

NHIPPS Security Administrator Step by Step Guide

NHIPPS Security Administrator Responsibilities

The NHIPPS security administration is a critical role at each agency and a key position as defined in your subgrant. While SAPTA is happy to provide you with comprehensive NHIPPS system support, it is impossible for us to know if a call requesting security administrator support, such as resetting a password, is legitimate. This creates a substantial security liability for you. It is therefore essential that your agency designates both a primary and backup NHIPPS Security Administrator to handle your agency's security needs.

NEW SYSTEM USER SET-UP:

- Set up the Provider Staff record in NHIPPS for each system user (unless this role is assigned to your HR department)
- Assign a user ID and default password in the NHIPPS Security Staff record for each system user
- Assign location access and roles / permissions to each system user
- Identify NHIPPS Security Administrators by title in the Provider Staff List record

PASSWORD / USER ID MANAGEMENT:

- Reset passwords to the default password for suspended or expired passwords
- Disable NHIPPS IDs when employees are terminated or if there is a risk that client data may be deliberately sabotaged – specific steps:
 - Enter a unique termination ID in the User Profile record for terminated employees
 - Disable the employee's password in the User Profile record
 - Enter the termination date in the Provider Staff record for terminated employees

OTHER SECURITY DUTIES:

- Communicate and monitor individual security and confidentiality responsibilities to agency staff members
- Take all security requests and issues seriously and immediately initiate the correct action
- Train new NHIPPS Security Administrators as needed
- Ensure that security and confidentiality measures are being employed by all system users – specific steps:
 - Ensure correct physical placement of computer monitors to assure confidentiality of displayed data
 - Ensure that system users are not leaving a work area without logging out off NHIPPS
 - Ensure that no one in your agency is sharing their NHIPPS user ID or password
 - Ensure that browser password save features (i.e. AutoComplete) are disabled at each workstation in your agency
 - Ensure that no one activates a password save feature (i.e. AutoComplete) on their workstation
 - Ensure that only authorized personnel have access to NHIPPS data

NHIPPS Security Administrator Step By Step Guide

Since compliance with Federal confidentiality laws is a critical part of substance abuse prevention and treatment, your agency should establish a firm and effective policy to deal with situations where security and confidentiality are breached due to system user negligence.

Responsibilities of the General System User

Every NHIPPS system user has a responsibility to ensure the quality and protect the confidentiality of client or other data stored in NHIPPS. Some things you can communicate to general users to ensure NHIPPS data is secure:

- Position computer terminals in such a way that others cannot view confidential data when they walk by or enter your work area
- Never share User ID or password with anyone
- Never allow Internet Browser, i.e. Microsoft Internet Explorer, to save passwords
- Always log off of NHIPPS or lock workstation whenever you leaving the work area
- Report any security concerns to management or NHIPPS Security Administrator

Step by Step Guide for NHIPPS Security Administrators

WEBSITES for NHIPPS production and training databases:

URLs For NHIPPS PRODUCTION (LIVE) Server

<https://prodnhipps.nv.gov/nhipps/frontpage.asp>
<https://prodnhipps.nv.gov/nhippsnet/>

(NHIPPS Classic)
(NHIPPS Silverlight)

URLs For NHIPPS TEST (training) Server

<https://testnhipps.nv.gov/nhipps/>
<https://testnhipps.nv.gov/nhippsnet/>

(NHIPPS Classic)
(NHIPPS Silverlight)

NHIPPS Security Administrator Step By Step Guide

TO ADD ICONS ON THE DESK TOP FOR BOTH TRAINING AND PRODUCTION DATABASES

1. Open the URL you want to add
2. Move the cursor into the body of the page
3. Right click and select "Create a Shortcut"
4. Be sure to NAME the Icon correctly by right clicking on the Icon text and selecting RENAME

BEFORE YOU START:

