COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF HEALTH AND HUMAN SERVICES
MASSHEALTH PROVIDER ONLINE SERVICE CENTER (POSC)
PRIMARY USER POLICY

Introduction

Upon enrollment in MassHealth, each Provider organization attests that it will comply with all federal and state laws, regulations, and rules applicable to the Provider's participation in MassHealth, now existing or adopted during the term of the Provider's participation in MassHealth. Additionally, all MassHealth trading partners attest that they are responsible for the security of data in their possession upon execution of the MassHealth Trading Partner Agreement. The Executive Office of Health and Human Services (EOHHS) requires that any and all providers, business partners, and relationship entities (henceforth, "organizations"), at a minimum, manage access to their information within MassHealth's Medicaid Management Information System (MMIS) Provider Online Service Center (POSC) using the "Administer Account" function on the POSC and comply with MassHealth's Primary User Policy.

The POSC is structured to enable all organizations to access and manage information entered or exchanged with MassHealth at the Provider ID/Service Location (PID/SL) level. Access to the POSC and MassHealth's HIPAA transaction connectivity methods (Healthcare Transaction Service [HTS], Simple Object Access Protocol/Web Services Description Language [SOAP/WSDL], or Hypertext Transfer Protocol [HTTP] Multipurpose Internet Mail Extensions [MIME] Multipart Web service) are securely managed through use of the Virtual Gateway (VG) User ID and password.

Ineffective management of the access to this information could allow staff and affiliate organizations to continue to access the organization's information and submit transactions on behalf of an organization after the termination of contractual agreements or employment. This could leave organizations vulnerable to fraud and allow persons or entities to leverage the organization's information to benefit themselves or other organizations.

The Primary User within each organization PID/SL is the person responsible for managing access to the organization's information on the POSC. This includes the creation and inactivation of users' accounts and password resets. The Primary User manages subordinate IDs for all other users within the organization and can authorize access for business partners, such as billing agencies, to perform POSC and connectivity method functions on behalf of the organization. This Primary User Policy defines the minimum responsibilities of both the organization and the Primary User assigned to each organization PID/SL to maintain access to the organization's POSC information.

1. Organization Responsibilities

I. Each organization enrolled with MassHealth must ensure that access to its information within the POSC is managed appropriately. Specifically, the organization must:

   a. Assign a single Primary User to manage access to the organization's information within the POSC at the PID/SL level. Access includes the user's ability to use MassHealth's HIPAA Transaction Connectivity Method. Organizations can assign the same Primary User to manage access for multiple PID/SLs as required.

b. Assign a single backup Primary User at the PID/SL level to manage access to the organization's information if the Primary User is unavailable.

c. Ensure that both the Primary User and backup Primary User roles are filled and actively managing access to the organization's information at all times.

d. Implement policies to ensure that only those users who should have access to the organization's data can view, submit, or receive information on behalf of the organization.

II. Each organization enrolled with MassHealth must ensure that procedures are in place to support the secure management and access of the organization's information. Specifically, organizations must ensure that:

a. User education, and the assignment and maintenance of the Primary User and the backup Primary User, is timely and accurate.

b. User IDs are inactivated on a timely basis once a staff person or affiliate has left the organization been terminated.

c. User access is modified on a timely basis once a staff person's role has changed within the organization or the contractual relationship with an affiliate has been modified. This includes the addition or removal of POSC services.

d. A semi-annual, or annual review of all POSC user access is established and maintained to ensure that only those individuals who should have access to the organization's data can view, submit, or receive information on behalf of the organization.

e. Only one User ID is assigned to each individual staff person or affiliated individual. Users must safeguard the data and must not share User IDs or passwords under any circumstances.

f. There is not a single Primary User responsible for managing access to a large provider organization's information for an excessive number of PID/SLs. The number of staff and affiliate organizations associated with multiple PID/SLs can become difficult to maintain. Large provider organizations must align the PID/SLs across multiple Primary Users based on the size of the organizations that they will be responsible for managing. This will ensure the level of review and maintenance can be maintained effectively.

III. **Please note:** The Virtual Gateway (VG) User IDs generated under the "Manage Account" function on the POSC can be used to perform the following activities:

a. View, send, or receive MassHealth information via the POSC. Any information exchanged on the POSC should be used by people performing direct data entry or manual file upload/download of HIPAA transactions or other files. If an organization is actively using Robotics Processing Automation (RPA) tools to perform functions that a human would typically perform on the POSC and the RPA tool has not been approved by MassHealth, it is a direct violation of the

MassHealth RPA policy. MassHealth requires that any organization that uses RPA tools to register the tool with MassHealth and seek approval to use the tool on the POSC.

b. Send or receive HIPAA transactions without any human intervention via MassHealth's connectivity method. Each party is responsible for the preservation, privacy, and security of data in its possession.

2. Primary User Responsibilities

I. The Primary User is responsible for managing access to the organization's MassHealth MMIS information. The POSC enables the Primary User to manage and perform the following basic tasks for subordinate users:

a. Creating User IDs for subordinate users (staff, affiliates) and grant them access to perform certain POSC functions on behalf of the organization.

b. Linking subordinate users to PID/SLs to allow them to perform certain POSC functions on behalf of specific enrolled service locations managed by the organization.

c. Resetting passwords for subordinate User IDs.

d. Modifying POSC access for subordinate User IDs to align with the user's job functions.

e. Deactivating and reactivate subordinate User IDs.

