MANAGING PROVIDER USER SECURITY

Organization Administration

The Organization Administrator is the designated person with the primary responsibility and authority to establish accounts and passwords for access to provider specific secure information in ND Health Enterprise MMIS.

Important:

If a provider did not identify an Organization Administrator during the re-enrollment application process, then they must first perform a web portal registration in Health Enterprise with their new 7-digit Medicaid provider number on the Home page of the web portal. Once web portal registration is complete, the Organization Administrator’s user ID and password will be mailed to the provider.

**IF you did not register for web portal access during re-enrollment, you can register on Health Enterprise.** The user ID and password will be mailed in separate provider letters. Following that step, additional Organization Administrator accounts and other user accounts can be established.

This instruction shows how an Organization Administrator works with security accounts for users within their organization. User has the ability to add, edit, reset passwords and delete user accounts.

**Important:** The Organization Administrator should set their profile to include Provider-Organization Administrator and Provider-Primary Account Holder.

1. Add a user
2. Search for a user
3. Reset a user’s password
4. Deactivate a user
5. Unlock a user account
1. Add a user

*Any field with an asterisk requires data
Provider Accounts Security Role Options

<table>
<thead>
<tr>
<th>Provider Staff Role</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider-Organization Administrator</td>
<td>Ability to create and configure other Provider organizational users and define their role(s) (Security only)</td>
</tr>
<tr>
<td>Provider-Primary Accountholder</td>
<td>Has full access (view/add/update) to all provider functions and privileges (including Security)</td>
</tr>
<tr>
<td>Provider-Authorizations Staff</td>
<td>Ability to request/edit/view service authorization requests</td>
</tr>
<tr>
<td>Provider-Billing Staff</td>
<td>Ability to submit claims via the web portal; check claims status</td>
</tr>
<tr>
<td>Provider-Eligibility Staff</td>
<td>Ability to verify member/patient Medicaid eligibility information</td>
</tr>
<tr>
<td>Provider-Enrollment Staff</td>
<td>Ability to view/add/update provider enrollment data</td>
</tr>
<tr>
<td>Provider-Financial Staff</td>
<td>Ability to view Remittance Advice and other provider accounting information</td>
</tr>
<tr>
<td>Provider-FES</td>
<td>Ability to view/add/update the Submit Payment Alert/Hospice Election Form (Functional Eligibility System)</td>
</tr>
<tr>
<td>Provider-Trading Partner Enrollment</td>
<td>Ability to view/add/update Trading Partner details</td>
</tr>
</tbody>
</table>

**Important:** The Organization Administrator should set their profile to include Provider-Organization Administrator and Provider-Primary Account Holder.

**Special Considerations**

**Complex Functional Organizations** - For organizations where Medicaid processing is assigned to several individuals or departments we recommend the Organization Administrator create at least one Backup Organization Administrator. In addition, create additional accounts for individuals in the functional areas noted above (Provider Roles) and also create backups for each role in the event of staff absences, job change, or turn over.

**Moderate Functional Organizations** – For organizations where individuals perform two or more business functions we recommend the Organization Administrator create a Backup Organization Administrator and create additional accounts assigning functional areas, as appropriate for work organization and processes.

**Simple (single person)** - For organizations where one person performs all business and security functions, the single provider Organization Administrator account also has the Primary Accountholder role assigned and can perform all functions.
If the user ID is invalid or already used by another provider, the system will suggest alternate user ID's:

Select Add to save to the database.
2. Search for a user

Select My Account

Search for the user by entering first name, last name or by User ID
3. **Reset a user’s password**
   
   a. Use step 2 above to search for a user
   
   b. Follow steps below to reset a user’s password

The provider has the option to reset the password; this password is for a one-time use only.
4. **Deactivate a user**
Select the deactivate option

Enter the deactivation reason in the box asking *What is the reason for this action?*

5. Unlock a user account

*Follow Step 2 above by searching for the user by entering first name, last name or by User ID*
Select user from user list

Select the unlock option

Enter the unlock reason in the box asking *What is the reason for this action?
The Organization Administrator can determine if the password should be reset. Otherwise, the user can resume using the password that is in current use.