- There are two agency layers or levels in NHIPPS, the **Business Level** and the **Treatment Location** levels – these are referred to as **Location Entries**
- Users may be given access to multiple locations within an agency, this is typical of treatment providers rather than prevention providers
 - If this is the case, there will be multiple location entries in the user's name in both the **Provider Staff List** and the **Security Staff List** – these are not independent of one another but are linked
- Access is granted in 3 steps
 - Creating a Staff record from within the **Provider Staff List**
 - Creating a **User ID** and password from within the **Security Staff List**
 - Adding roles to each location entry from within the **Security Staff List**
- If a user is given access to multiple locations, an equal number of **Location Entries** in the system -- these are not separate records but are linked together
- Changes to the Staff record and to the **User Profile** part of the Security record propagate to each **Location Entry** in the respective screens
- Roles do not propagate but must be set at each location entry from within the **Security Staff List**

NHIPPS Security Administrator Step By Step Guide

TO ADD A STAFF MEMBER TO YOUR AGENCY:

1. From within the NHIPPS application, open (click on) Business Office button
2. Click “Change Business Entity”
3. Go to your Business Level (if not already there)
 - a. Click “Select” -- this will set you at the location you’ve chosen and return you to the Business Office menu
4. Select “Provider Staff List” from the Business Office menu
5. Select “Add Staff Member”
6. **Treatment Providers** -- Select all locations (from the Business Entity dropdown) that staff member will need access to
 - a. Be sure to give access at the Business Level if the employee will need to access multiple treatment locations – this will allow them to see a full record set for clients who have moved within the agency
7. **Prevention Providers** – give system user access to the Business Level only. Access to additional locations listed in the Business Entity drop down not required.
8. Select default sign-in location (Primary Business Entity) depending upon where the main work location is for the system user
 - a. **Prevention Providers**– set the Primary Business Entity to the business level
9. Use full or last 4 of social security number (or 0’s, etc.) if needed
10. *You will need to enter 3 initials for the staff record*

Once the staff record is saved, you will see a staff record with the system users name assigned to that person;

Prevention Providers– you should see only one staff record at the business level

Treatment Providers – you should see one staff record for each location entry the system user will access

NHIPPS Security Administrator Step By Step Guide

TO SET USER ID AND PERMISSIONS AT EACH LOCATION:

Permission to access multiple locations must be given at each individual location.

Treatment Providers – for system users who may need to work from multiple locations, permissions are needed at each location via the specific staff security record for that location.

Prevention Providers - system users need permissions only at the Business Level.

1. Quit the “Provider Staff List” screen and select “Security Staff List”
2. **Prevention Providers** -- Open the business level ID
3. **Treatment Providers** -- Open either the business level ID or, if you have not given the system user access to the business level, open the Primary Business Entity ID.
4. Set the user name
 - a. You can use a standard user name convention, such as first initial and last name.
 - b. *Remember that these fields are CASE SENSITIVE*
5. Set the default password
 - a. *(Password must be >6 characters with at least 1 numeric character)*
6. Set the account status to “New Account”
7. When you save this record, you’ll be returned to the Security Staff List menu with user ID’s displayed
8. Re-open the “ID” you just saved to set roles (permissions)
9. Open “Add Roles”
10. Select roles per the handout given
11. Save the roles page – you will be returned to the User Profile screen
 - a. *QUIT the User Profile page so the password isn’t altered*
12. **Treatment Providers** -- go into each of the remaining location “ID’s” and set roles for each location
13. Repeat 6 through 10

Treatment Providers: Both the Provider Staff List and the Security Staff List may display a User ID for each location where access is given. *These are not separate IDs, but separate permissions must be given under each so specific location access is controlled.*

FYI – it’s a good idea to define a standard “default” password to use for a reset or first ID setting so everyone at your agency knows this. Typical default password is *change123*. *Remember that User IDs and passwords are case sensitive.*

Treatment Providers – There are two layers of locations – the business level and the treatment locations

Business Level

Treat location entry 1

Treat location entry 2

NHIPPS Security Administrator Step By Step Guide

TO RESET PASSWORD

1. Open Business Office
2. Change Business Entity to Business Level
 - a. If user does not have business level access, any location entry will do
3. Open Security Staff List
4. Select the user's ID at the Business Level
5. Type and confirm the default password
6. Set account status to "New Account"
7. Save
8. Notify user

Treatment Providers – A password reset need only occur at the Business Level or one location entry if multiple levels are given to the system user.

