# Table of Contents

**Security Management System – SMS**............................................................................................................... 4
- Application Overview .............................................................................................................................................. 4
- How does SMS work? ............................................................................................................................................. 4
- What is the role of the Security Manager? ............................................................................................................ 4
- Help Center .......................................................................................................................................................... 4
- System Requirements .......................................................................................................................................... 5

**Self-registration of Security Manager** ............................................................................................................. 5

**Token Activation and Pin** ..................................................................................................................................... 5
- To activate your own Token Using RSA Deployment Manager ........................................................................... 5
- Create PIN ............................................................................................................................................................ 8
- First-time Log-In .................................................................................................................................................. 10

**Using SMS** ......................................................................................................................................................... 12
- Login Procedure for Security Manager ................................................................................................................ 12
- Users Page .......................................................................................................................................................... 13
  - "User List" Section ........................................................................................................................................... 14
  - "New User" Button ....................................................................................................................................... 15
  - "Search Criteria" Section ............................................................................................................................... 15
  - "Go To" Link ................................................................................................................................................... 17
  - "Help" Link ..................................................................................................................................................... 18
  - "Logout" Link ............................................................................................................................................... 18
- Edit User Information ........................................................................................................................................... 18
  - Accessing the "Edit User" ............................................................................................................................. 18
  - Changing a User’s name, email address, date of birth or gender ................................................................. 19
"New User" Button ......................................................................................................................................................... 19
"Deactivate" Button ....................................................................................................................................................... 19
"Reset Password" Button............................................................................................................................................. 19
"Users" Button ................................................................................................................................................................ 19
Add New User........................................................................................................................................................................ 20

Adding User with Existing User ID........................................................................................................................................ 20
Adding a User who does not have a User ID ................................................................................................................................ 20
"Users" Button ......................................................................................................................................................................... 21
Update the address used to mail tokens .................................................................................................................................. 21
Log-off...................................................................................................................................................................................... 21

Applications Using the Security Management System ........................................................................................................... 21

Patient Characteristics Survey (PCS) ........................................................................................................................................ 21
How will SMS be used for the PCS web application? .................................................................................................................. 21
Granting access to the PCS Application .................................................................................................................................. 21
Assigning User to PCS Security Group .................................................................................................................................... 22
Associating Submitters to Program Units and Sites .................................................................................................................. 22
What sites are Shown? .................................................................................................................................................................. 24
Save the User’s Assigned Access ........................................................................................................................................ 24

Psyckes Medicaid ........................................................................................................................................................................ 25
Authorized Access ........................................................................................................................................................................ 25
Granting Access to the Psyckes Medicaid Application ............................................................................................................. 25
Save the User’s Assigned Access ........................................................................................................................................ 25
Exiting the "Edit User" ............................................................................................................................................................. 26

Mental Health Provider Data Exchange (MHPD) Module ......................................................................................................... 26
Assurance Level 2 ........................................................................................................................................................................ 26
Registration to NY.gov by Security Manager ............................................................................................................................ 26
If the User Already Has an NY.gov account ................................................................................................................................ 31
Transition Period: April 8, 2015 – June 30, 2015 .............................................................................................................................. 31
Assigning MHPD Roles ............................................................................................................................................................. 31
User List ...................................................................................................................................................................................... 32
Edit User Screen ........................................................................................................................................................................34
Updating User Information ..............................................................................................................................................................35
Email Notification ..............................................................................................................................................................................35

New York Employment Services System (NYESS) .....................................................................................................................35
NYESS Provider-Specific Reporting is available at four role levels. ..........................................................................................36
Security Management System – SMS

The NYS Office of Mental Health (OMH) is distributing this SMS/Security Management System Reference Manual to facility Security Managers to provide them with information about and instructions for accessing and using the OMH Security Management System (SMS).

Application Overview

The Security Management System (SMS) is a Web-based application that facilities will use to authorize staff members to access certain NYS Office of Mental Health (OMH) Web applications.

SMS will greatly improve the efficiency of adding and removing users and expanding or reducing users’ access to sensitive data. By appointing a responsible person to authorize data access, each facility in the public mental health system will be able to control access in a secure manner that offers the flexibility to accommodate staff turnover, reassignment or leave.

How does SMS work?

