



CENTERS FOR MEDICARE & MEDICAID SERVICES

DATE: April 13, 2020

TO: All Current and Prospective Medicare Advantage, Prescription Drug Plan, Section 1833 and 1876 Cost, PACE, and Demonstration Organizations and HPMS Consultant Users

FROM: Amy Larrick Chavez-Valdez, Director
Medicare Drug Benefit and C & D Data Group
Center for Medicare

Kathryn A. Coleman, Director
Medicare Drug & Health Plan Contract Administration Group
Center for Medicare

Jennifer Lazio, Director
Parts C & D Actuarial Group
Office of the Actuary

SUBJECT: Instructions for Requesting Consultant Access to the Health Plan Management System (HPMS)

Consultants may require access to HPMS to perform business functions on behalf of Medicare Advantage, Prescription Drug Plan, Section 1833 and 1876 Cost, PACE, and Demonstration organizations. CMS requires sponsoring organizations to submit official letters to authorize HPMS access for these designated consultant users.

The following table outlines the consultant user profiles that are currently supported by HPMS:

User Type	HPMS Functionality
Actuarial Certification Consultant (consultants or plan employees serving in this role)	This user completes the actuarial certification portion of the bid submission process. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations. Plan employees serving in this role will only perform this function on behalf of their own organization.
Bid Consultant	This user prepares and/or submits plan bids on behalf of an organization. The consultant is not a direct employee of the

User Type	HPMS Functionality
	organization and may perform this function on behalf of multiple sponsoring organizations.
Formulary Consultant	This user prepares and/or submits formulary and related data on behalf of an organization. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations.
General Plan Consultant	This user prepares and/or submits various data in HPMS on behalf of an organization. The consultant is not a direct employee of the organization and may perform similar functions on behalf of multiple sponsoring organizations. Note: This category is intended to capture functionality that resides outside of the other defined consultant types (e.g., application submission, audit support, and performance assessment monitoring). The sponsoring organization must identify the functions needed by each general consultant using the form available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/UserIDProcess.html
Marketing Consultant	This user prepares and/or submits marketing materials on behalf of an organization. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations.
Plan Reporting Data Validation Consultant	This user submits plan reporting data validation findings via the HPMS Plan Reporting Data Validation Module. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations.

The consultant access instructions are determined by a given user’s current access situation. The table below provides the submission requirements for each of the following user scenarios:

User Scenario	Submission Requirements
A new user that needs both a CMS user ID and consultant access in HPMS	Complete a request for a CMS user ID via EFI submission making sure to select the correct consultant type for the question “I am a”. Instructions can be found on website: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/UserIDProcess.html Complete the steps described in Attachment A to request consultant access. Include the completed General Consultant form in the submission, if applicable.

User Scenario	Submission Requirements
An existing HPMS user that needs to add consultant access	Complete the steps described in Attachment A to request consultant access. Include the completed General Consultant form in the submission, if applicable.
An existing HPMS consultant user that needs to add or delete contracts	Complete the steps described in Attachment A to request the addition or removal of contracts for consultant access. Include the completed General Consultant form in the submission, if applicable.
An existing HPMS consultant user with no changes needed	Complete the system access certification (SAC) and security computer-based training (CBT) on an annual basis, and current access will be retained without further action. Review Attachment B for recertification and password guidance.

CMS no longer requires official letters to be submitted on an annual basis to retain existing consultant access. While this process reduces the burden on both sponsoring organizations and CMS, it also requires that organizations invest a greater level of effort in monitoring HPMS to ensure that only appropriate individuals have access.

In accordance with the HPMS Rules of Behavior, the sharing of CMS user IDs is **strictly prohibited**. If CMS determines that individuals are sharing a user ID, the user ID will be revoked immediately.

Managing HPMS User Access

Ultimately, it is the responsibility of the sponsoring organization to manage and maintain the set of users for whom they have authorized access to HPMS. This general principle applies to both plan staff and any consultants that are serving as agents of the sponsoring organization.

CMS provides organizations with reports in HPMS that can be used to manage user access to their contract number(s). These reports can be viewed under the “User Resources > User Access Administration” link in HPMS. If a user within a sponsoring organization does not currently have access to the “plan user access” reports, organizations must submit a request to hpms_access@cms.hhs.gov.

Sponsoring organizations may request the removal of a user from accessing their data in HPMS at any time. These requests should be sent to hpms_access@cms.hhs.gov. Requests must contain the user ID, the name of the individual, the individual’s organization name, and the reason for the user’s proposed deletion.