II. Once the Primary User has been established for the organization's PID/SL (or multiple PID/SLs), the Primary User must conduct the following activities to create subordinate user accounts:

a. Immediately assign a backup Primary User to perform Primary User responsibilities in the Primary User's absence. This can be accomplished by creating a User ID for that individual.

b. Grant the backup Primary User access to perform all functions that the Primary User can perform. This includes the "Manage Subordinates" function. This function allows the Primary User and the backup Primary User to create and maintain subordinate User IDs for the organization and its affiliates. The Primary User and backup Primary User must not grant access to the "Manage Subordinates" function to any other user.

c. Establish and maintain subordinate accounts and grant POSC access to users (staff, affiliates) to view, submit, or receive information on behalf of the organization (e.g., submit claims).

i. Only create user accounts for those individuals who should have access to the organization's data to view, submit, or receive information on behalf of the organization.

ii. Do not grant every user full access to all the POSC features. The Primary User must only assign access to specific POSC service functions to those users who need access to perform their specific job functions.

iii. Do not assign anyone, other than the backup Primary User, access to the "Manage Account" function. If any other user currently has this permission, the account must be modified immediately to remove the access to this function..

iv. The Primary User can grant each subordinate user access to multiple PID/SLs. This will allow the subordinate user to access information and perform services on behalf of several different service locations.

v. Do not create more than one User ID per person. Only one User ID per user is allowed. Users are prohibited from sharing User IDs.

vi. User IDs for staff who no longer work for the organization, or affiliates that have been terminated or no longer perform functions on behalf of the organization, are promptly deactivated or de-linked. They can no longer view, submit, or receive information on behalf of the organization.

vii. **Please note:** If users are not deactivated or delinked, they will still be able to view, send, and receive information on behalf of the organization. This will place the organization at risk for fraud and abuse.

viii. POSC access must be promptly modified for staff or affiliates whose job functions performed on behalf of the organization have changed. Specifically, these users' access must be updated so that they can only perform the functions that they are currently authorized to perform on behalf of the organization.

ix. Do not link subordinates to any PID/SL if they are not entitled to view, send, or receive information on behalf of that PID/SL. An excessive number of PID/SL assignments may also impact a user's ability to effectively navigate the POSC.

III. The Primary User must ensure that organization staff and its affiliate staff are notified and aware of key information regarding user access and the role of the Primary User. Staff and affiliates must know:

a. Who the Primary User and backup Primary User are, how to contact them, and under what circumstances they must be contacted.

b. The role of the Primary User and what functions the Primary User can perform.

c. The organization's policy and protocols regarding User ID and secure access.

Each user must also be aware of the following:

a. Each User is solely responsible for the use of the Virtual Gateway (VG) User ID and password and must not share it with any other individual.
b. Sharing User IDs and passwords is a violation of the VG Terms and Conditions that each user attests to upon initial sign-on to the VG.
c. Violation of the VG Terms and Conditions may result in the termination of their User ID.

d. MassHealth monitors shared User ID activity on a regular basis to identify noncompliant use of the POSC.

IV. The Primary User must establish and maintain a quarterly, semi-annual, or annual review and alignment of all user access to safeguard the organization's MassHealth information. In such review, at a minimum, the Primary User must:

a. Validate which users are actively performing services for the organization (staff and affiliates) and which users have left the organization or the affiliate organization(s).

b. Validate that each active user only has access to perform the services that they are required to perform on behalf of the organization.

c. Modify and/or inactivate User IDs to ensure that the access aligns with the active user's responsibilities.

d. Generate a report that is used to monitor and report the status of user access.

V. Both the Primary User and the backup Primary User must notify management immediately if either leaves the position so that these roles can be filled as soon as possible.

a. It's imperative that the roles are filled immediately so that the organization can securely manage its data and ensure that staff and affiliate access is kept up to date. This will allow staff and affiliates to have access to the POSC services required to perform their business functions.

b. Each organization is responsible for managing access to its data. MassHealth is not responsible for managing access to any organization's information and has limited capacity to expedite latent subordinate User ID access issues due to the untimely reassignment of the Primary User or the backup Primary User roles.

Please note: Primary Users and backup Primary Users who do not, at a minimum, adhere to the Primary User responsibilities noted above may introduce data security risks to the organization. Such data security risks have the potential to result in fraud or abuse.

3. Primary User Assignment & Maintenance

I. Each organization must establish and maintain a Primary User and a backup Primary User to manage access to the organization's information on the POSC.

a. In order to establish a Primary User, organizations must complete a Provider Enrollment Data Collection Form during the enrollment of a new PID/SL and submit the form to MassHealth along with the provider enrollment package.
   i. MassHealth will evaluate the Data Collection Form. Upon approval, MassHealth will issue a Virtual Gateway User ID that will enable the Primary User assigned to the newly established PID/SL to access the POSC. The Primary User can then begin to create subordinate users under the "Administer Account" function.

ii. Organizations can assign the same Primary User to multiple PID/SLs as necessary.

b. In order to modify the Primary User for an existing PID/SL, organizations must complete the Existing Provider Modification Data Collection Form. This form can be submitted to MassHealth any time the organization needs to modify the Primary User.

c. The MassHealth Data Collection Form process and FAQ can be found at mass.gov/RegisterMassHealthProvider.

II. The Virtual Gateway (VG) serves as a single access point of entry to all EOHHS-hosted applications. It's a secure portal that provides access into the MMIS POSC upon appropriate User ID and password authentication.

a. Each user is prompted to agree to the VG Terms and Conditions upon initial sign-in.

b. All organizations that have been assigned a User ID and Password to access the VG-hosted MMIS Provider Online Service Center (POSC) and connectivity methods are solely responsible for the use of that User ID and must not share it with any other individual.

c. If a user violates the VG Terms and Conditions, their User ID may be terminated.

4. Additional Resources

MassHealth Data Collection Form FAQ

Virtual Gateway Login Job Aid

Subordinate ID Job Aids

MassHealth Robotics Processing Automation (RPA) Policy