Quick Tips for Local Organization Admininstrators

Quick Content Finder

Enrolled organizations have one or more staff members designated as a Local Organization Administrator (LOA) to maintain their Florida SHOTS account. This includes access to the organization's Personnel List where other staff members can be added or terminated from the account. The Personnel List should be reviewed routinely to ensure only those authorized users have access to Florida SHOTS. This guide provides instructions for completing several important responsibilities for LOAs.
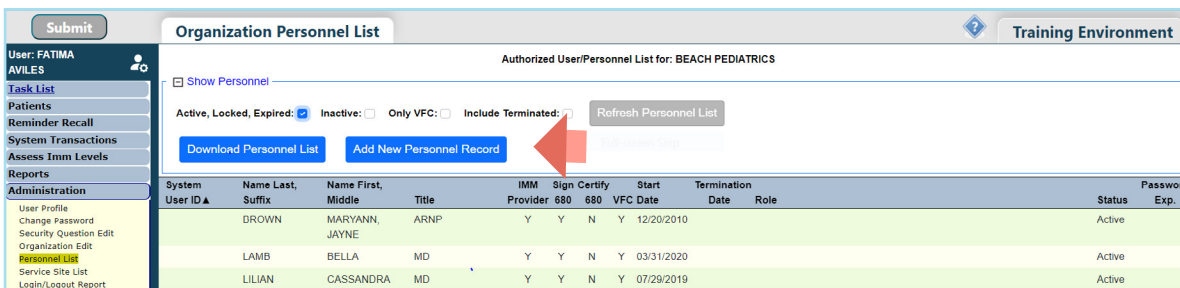
PERSONNEL LIST MAINTENANCE

▶ ## Add New User:

LOAs can add new users to the organization account by selecting **"Personnel List"** under the **"Administration"** menu option.
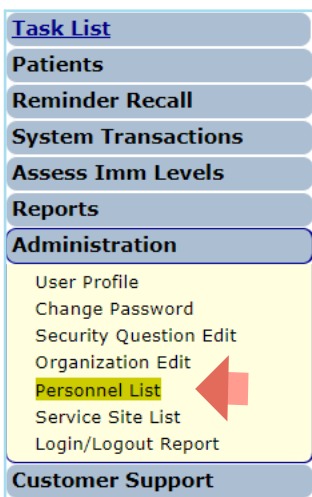
Select the **"Add New Personnel Record"** button from the **"Organization Personnel List"** page.

Once on this page, administrators can enter the details about the new user. The information for medical providers should be entered in Florida SHOTS *exactly how it appears on their medical license.*

- **Email Address:** Provide user's email address for future communications (such as unlocking account, password resets, user authentication etc.,).

- **Start Date:** Defaults to the date the new user is being added, but this date can be changed. *Example: If you have an immunization provider who participated in an outreach clinic prior to entering the administrations, you may need to change the start date here.*

- **Termination Date:** Corresponds to the date when the person is no longer associated with the organization. If this field is grayed out, Service Site Responsibilities must be removed before an End Date can be entered.

- **Immunization Provider:** Select **"Yes"** if this user will administer vaccines to patients.

- **Provider Person ID:** The system will automatically generate an ID when **"Yes"** is selected for Immunization Provider. This will allow for the user to be identified as the person administering the vaccine within a patient record.

- **Certify Form 680:** Select **"Yes"** for any user who is authorized by Chapter 64D-3.046, Florida Administrative Code to sign and certify the DH Form 680. Click on Help Text Icon 🔷 to review conditions.

- **Work Location:** For organizations with multiple service sites, please designate the site(s) where the user works.

- **System User:** This should only be checked for users who require login access to Florida SHOTS. If the box is left unchecked, the user will not be able to log into Florida SHOTS but will appear on your organization's list of immunization providers.

- **Reason for Access:** Provide reason to indicate why this person needs access to Florida SHOTS.

- **System User ID:** This is automatically generated but can be changed.

- **Password Expiration:** This is automatically generated each time a new password is created.

- **System User End Date:** Leave this blank as it corresponds to the date the user no longer needs log in to Florida SHOTS.

- **System Password:** A temporary password must be created by the administrator and will need to be entered again in the Confirm Password field. Click on Help Text Icon �e to view password parameter requirements.

- **Roles:** This determines some of the permissions for the user. Most users are set to **"Local Org Staff."** Contact the Florida SHOTS help desk to assign the user as a Local Organization Administrator role.

- **Create Certified Form 680:** Select **"Yes"** to authorize user to create a certified Form 680 with a provider's electronic signature.

- **User must change password at next logon:** Should be checked to prompt the user to create their own password during the initial login.