TO TERMINATE / SUSPEND AN ID

1. Open Business Office
2. Change Business Entity to Business Level if needed
3. Open Provider Staff List
4. Open ID at Business Level
5. Click Edit
6. Add a termination date (any date will cause the record to terminate)
7. Save

TO "UN-TERMINATE" AN ID

1. Open Business Office
2. Change Business Entity to Business Level if needed
3. Open Provider Staff List
4. Open the staff record at Business Level (or TX location if not at the Business Level)
5. Click Edit
6. Remove the termination date (and edit the hire date if necessary)
7. Save
8. Return to the Business Office
9. Open Security Staff List
10. Open the staff record at the Business Level (or TX location if not at Business Level)
11. Follow "Reset the Password" steps

Assigning Roles – Remember, if you're setting up a new Security Administrator, you give them the Security Administrator role and ALL THE ROLES THEY CAN ASSIGN TO OTHERS.

Security Administrator Roles

- Role Assignment (BOTH)
- Assessor (TREATMENT)
- NHIPPS Administrator (TREATMENT)
- NHIPPS View Only (BOTH)
- NHIPPS Security Adm (BOTH)

NHIPPS Security Administrator Step By Step Guide

- Intake Coordinator (TREATMENT)
- Intake Clerk (TREATMENT)
- Intake Screener (TREATMENT)
- Admission Specialist (TREATMENT)
- Service Provider (TREATMENT)
- Super Service Provider (TREATMENT)
- Discharge Specialist (TREATMENT)
- Follow Up Specialist (TREATMENT)
- Human Resources Coordinator (BOTH)
- Facility Manager (BOTH)
- Reporting Specialist (BOTH)
- Request for Advance/Reimbursement Specialist (BOTH)
- Financial Status Report Specialist (BOTH)
- Available Capacity Specialist (TREATMENT)
- Reports Only (BOTH)
- Session Activity Specialist (PREVENTION)

Treatment Providers

➤ **Counselor Roles**

- Assessor
- NHIPPS Administrator (*Clinical supervisor only*)
- Intake Coordinator
- Intake Clerk
- Intake Screener
- Admission Specialist
- Service Provider (*if restricted access is desired*)
- Super Service Provider (*if no restricted access is desired*)
- Discharge Specialist
- Follow Up Specialist
- Reporting Specialist
- Available Capacity Specialist

➤ **Business/Administration staff Roles**

- Reporting Specialist
- Request for Advance/Reimbursement Specialist
- Financial Status Report Specialist
- Reports Only

Administrators / Directors (non-counseling)

- Facilities Management
- Human Resources Coordinator

NHIPPS Security Administrator Step By Step Guide

Roles for Fiscal / Financial Staff

- Request for Advance/ Reimbursement Specialist
- Financial Status Report Specialist

Prevention Providers

➤ **Business/Administration staff Roles**

- Reporting Specialist
- Request for Advance/Reimbursement Specialist
- Financial Status Report Specialist
- Reports Only

Administrators / Directors (non-counseling)

- Facilities Management
- Human Resources Coordinator

Roles for Fiscal / Financial Staff

- Request for Advance/ Reimbursement Specialist
- Financial Status Report Specialist

Roles for Primary Prevention Staff

- Session Activity Specialist

5. AutoComplete (Windows):

1. To turn off the Auto Complete Feature (for password save)
2. Open Windows Internet Explorer
3. Open Tools
4. Open Internet Options
5. Open Content
6. Open Auto Complete
7. Turn off User Names and Passwords on Forms
8. Clear Passwords
9. Exit via "OK"

Make sure your staff knows they are NOT TO INVOKE THIS FEATURE on their computers.