OMH sends an email to the Director of the facility which contains information on how to register a Security Manager. The Director appoints the Security Manager and entrusts him with this information. This Security Manager uses the information to self-register to use SMS. After OMH receives and approves the electronic self-registration request, the application will issue the Security Manager a User ID and a SecurID token to log-on to SMS.

What is the role of the Security Manager?

The Security Manager is designated by the Facility Director to use SMS to grant staff persons from his facility access to certain OMH applications and the security groups within the applications. In the PCS application, the Security Manager also associates persons in the “Submitter” security group with selected units or sites. Multiple active Security Managers are allowed from each facility. A person may serve as Security Manager for two facilities, but must register separately for each facility and will be assigned a separate User ID for each facility.

Help Center

To resolve questions or problems, you can contact the OMH Help Center, Sunday through Saturday from 7 a.m. to 8 p.m. at (518) 474-5554 or 1-800-435-7697 (1-800-HELP-NYS).

Note: Before contacting the OMH Help Center, please refer to the instructions provided in this guide.
**System Requirements**

SMS can be accessed only by using Internet Explorer 5.5 and above. The system may not work properly with other browser applications, e.g., Mozilla, Firefox or Netscape.

Note: Pop-Up Blockers must be turned off or uninstalled for the SMS application to function properly. Examples of pop-up blockers are: Yahoo Toolbar, Google Toolbar and MSN Toolbar. For help turning off pop-up blockers, please contact the OMH Help Desk.

**Self-registration of Security Manager**

For Self-registration, contact your director.

**Token Activation and Pin**

**To activate your own Token Using RSA Deployment Manager**

After successfully registering as a Security Manager, you will receive an email with instructions to activate the SecurID token.

To assign and activate a token, you should click the link contained in the email; e.g., https://dm.omh.state.ny.us/WXUserActivateToken.do?tnApprovalCode=12345678&tnUserId=SMUSERID

The following page will display.

![RSA Web Express: Activate Token - Microsoft Internet Explorer](image)

Enter the serial number imprinted on the back of the token in the "Token Serial Number" field, and then click "Next". (The token serial number is typically 8 or 9 digits long.)
On the "Confirm Your Activate Token Information" page, make sure the User ID and the serial number are correct, and then click "Submit".
The following screen should be displayed:

On the "Token Activation Complete" page, you should click the "Logout" link on the top right side of the page. The following page will display:

This completes the "Token Activation" process.
Create PIN

The next step is to create a Personal Identification Number (PIN). Each user must set his or her own PIN. To start the process, navigate to https://sms.omh.state.ny.us, enter your User ID in the "Userid" field, and in the "Password or Passcode" field, enter only the 6-digit code displayed on the token.

The following "ClearTrust 'SecurID' Login" page will be displayed:
You can either enter a 4-digit Personal Identification Number you have selected, or select the option for the system to generate a PIN. The PIN will be used for with the token to sign on to and access ClearTrust-protected OMH Web applications. The following is an example of the screen you will see when you select your own 4-digit PIN. After clicking the “Go” button, you will be prompted to wait for the number on the token to change, and then enter the new PIN followed by the refreshed token code. If you choose your own PIN, you can skip the next two pages of instructions and proceed to “First-time Log-In.”

If you choose to let the system generate a new PIN, click the “Create PIN” button and the following page will be displayed. You are given the option to proceed (the “Yes” option), or to return to the previous screen (the “No” option) to assign your own PIN. To have the system generate the PIN, you should select option “Yes” and click the “Submit” button:
ClearTrust displays the system generated PIN on a page similar to the following screen print. You should write down or memorize your PIN. It will be needed to complete the activation process.

First-time Log-In

After obtaining your self-selected or system generated PIN, the following ClearTrust Login page will be displayed:
It is important to wait for the 6-digit code on the token to update before proceeding. After the token code changes, enter the new PIN in the Passcode field followed immediately (with no embedded spaces) by the 6-digit code displayed on the token:

After entering the new PIN and 6-digit token code in the Passcode field and clicking the "Go" button, the "User List" page will be displayed.

Congratulations! You have successfully logged-in with your SecureID Passcode.
Using SMS

Login Procedure for Security Manager

The Security Management System Homepage (http://www.omh.ny.gov/omhweb/sms/), provides a description of the application, the user manual, answers to Frequently-Asked Questions (FAQs), and links for self-registration and log-in to the application. The Security Manager follows the link to SMS, enters the User ID, and Passcode (consisting of the PIN and 6-digit token code).
After logging in, the SMS Users page will appear. This page identifies all users for your facility (If no users are listed, the message "There are no users" is displayed. Once users are added, this message will no longer appear when entering SMS).

