information.
- On the Organization Information page, users **must** select the Option for:
  - Program Office: Office of Medical Assistance Programs (OMAP)
  - Business Category: MA Managed Care Organization – Physical Health
- On the Organization Role page, users **must** select "I am a non-Administrative Business Partner user".
- When entering the Electronic Signature, the user's name **must** match what is listed in their profile. There should be a single space between the first and last name and no spaces before or after.

MCO Delegated Administrator Responsibility:

- The DA processes the 1st level approval for eCIS user registrations within Identity Manager. 2nd level/final approval is processed by BDCM.

- Identity Manager can be accessed via the link in the eCIS registration notification or directly via Identity Manager.

- DAs can revoke eCIS access at any time.
  - Navigate to Identity Manager and log in.
  - Click on Business Partner Management tab.
  - Under Tasks, click on Manage Users then click Revoke eCIS Application Access.
  - Search for the user by b-account ID, Last Name, First Name, or Email. Click on Select.
  - Check off the role for MA Managed Care Organization – Physical Health.
  - Enter Comments as to why access is being revoked.
  - Choose the Revocation Reason from the drop-down list and click Submit.

- DHS will provide quarterly MCO user reports for eCIS to assist the DAs in keeping track of their users. DAs can contact the BDCM Security Access Request Mailbox for further information.

- eCIS User Recertification:
  - DHS (RA-PWUAC@pa.gov) will send an Action Required email to the DAs on a yearly basis for access to the MCO's list of users with eCIS access.
  - The DAs will click on Start Task within the email and then log into the SailPoint tool with their b-account ID and password.
  - On the right side under Decision, the DAs must indicate if a user's access is Approved or Revoked.
  - The recertification process is also outlined in the eCIS Access Recertification Guide. DAs can contact the RA-PHMCOSecurityReq@pa.gov mailbox to request a copy.

Additional information regarding eCIS registration and DA 1st level approval can be found in the eCIS Registration Guide located on the DHS Website. The Guide can also be accessed via a link provided on the Welcome Page of the eCIS Registration Tool.

PROMISe INTRANET ACCESS (PH, CHC, CHIP MCOs)

PROMISe Intranet provides access to Provider, Claim, Prior Authorization, Reference File and Eligibility Verification System (EVS) information. Access allows users to look up:

- Provider information regarding providers enrolled in Medical Assistance (MA).
- Prior authorizations approved by MA (will need the prior authorization number).
- Reference file information in PROMISe (e.g., Diagnosis and Procedure Code).
- EVS information (e.g., Provides the most current eligibility status for MA recipients/participants).

- Claims submitted by the MCO:
    - Access to claims information is not automatically provided. If a user needs access to claims information in PROMISe, they must state, **"I need claims access"** in the Justification box during the self-registration process.

User Responsibility to Request Access:

- Users **must** contact their DA to inform them access to PROMISe is needed. The DA will then submit email approval to DHS.

- Registration should be completed within one (1) week of the DA sending the email approval to the BDCM Security Access Request Mailbox.

- Navigate to the PROMISe Intranet Registration Link via the PROMISe Intranet Login Page: https://pwpromise.dpw.state.pa.us/PROMISe.
    - Click on *Register Business Partner* User under *Self-service Business Partner.*

- **Existing b-account ID Users:**
    - Click on *Existing Business Partner Account – CLICK HERE* (located beneath the Welcome paragraph).
    - Users should log in using their b-account user ID and password.
    - Follow the instructions for registering.
    - Indicate why access is needed in the justification box. **If a user needs claims inquiry**, they must state, **"I need claims access"** in the justification box.

- **New Users (who do not have a b-account user ID):**
    - Click *NEXT* and follow the instructions for registering.
    - Users **must** enter the correct **Organization Tax ID** with no dashes. The DA will provide this information.
    - Indicate why access is needed in the justification box. **If a user needs claims inquiry**, they must state, **"I need claims access"** in the justification box.

Once the registration approval email is received, users should wait at least 15 minutes before logging in to PROMISe Intranet.

If the DA did not send PROMISe Intranet approval to the Security Access Request Mailbox, the registration will be denied, and the user will be instructed to contact their DA.