In the case of consultant users, it is **critical** to remember that these individuals typically serve multiple organizations. When requesting the removal of a consultant, clearly state that the individual is a consultant and only request the removal of specific contract numbers, not the removal of the user’s account. Failure to provide this level of detail may result in the deletion of

a consultant's CMS user ID rather than simply the consultant's access to certain contract number(s).

For questions related to this memo, please contact HPMSConsultantAccess@cms.hhs.gov.

Attachment A – Requesting HPMS Consultant Access or to Add or Delete Contracts for Existing Consultant Access

To add consultant access or to add or delete contracts for existing consultant access, the user must perform the following steps:

1. Prepare an official letter that states the user's name, CMS user ID, consultant company name, the type of consultant access being requested, and the contract number(s) for which consultant access is needed. The letter must be provided on the sponsoring organization's official letterhead **and** signed by a senior official of the organization. Organizations can submit one letter and include multiple consultants on that letter if they are all obtaining the same consulting access type. CMS recommends the use of the following sample language:

(Name of organization) hereby requests that (name of consultant user, the CMS user ID, and consultant company name) be granted (indicate type of consultant access) for the following contract number(s): (list specific contract numbers).

2. Submit the official letter via e-mail in scanned PDF format to HPMSConsultantAccess@cms.hhs.gov. To facilitate timely processing, please indicate the type of consultant access in the subject line of the e-mail.

NOTE: If a user is serving multiple organizations, only **one** CMS user access form is required. However, an official letter must be provided from **each** organization for which the user will be serving as an agent in HPMS.

Attachment B – Recertification and Password Maintenance

Annual Recertification Process

CMS user IDs must be recertified electronically on an annual basis using CMS' System Access Certification (SAC) application at <https://eua.cms.gov/eurekify/portal/login>. For assistance with the SAC, the security computer-based training (CBT), and passwords, please contact the **CMS IT Service Desk at 1-800-562-1963 or 410-786-2580**.

If you do not complete the recertification in a timely manner, your CMS user ID will be revoked, and you will have to re-apply as a new user.

Upon receipt of a recertification email notice from eua@cms.hhs.gov, you must complete both Steps 1 and 2:

Step 1: System Access Review

1. Log into the SAC at <https://eua.cms.gov/eurekify/portal/login> using your HPMS credentials.
2. If you find a certification item on your home screen, select the “Certify” button to proceed.
3. Select the check box that appears next to your name. This action will automatically select the check boxes for all of your associated job codes.
4. Select the “Keep” button in order to retain access to the selected job codes.
5. On the summary page, select the “Submit” button to continue.
6. On the confirmation pop-up window, select the “X” that appears in the upper right hand corner in order to complete the system access review step.

Step 2: Security Training

1. Access the CMS security CBT (Information Systems Security and Privacy Awareness Training) at the following URL: <https://www.cms.gov/cbt/login/>
2. Log in using your CMS credentials and complete the training.
3. Once complete, print a copy of your certificate for your records, as it may be needed later in the process. Please note that you may need to log in a second time in order to generate your certificate. Your CBT is not considered to be complete until you obtain the certificate.

Step 3: Checking Your Status

You can check your System Access Review (SAC) and security CBT status in EUA at any time.

1. Log into EUA at <https://eua.cms.gov> using your HPMS credentials.
2. Enter the “Modify My Profile” link in the left hand navigation bar.
3. Your identity information will appear on the subsequent page.

If the SAC Recert Status is "OK," the SAC Recert Completion Date has changed to the day you completed your system access review, and the SAC Recert Due Date changed to the following year, you have completed the system access review step successfully.

If the SAC Recert Status is "Pending," you have completed the system access review, but it is pending CMS approval.

If the SAC Recert Status is "Due," you must complete the system access review as described in Step 1 above. Upon completion, your system access review will be sent to CMS for approval.

If your CBT Recert Status is "OK," you have completed the CBT and no further action is required on this step. The CBT Completion date should reflect the day you completed your CBT, while the CBT Recert Due Date should reflect the following year.

If your CBT Recert status is "Due," you must complete the security CBT as described in Step 2 above. Please note that your CBT status will be updated overnight, not immediately. However, if the CBT status remains unchanged, send a copy of your CBT certificate to CBT@cms.hhs.gov and request that CMS update your CBT status manually in EUA.

For additional information, please visit: <https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/RecertAndPwdProcess.html>.