**Users Page**

After signing-on to SMS, the SMS "Users" page will be displayed. This page contains a scrollable list of all the User IDs assigned to your agency. Initially, the list may be empty (indicated by [Count: 0]), or if your agency has users of OMH applications such as CAIRS, NIMRS, or NYISER, their User IDs will be displayed. Any User IDs that you add should also appear in this list.
"User List" Section

The "User List" contains one row for each User ID defined for your agency. Each row contains the following columns:

- **Edit** (this icon is a picture of a small pencil). You click this icon to edit the user record. This is one of two ways you will grant access to OMH applications. This process is described in the **PCS** and **PSYCKES Medicaid** sections of this document.
- **User ID**. This is the OMH identifier for the user. This identifier is used to sign-on to OMH applications.
- **Name**. This field displays the user's last name, followed by the user's first
name and middle initial.

- **Token Assigned.** While some OMH applications may be accessed with a password, others (e.g., PSYCKES Medicaid), require a SecurID token. This column allows the Security Manager to track token status. The possible values are:
  - "Yes" (the user has a SecurID token)
  - "No" (the user does not have a SecurID token)
  - "Expired" (the user has a SecurID token, however it has expired)
  - Requested-mm/dd/yy" (a token has been requested for this user on the date specified)
  - "Sent-mm/dd/yy" (a token was sent to this user on the date specified)

In rare circumstances, it is possible for an individual to have an OMH User ID, but not appear on the User List. In this case, you can create the association between the existing User ID and your agency by using the "New User" function, described in Add New User. The SMS association will be established by entering the existing User ID on the "New User" page.

"New User" Button

A "New User" button is displayed immediately following the listed users. When you click this button, the "New User" page will be displayed. You must use the "New User" page to add a new User ID for your agency or to associate an existing User ID with your agency so it appears on the User List. See "Add New User".

"Search Criteria" Section

The “Search Criteria” section is located at the bottom of the “Users” page following the User List and New User button. The “Search Criteria” section is the mechanism Security Managers use to limit the User IDs displayed in the User list. It contains the following searchable fields: Application, User ID, Last Name, and First Name. In your search query you may select an OMH Application from the drop down list, enter a specific User ID, last name or first name, or you may enter just the first part of any of these fields. Then, when you click the “Search” button, these fields will be used to filter the search results and display only User IDs that match the criteria you selected. If you enter values in more than one of the fields, the search results displayed in the User list will include only User IDs that match all of the criteria selected.

For example, users with access to the PCS application can be searched by selecting the option ‘PCS’ in the drop down for the Application field and clicking the “Search” button.
The User list returns users with access only to particular application (in this case the PCS). Specific users can be searched by User ID and/or first and last names.
"Go To" Link

In the SMS application, you can navigate to other SMS pages (e.g., Update My Mailing Address) by positioning the mouse pointer over the "Go To" link at the top left-hand side of the screen, and clicking on the drop down link of the desired page. (Go To choices at this time are limited to "User List", "New User", and "Update My Mailing Address".)
"Help" Link

The Help Link at the top right hand side of the screen will open the SMS User Manual.

"Logout" Link

You can sign-out and exit SMS from the SMS "Users" page, or from any other page in SMS, by clicking on the "Logout" link at the top right-hand side of the page.

Edit User Information

Accessing the "Edit User"

To edit the information for an individual at your agency, you will need to sign-on to SMS as described in Log-in Procedure for Security Manager. From the SMS "Users" page, you should access the "Edit User" page by clicking on the "pencil icon" in the "Edit" column on the row for the user in the "Users List" section. The "Edit User" page will be displayed with the user’s name, email address, date of birth, gender, and current application access.
Changing a User’s name, email address, date of birth or gender

You type over the textboxes with new or corrected information and then click the "Update" button to save the changes.

"New User" Button

Following "User Information", a "New User" button is displayed. You should click this button to add a new User ID for your agency or to associate an existing User ID with your agency so it appears on the list. When you click the "New User" button, the "New User" page will be displayed. Add New User describes how to use the "New User" page.