MCO Delegated Administrator Responsibility:

- Send an email to the RA-PHMCOSecurityReq@pa.gov mailbox indicating the user is approved to request access to PROMISe.

- PROMISe Intranet User Recertification:
    - DAs must be registered for PROMISe in order to access the recertifications.
    - DHS (RA-PWUAC@pa.gov) will send an Action Required email to the DAs on a quarterly basis for access to the MCO's list of users with PROMISe access.
    - The DAs will click on Start Task within the email and then log in with their b-account ID and password.
    - On the right side under Decision, the DAs must indicate if a user's access is Approved or Revoked.

Reminder: The above registration instructions are for MCO user access to the PROMISe Intranet only.

PROMISe Internet - The Gainwell Provider Assistance Center (PAC) manages access for the PROMISe Internet. MCO users can call PAC (1-800-248-2152) to request access. Additional information for this site can be found in the Internet Help Manual (This manual must be opened in Internet Explorer or Google Chrome; it will not open in Microsoft Edge).

DOCUSHARE ACCESS (PH & CHC MCOs)

DocuShare provides access to view/post/receive documents (e.g., policies and procedures) to/from DHS.

DocuShare Site URL: https://www.dpwds.state.pa.us/docushare/dsweb/HomePage. Users must be assigned access as indicated below.

User Responsibility to Request Access:

- **Existing b-account ID users do not need to register for DocuShare.** Users **must** contact their DA to request access. The DA will email the BDCM Security Access Request Mailbox to request the user's access to DocuShare.

- **New Users (who do not have a b-account user ID):**
  - New users should contact their DA to request DocuShare access and will also need to complete the self-registration process which is done through the PROMISe self-registration link.
  - Registration should be submitted within one (1) week of the DA sending the email approval to the BDCM Security Access Request Mailbox.
  - Navigate to the DocuShare (PROMISe) registration link: https://pwpromise.dpw.state.pa.us/PROMISe.
  - Click on *Register Business Partner* User under *Self-service Business Partner.*
  - Click NEXT and follow the instructions for registering.
  - Users **must** enter the correct **Organization Tax ID** with no dashes. The DA will provide this information.
  - Users should enter **"I need DocuShare access"** in the Justification box.

- **When logging into DocuShare, all b-account users must select "Managed" for the Domain.**

NOTE: BDCM processes the DocuShare new user registrations for all PH-MCO and CHC-MCO users and handles requests for access to OMAP-BDCM, OMAP-BMCO, OLTL-CHC, and OLTL-MIPPA folders.

For access to Bureau of Program Integrity (BPI) folders for PH & CHC MCOs:

- DAs or business partner users must contact BPI directly to request access to BPI folders.
  - Bret Ruch (bruch@pa.gov) handles Geisinger, Health Partners, United.
  - Jonathan Weidler (jweidler@pa.gov) handles AmeriHealth/Keystone (PH & CHC), Highmark Wholecare (formerly Gateway), UPMC (PH & CHC).
  - Brandy Hershey (brahershey@pa.gov) handles PA Health & Wellness (CHC).

All other Program Offices must be contacted directly for access to their folders.

MCO Delegated Administrator Responsibility:

- Send an email to the RA-PHMCOSecurityReq@pa.gov mailbox indicating the user is approved to receive access to DocuShare. Email **must** include:

- The user's b-account ID or indicate that the user does not have a b-account ID and will be registering for DocuShare.
- What access the user needs (read only or read/write/modify access).
- Which eligible Program Office access is needed and if the user is restricted to specific folders.
- For MCOs that are both PH and CHC, indicate which access is needed (PH, CHC or both).

- DAs should email the RA-PHMCOSecurityReq@pa.gov (or the appropriate Program Office) to request DocuShare user terminations.

HEALTHCHOICES EXTRANET ACCESS (ALL BUSINESS PARTNERS)

The HealthChoices Extranet is a comprehensive website that provides information regarding the following Programs: PH HealthChoices Managed Care Program, PH Enrollment Assistance Program (EAP), Community Health Choices (CHC), CHC Independent Enrollment Broker, and Medical Assistance Transportation Program (MATP).