When a new user signs into Florida SHOTS, they will see a task in the **"User Task List"** to acknowledge training. From there, they can link to the training and resources page within Florida SHOTS and check the box to acknowledge training. Administrators may also check the box next to Florida SHOTS training acknowledged within the personnel record.
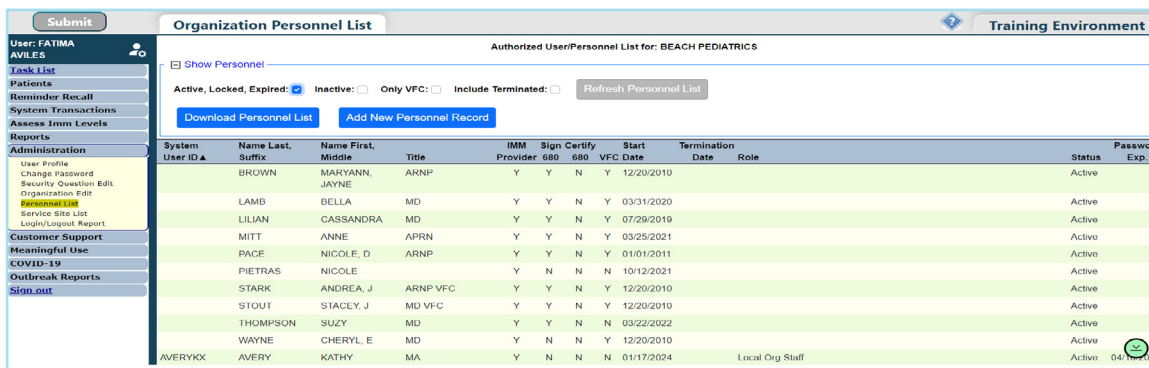
Click on the **"Submit"** button to save the information.

The user will need to login within three days of the Start Date or the account will inactivate.

▶ Add VFC Responsibility to User:

Users from organizations that participate in the Vaccines for Children (VFC) Program and have been designated as a VFC Enrollee, Primary, or Secondary Contact within the organization can assign selected staff record various responsibilities (inventory access, ordering vaccines, and temperature logs).

Select the user from the **Organization Personnel List** to access the **Personnel Maintenance**.

Click on the **"Service Site Responsibilities"** button.

Select any responsibility to grant the user permissions for each associated service site if applicable. Click on the **"Submit"** button to save.

Activate User Account:

Users who have not changed their password in over 90 days or have not logged in within a 30 day period will be set to Inactive. Upon login, inactive users will be instructed to contact their LOA for assistance.

From the Personnel List, check the **"Inactive"** box and click on **"Refresh Personnel List"** to find the user. Select the user from the List to access the Personnel Maintenance.

Remove the date from the **System User End Date** field and leave it blank. A new password should be created for the user by entering in the **System Password** and **Confirm Password** fields.

Click on the **"Submit"** button to save.

Terminate User Access:

Users that have left the organizations or no longer need to access to the system must be terminated in Florida SHOTS immediately.

From the **Organization Personnel List** select the user to access the **Personnel Maintenance**.

For users that were associated with the organization but were not system users, enter the termination in the **"Termination Date."**

For users who did have system user access, enter the end date in the **"System User End Date"** field.

> **NOTE:** The **"Termination Date"** may not be set if the staff has any VFC site responsibilities. The VFC Enrollee, Primary or Secondary contacts can remove these by clicking on **"Service Site Responsibilities"** button first. Uncheck the assigned responsibility and click on **"Submit"** to save. Then return to the Personnel Maintenance to terminate.

Click on the **"Submit"** button to save.

UNLOCK USER ACCOUNT

Users have three opportunities to successfully login to Florida SHOTS. After a third failed attempt, their account will be locked. They will receive a message alerting them that their account is disabled and to either use the **"Need Password Assistance"** feature to reset the password or contact the Administrator.

From the **Organization Personnel List** select the user to access the **Personnel Maintenance.**

Remove the check mark from the **"Account Locked"** box. A new password may be created for the user by entering it in the **System Password** and **Confirm Password** fields. Click on the **"Submit"** button to save.

▶ Edit Contact Information:

Local Organization Administrators can edit contact information on the **"Enrolled Organization Maintenance"** page by choosing **"Organization Edit"** under the **"Administration"** menu option. If any other information is incorrect, please send an email to the Florida SHOTS help desk (flshots@flhealth.gov) for assistance.

UNLOCKING PATIENT RECORDS

LOAs can unlock patient records that have been locked by a user within their organization. To do so, click on **"Clear Patient Token"** under **"Patients"** in the sidebar menu.
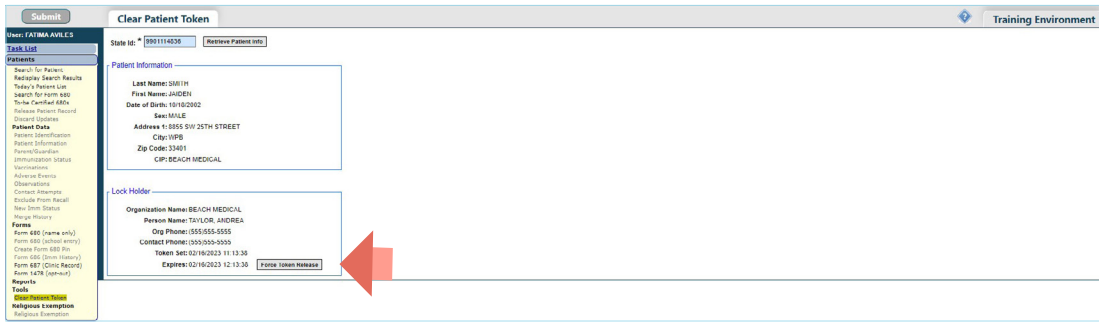

Enter the patient's Florida SHOTS record ID and click on **"Retrieve Patient Info."**

Click on **"Force Token Release"** to complete and clear the lock.

Help Desk

FREE TECHNICAL SUPPORT:
877-888-7468 (SHOT)
MONDAY – FRIDAY, 8 A.M. TO 5 P.M. EASTERN

INCLUDING:

- Merging duplicate patient records
- Adding account administrators
- Unlocking Florida SHOTS accounts

- Questions about any Florida SHOTS features
- Requesting Florida SHOTS materials