"Deactivate" Button

Click the "Deactivate" button to remove a user’s access to any OMH application. A warning message will appear explaining that the user will lose access to all OMH applications and ask if you wish to do this. Click the "OK" button in the message to deactivate the user’s access.

"Reset Password" Button

Click "Reset Password" to reset the user’s password. This system responds with the following message once the password is reset.

"Users" Button

Click the "Users" button to return to the Users page.
On the bottom of the Edit User screen is a section where you may grant access to various applications, assign users to a security group within the application, and in the case of the PCS, associate users with specific units or sites. These processes will be described in the Application-specific sections.

Add New User

Adding User with Existing User ID

If a User already has an OMH User ID for access to another application (e.g., MHPD, CAIRS, NIMRS) please enter it in the User ID field.

Upon entering a current User ID in the field and exiting the field, the screen will respond with a message that the User ID is valid and will display the retrieved User information. You may close the window. A similar message will display if the User information was not found in the security database. You can edit the User’s email address and your edits will be stored in the SMS application. Fields denoted with an asterisk (*) are required.

Adding a User who does not have a User ID

If the User does not have an existing ID, leave the User ID box blank. The Security Manager proceeds to complete the User information and select the "Create User" button. Fields denoted with an asterisk (*) are required. A new User ID will be generated for the User. If a User by that name already exists for the agency, the system will show a message that a User with that name is among the “active” or “inactive” users. To check the inactive users, see the Search Criteria section of the User’s Page.
"Users" Button

Click the "Users" button to return to the Users page.

On the bottom of the "Add New User" screen is a section where you may grant access to various applications, assign Users to a security group within the application, and in the case of the PCS, associate Users with specific units or sites. These processes will be described in the Application- specific sections.

Update the address used to mail tokens

To edit the address used to mail tokens, you will need to first sign-on to SMS as described in Log-in Procedure for Security Manager. On the SMS "Users" page, you should position the mouse pointer over the "Go To" label in the top left-hand side of the page and click the "Update My Mailing Address" link to display the "Update My Mailing Address" page. You can type over the address displayed with your correct mailing address, or you can click the round "radio button" next to "Use the Agency Address above as the mailing address for SecurID tokens". Click the "Update" button to save your changes.

Log-off

You can exit SMS from any page by clicking on the "Logout" link at the top right-hand side of the page. Be sure to save any changes by clicking on the "Update" button before exiting the system.

Applications Using the Security Management System

Patient Characteristics Survey (PCS)

How will SMS be used for the PCS web application?

In SMS, each facility’s Security Manager will add and edit Users and determine each User’s level of access to the PCS Web application by assigning the User to a security group. For example, the security manager may grant:

- Persons A and B the ability to submit and view data for service recipients of the facility’s unit 101
- Person C the access to submit data for service recipients of the facility’s unit 102
- Person D the supervisory authority to submit, view or download client data for all of the facility’s units

Granting access to the PCS Application

After editing or adding users to the User Page, the Security Manager follows three steps to grant a person access to the PCS application:
1. Assigns the User access to a PCS security group (Submitter or Supervisor)
2. Associates Users in Submitter security group with specific program units and sites
3. Clicks "Update" to save the User's assigned access

Assigning User to PCS Security Group

Below the User Information section of both the "Edit User" and "Add New User" screens, the PCS application is listed and followed by the PSYCKES Medicaid application. To assign a User to a PCS security group, the Security Manager checks one of the two boxes: "Submitter" or "Supervisor". The definitions of PCS security groups are:

- **Submitter** – A person assigned by the Security Manager to enter/edit data and view/print reports in the PCS Web application for the units or sites with which she or he is associated.
- **Supervisor** – By definition, the Supervisor may upload the facility’s data into the PCS application (if the facility has received prior approval), perform all of the functions of a Submitter for every unit throughout the facility, and may also download the facility’s data file in MS Excel.