Information surrounding these programs includes but is not limited to:

- HealthChoices Agreements
- Systems Notices, MA Bulletins, Ops Memos, Provider Quick Tips
- File Schedules and Specifications
- Forms, Codes, Fee Schedules
- Recipient Coverage, Data Files, Reporting Requirements
- Security Access Information

User Responsibility to Request Access:

- DA approval is **not** needed for HealthChoices Extranet registrations.

- HealthChoices Extranet Site URL: HealthChoices Extranet (SharePoint). All users **must** have a Microsoft account to access the HealthChoices Extranet through SharePoint. This site **cannot be accessed without receiving a Microsoft SharePoint Invitation email to create a Microsoft account or register an existing work-related account.**

- **Microsoft Account Registration for HealthChoices Extranet Site Access:**
  - New Extranet users **must** email the HC Extranet mailbox (RA-PWHCEXTRANETAPVR@pa.gov) to request access. Users will be sent a Microsoft SharePoint Site Invitation email which will contain the link to create a Microsoft account or register an existing one. NOTE: Microsoft accounts **must** be tied to the user's work email. **Personal emails cannot be used.**
    - Click on the link in the SharePoint Site Invitation email and follow the instructions for creating/registering the account.
  - Additional instruction for creating/registering a Microsoft Account can be obtained by contacting the MCO Delegated Administrator or by contacting the HC Extranet mailbox (RA-PWHCEXTRANETAPVR@pa.gov).

- **B-Account ID Registration for HealthChoices Extranet Forms Access** *(To be completed only after the user has successfully registered a Microsoft account and gained access to the Extranet)*:
  - Navigate to the HealthChoices Extranet Forms Registration Link: https://www.hhsidm.state.pa.us/iam/im/businesspartnerspub/ca12/index.jsp?task.tag=HealthChoicesBPUserSelfRegistration

  - **Existing b-account ID Users:**
    - Click on *Existing Business Partner Account – CLICK HERE* (located beneath the Welcome paragraph).

        - Users should log in using their b-account user ID and password.
        - Follow the instructions for registering.
    - **New Users (who do not have a b-account user ID):**
        - Click on NEXT.
        - Users **must** enter the correct **Organization Tax ID** with no dashes. The DA will provide this information.
        - Follow the instructions for registering.

MCO Delegated Administrator Responsibility:

- DAs should email the RA-PHMCOSecurityReq@pa.gov to request HealthChoices Extranet user access terminations.

SELF-SERVICE FOR BUSINESS PARTNERS – USER ID, PASSWORD, EMAIL

On the Keystone Key login pages for eCIS and PROMISe, under Self-Service for Business Partner, there is a way for users to obtain their user ID and password, if they have forgotten them. This only applies if the user has set up security questions during the self-registration process. On the DocuShare login page, the links are listed under *For Business Account Users ONLY* (b-).

Users can change their password, set up or change their security questions, and update their email address by clicking on the **Edit Profile** link. Users will be taken to a log-in screen where they need to enter their b-account user ID and password. Users should then be taken to a screen where they will select what action to take.

- When creating answers to the security questions, users should keep in mind that the answers are **case-sensitive.**
- A user's account profile email must match their current work email address for the MCO they are registered under.

The Self-Service for Business Partner menu can also be accessed directly via Identity Manager.

Expired Passwords:

- **Passwords expire every 60 days.** Users **must** go in **before the 60 days to renew their password**.

- **All users must set up Security Questions** so that if they ever need to have their password reset, they can do it themselves instead of calling the DHS Helpdesk.

- If a user's password expires and they haven't previously set up their Security Questions, they must contact the DHS Helpdesk **1-800-296-5335 (press Option 1, then Option 2)** to get their password reset.

Error Messages:

If a user receives any of the below messages, the user must do the following:

- **9999** – User Does Not Exist – Call the DHS Helpdesk 1-800-296-5335 (press Option 1, then Option 2) to reset password.
- **1000000000** – PID Locked – Call the DHS Helpdesk 1-800-296-5335 (press Option 1, then Option 2) to unlock PID.
- **02000000** – Send a screen shot of the error to: RA-PHMCOSecurityReq@pa.gov.
- **03000000** – Send a screen shot of the error to: RA-PHMCOSecurityReq@pa.gov.
- **All Other Errors** – Send a screen shot of the error to: RA-PHMCOSecurityReq@pa.gov.