**Note:** A user can only be a **Submitter** Or **Supervisor** and cannot be both.

<table>
<thead>
<tr>
<th>PCS Access:</th>
<th>Facility/Program/Site Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Facility: [0003] - Buffalo Psychiatric Center</td>
</tr>
<tr>
<td></td>
<td>Program: [876] - ALLIANCE HOUSE SOCIAL CLUB</td>
</tr>
<tr>
<td></td>
<td>Program: [511] - BPC - Butler Clinic</td>
</tr>
<tr>
<td></td>
<td>Site: [5003] - BPC - Butler Clinic</td>
</tr>
<tr>
<td></td>
<td>Site: [2001] - Lancaster Clinic Satellite</td>
</tr>
<tr>
<td></td>
<td>Site: [1001] - Miller-Broadway Clinic Satellite</td>
</tr>
<tr>
<td></td>
<td>Program: [965] - BPC-Del Nor CDT</td>
</tr>
<tr>
<td></td>
<td>Program: [805] - Centralized Activity Therapy</td>
</tr>
<tr>
<td></td>
<td>Program: [417] - Choices Clinic</td>
</tr>
<tr>
<td></td>
<td>Site: [6829] - Choices Clinic</td>
</tr>
<tr>
<td></td>
<td>Site: [1001] - Ransomville Clinic Satellite</td>
</tr>
<tr>
<td></td>
<td>Program: [964] - COMMUNITY EVALUATION TEAM</td>
</tr>
</tbody>
</table>

Associating Submitters to Program Units and Sites

When a person is assigned as a Supervisor, all programs and sites in the facility are automatically selected because the Supervisor’s access, by definition, is facility-wide.

To assign someone as a Submitter: Click the Submitter check box and then select the Program/Sites for which this Submitter will be entering PCS information. This associates the Submitter with the selected programs/sites. The Security Manager must associate
the Submitter with at least one program/site and up to all programs/sites. The complete list of program units currently listed in the Facility Survey (or PCS Web application) can be viewed on the list.

<table>
<thead>
<tr>
<th>PCS Access:</th>
<th>Facility/Program/Site Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Facility: [7144] - Rehabilitation Support Services, Inc.</td>
</tr>
<tr>
<td></td>
<td>Program: [545] - ADULT BCM - Team 2 (Orange Co)</td>
</tr>
<tr>
<td>✅</td>
<td>Program: [546] - ADULT BCM Team 1 (Orange Co)</td>
</tr>
<tr>
<td></td>
<td>Program: [017] - ALBANY MICA NETWORK</td>
</tr>
</tbody>
</table>

Once a User is "associated" with sites, the User will be able to enter and edit information in the PCS application for all clients in that site.

By default, program units are shown, but the list can be expanded into sites or collapsed into programs by clicking on the expand and collapse buttons:

- Expand Button – reveal sites associated with a program
- Collapse Button – hides the site information

For the licensed outpatient program types in the table below, agencies are expected to report Patient Characteristics Survey data at the site-level. The Security Manager may grant site-level access; i.e., grant one person access to some of the unit’s sites and another person access to another set of sites.

<table>
<thead>
<tr>
<th>Program Type CD</th>
<th>Program Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0200</td>
<td>Day Treatment</td>
</tr>
<tr>
<td>0800</td>
<td>Assertive Community Treatment</td>
</tr>
<tr>
<td>1310</td>
<td>Continuing Day Treatment</td>
</tr>
<tr>
<td>2200</td>
<td>Partial Hospitalization</td>
</tr>
<tr>
<td>6340</td>
<td>Comprehensive PROS with Clinical Treatment</td>
</tr>
<tr>
<td>7340</td>
<td>Comprehensive PROS without Clinical Treatment</td>
</tr>
<tr>
<td>8340</td>
<td>Limited License PROS</td>
</tr>
<tr>
<td>2100</td>
<td>Clinic Treatment</td>
</tr>
<tr>
<td>2320</td>
<td>Intensive Psychiatric Rehabilitation Treatment</td>
</tr>
</tbody>
</table>
To grant site-level access, the Security Manager expands the program unit listing and selects the desired sites.

We recommend that the Security Manager collapse the list into program units to associate PCS Submitters with specific programs. If the Security Manager chooses to grant only site-level access for some outpatient programs, he should expand the program/site list for those outpatient programs and associate the PCS Submitters with the specific sites.

**What sites are Shown?**

Information about the facility in the SMS application is drawn from the OMH master provider directory and may be updated by submitting corrections via the Mental Health Provider Data Exchange (MHPD). A description of MHPD is available at [http://www.omh.ny.gov/omhweb/mhpdr/](http://www.omh.ny.gov/omhweb/mhpdr/). In preparation for the collection of PCS data, providers completed the facility survey found on MHPD’s Survey tab, correcting facility data and program unit data for all programs expected to report on the PCS.

For certain facilities, the SMS list of programs/sites may be so long that the User may have to scroll down to see all the programs/sites for that facility.

In the SMS application, any list that you display on your screen may be printed in its entirety by right-clicking on the screen with the expanded list of programs and their corresponding sites and selecting the “print” option.

**Save the User’s Assigned Access**

Once the fields are populated and PCS access is assigned for the prospective User, click “update” to submit the request.
An email will be generated for the prospective PCS User, giving instructions. If the Security Manager registered the PCS User with an existing OMH User ID, the email will list the ID and instruct the User to use his or her existing password or token. If the User forgets his password, the OMH Help Center can reset it. If the PCS User was not registered with an existing User ID, a new ID is sent to the User's email address along with a notice to expect another email with a password and instructions. The second email will contain the new User password and instructions for use.

Upon finishing the request, the Security Manager should click the “Go To” button in the top left corner and click “Users” to exit the current request and return to the User Menu screen.

Psyckes Medicaid

Authorized Access

Agencies are responsible for ensuring that staff have access only to those applications for which they are authorized. For example, at this time the OMH application PSYCKES Medicaid is being implemented only in agencies participating in the NYS OMH Quality Improvement Initiative. If your agency is not participating in this QI Initiative, your Security Manager should not use SMS to provide anyone at your agency with access to PSYCKES Medicaid.

Granting Access to the Psyckes Medicaid Application

To add a User to an application, you will need to sign-on to SMS as described in the Login Procedure for Security Manager section. From the SMS "Users" page, you should access the "Edit User" page by clicking on the "pencil icon" in the "Edit" column on the row for the User in the "Users List" section. The "Edit User" page will display the User’s information and current application access. The PSYCKES Medicaid application is listed below the Patient Characteristics Survey (PCS) section. You can add or remove a User’s access to the PSYCKES Medicaid application by clicking the checkbox next to the application in the “Application Access” section. A check in the box indicates the User has access. If there is no check in the box, the User will not have access.

Save the User’s Assigned Access

You must click the "Update" button in the "User Information" section to save your
selection. An email will be generated for the prospective User, giving instructions.

**Exiting the "Edit User"**

You can return to the "User List" page by clicking the "Users" button, or by positioning the mouse pointer over the "Go To" label at the top left-hand side of the page, and clicking the "Users" link.

**Mental Health Provider Data Exchange (MHPD) Module**

In SMS the facility’s Security Manager can add, deactivate or edit Users, and assign a User’s level of access to MHPD. Only a Security Manager will be able to update a User’s name, email address, title and phone number (formerly an option for MHPD Users in MHPD).

**Assurance Level 2**

In accordance with Federal and State policies, OMH now requires the formal establishment of an identity assurance level 2 (AL2) for users accessing certain OMH resources, including MHPD. The additional identity checking of a user assures that the person is who they claim to be. At the same time, OMH will link or create an account in the NYS account system, NY.gov ID. April 8 through June 30, 2015 is a transition period during which NY.gov accounts may be established, but NY.gov log-in will not be implemented for MHPD until July 1, 2015. See Transition Period.

**Registration to NY.gov by Security Manager**

The Security Manager may grant a user access to MHPD with an AL2 account under the Edit User screen in SMS. First, the Security Manager (SM) opens Edit User for the user, verifies and updates "User Information" (e.g., email address). Second, the SM sets Assurance Level 2 security. Finally, the SM grants access in either an MHPD User or MHPD Administrator role.
On the Edit User screen, just above “Last Updated By,” you will see the “Assurance Level 2” status.

1. If “Assurance Level 2” is followed by “Yes,” the user has already been granted Assurance Level 2. In this case, proceed to Assigning MHPD Roles. If the user already has both AL2 access and has been granted an MHPD role, there is nothing more you need to do. The NY.gov account will be established.

2. If “Assurance Level 2” is followed by “No,” click the “Set Assurance Level” button. See screen below. If IDs are listed under “NY Gov User ID” and you receive the message, ‘Do you want to select this user?’, see If the user already has an NY.gov account.

3. If you receive the message, “There are no records in NY.GOV that match your search criteria.” the user does not have a NY.gov ID business or government account associated with their e-mail address. If you know the user does have an account in NY.gov, see If the user already has an NY.gov account.
4. Under the ‘* Identity Source:’ dropdown, select either ‘In Person’ or ‘NY DMV’:

   a. If you select ‘In Person’, (see screen below) you are certifying that you have independently verified, using the Identity sources that you indicate, that the applicant is whom he or she claims to be. One source must contain a Photo ID. You cannot combine a [B] document from Identity Source 1 and a [C] document from Identity Source 2 Identity Source:

      i. Select one document from the ‘* Identity Source 1:’ dropdown (Sixteen (16) choices split between A or B categories)

      ii. Select one document from the ‘* Identity Source 2:’ dropdown (Seventeen(17) choices split between A, B, or C categories)

      iii. To save the changes, click the ‘Update’ button. Once the SM updates the record, then an AL2 NY.gov account is created. The AL2 NY.gov User ID will be the same as the Salute User ID, if that user ID is available in NY.gov; otherwise a new User ID is created.
Assurance Level 2 account can be established by using the following two identity verification sources.

* Identity Source:  

  Please select the two documents verified.
  - One source must contain a photo ID
  - You cannot combine [B] document from Identity Source 1 and [C] document from Identity Source 2 Drop Down List.

  * Identity Source 1:  
  * Identity Source 2:  

By completing this request, you are certifying that you have independently verified that the applicant is whom he or she claims to be using current government photo ID containing either address or nationality of record.

Identity Sources:

b. If you select “NY DMV:”

Assurance Level 2 account can be established by using the following two identity verification sources.

* Identity Source: NY DMV

  * DMV Client ID:
  * Document Number:
  * Date of Birth:
  * Last 4 digits of SSN:
  * Zip Code:

Where can I find this?

i. Enter data in the 5 identification fields. Data submitted is not stored with OMH. It is used for processing the request only. Click “Where can I find this” to see figure below; an illustration of where the requested information is found on the driver’s license.

  - NYS DMV Client ID: Nine (9) digit ID near top of license.
  - NOTE: At this time, other state issued licenses are not acceptable.
- Document Number: Found in lower right corner of license (very small print)
- Date of Birth
- Last 4 digits of SSN (Social Security Number) from staff person
- Zip Code shown on license
  ii. Click the ‘Update’ button

c. AL2 security is now set. Proceed to Assigning MHPD Roles.
d. Select the “Update” button to register the MHPD access with NY.gov. The NY.gov account is established.
If the User Already Has an NY.gov account

If the User already has a NY.gov account, complete the ‘NY.gov User ID:’ field

1. If the user is found, you will now receive a message asking ‘Do you want to select this user?’ Click ‘OK’ to link the users
2. If you receive a message, “Email ID entered for this user doesn’t match with NY GOV Repository”, the e-mail address in SMS differs with the NY.gov ID e-mail address. It must be the same as the email used at the time you signed up for a previous NYS online business account. Correct the user’s email address in SMS, Update user information and restart registration for the user in SMS. If the user’s email in SMS is correct, you will need to correct the NY.gov email address. To do this, contact the NY.gov ID administrator of the agency (e.g., The Justice Center) which ‘owns’ the user account to have the email for the account corrected. Typically this is the agency with which the account was originally created. This number can be found under the link ‘Agency Contact Help’. If you do not know the agency, you should contact the Customer Care Center at 1-800-697-1323.
3. To complete the process, proceed to Assigning MHPD Roles.
4. Select the “Update” button to register the MHPD access with NY.gov. The NY.gov account is established.


During the transition period, the user continues to log into MHPD from Web salute. By completing the steps above, the user’s NY.gov account is established, but it will not be implemented in MHPD until July 1, 2015. Starting July 1, the user will log into MHPD via https://my.ny.gov. Unless the user accesses other applications through NY.gov, the first time he logs in, he will select the “Forgot your Username or Password?” option on the https://my.ny.gov main portal page. Anytime, he forgets his or her username or password, the user can use the self-service tools on the main portal page. NY.gov will list all the applications accessible to the user’s ID.

For technical questions about the transition application, MHPD or SMS, please contact the OMH Helpdesk at 1-800-HELP-NYS (1-800-435-7697).

Assigning MHPD Roles

After adding or editing Users on the User Page in SMS, the Security Manager grants the User access to MHPD.

For providers or counties, there are four roles in MHPD, each with their own specific levels of access and responsibility.

- **Provider User** – a User at an individual Facility who can access all the information currently available for that Facility in MHPD. A User with
Provider access can submit Change Requests, Administrative Actions and EZ PARs to add, update or close programs.

- **Provider Admin** – a User at an individual Facility who has all the Provider User functionality and can edit the facility information as well. Additionally, a User with a Provider Admin role can edit the facility maintenance page and assign persons to receive facility notifications sent out by OMH via email.

- **County User** – A County or New York City Mental Health Department User can search, view and request updates to Programs and Sites located in the county. They can view change requests and can request the opening or closing of existing unlicensed programs. They can view but cannot submit Administrative Actions and EZ PARs.

- **County Admin** – a User at a local government unit who has the same access as a County User, and has all the functionality of the Provider Admin for the County Department of Mental Health and each Facility located in the county.

The Security Manager can grant a User only one role, for instance, a User with Provider access cannot also have County access. The Security Manager can grant a User in a Provider role access only to the Security Manager’s Facility. If the User needs access to a second Facility, the Security Manager or Director for the second Facility should contact the OMH Helpdesk to request the MHPD System Auditor to associate the User with the second Facility.

To assign a User a chosen role in MHPD, after logging in to SMS, the Security Manager next selects the User from the User List or creates a New User if the person does not already have a User ID. To edit a User, the Security Manager clicks the “Edit” icon (the small pencil to the left of the UserID). To create a New User, the Security Manager clicks the “New User” button and follows the steps indicated.

**User List**

Once in the Edit User Screen, the Security Manager should first verify the User’s information, and then scroll down to the MHPD Module section of the screen. If any of the required fields (marked with asterisks*) are blank, the Security Manager will be
directed to enter information before being allowed to update.
Edit User Screen

To assign MHPD access, the Security Manager selects the appropriate Group Name from the Group Name list. Only one Group Name can be selected.

When finished with all edits, click the “Update” button above the MHPD section. The following screen will appear.

Next, click the “Users” button to return to the User List, “Close” to return to this Edit User screen if necessary, or “Logout” at the top right hand corner of the screen to log out of SMS and quit the application.
Updating User Information

Formerly, each MHPD user could update his or her email address, title and phone number in MHPD. Presently, the Security Manager must update this information.

It is important to keep this information current so that MHPD Users receive email notifications of Change Requests, Administrative Actions and EZ PARs that they submit and so that they may be contacted by phone or email by OMH or county staff who are reviewing the requests. To update User information, the Security Manager will select the User from the User list by clicking the “Edit Icon” to the left of the UserID. Once on the User Information Screen, the Security Manager simply corrects any information that needs updating, and then clicks the “Update” button. When finished, the Security Manager can log out at the top right hand corner of the screen, or click the “Users” button to return to the User List and select a different User to edit.

Email Notification

Duplicate notification email is sent to the Security Manager’s and User’s email addresses whenever a new User is entered in the system and/or a new password is generated and when a User is granted access to an application, such as when an MHPD Group Name is assigned. No email is sent when User information is updated.

New York Employment Services System (NYESS)

In SMS the facility’s Security Manager can manage user access to the New York Employment Services Systems (NYESS). See www.nyess.ny.gov for details about this program.

Three types of NYESS access are available: case management, provider-based reporting and cross-provider reporting. Within these categories, various roles are available.

Typically users of the NYESS Case Management system will require NYESSCM Business Services. This provides access needed to use the Case Management (OSOS) system for delivery of employment services.

Additionally, office supervisors may require NYESSCM Supervisory access, which allows staff to manage service offerings for their office.

Additional case management roles may also be available to select organizations. Questions about these roles should be addressed via the NYESS Contact form.
NYESS Provider-Specific Reporting is available at four role levels.

These are:

- Directly supported Seekers. This provides report access to job seekers for whom you are providing case management support directly. This is essentially reporting of the information you have entered in the case management (OSOS) system.
- Supervisor. This provides you access to not only individuals for whom you are providing direct case-management support, but also those job seekers who are being supported by staff you supervise.
- Office Administrator. This role provides report access to all job seekers supported by your selected office(s).
- Provider/Organization. This role grants access to reports for all job seekers handled by all offices within your organization.

NYESS Cross-provider Reporting is available to oversight organizations, such as state and local jurisdictions and provides aggregated data based on locale and/or funding streams. Access to these roles will require review and approval by the NYESS business office.