MICHIGAN TRAUMA REGISTRY

Facility Administrator Guide

1. Table of Contents

2. Disclaimer

The Michigan Department of Health and Human Services (MDHHS) Trauma Section staff strive to present the most accurate information at all times and in all communications, to the best of their understanding. Software instructions are based on the version that was currently in use when this guide was prepared. While the MDHHS Trauma Section staff are providing this document as an aid, it is the responsibility of each institution to manage the users and user access to the trauma registry.

3. Audience

This document is primarily intended to be a guide for those with Facility Administrator privileges, to aid with performing administrator-specific tasks. Other users may find this document useful to better understand the role of the Facility Administrators.

4. New Users/Accounts

In order to add data to the Registry, each facility must have active users in ImageTrend. If the facility has an existing Facility Administrator, accounts can be created using these steps. Otherwise, a user may request access by emailing the StateTraumaRegistrar@Michigan.gov mailbox. The MI Trauma Registrar will then perform these steps to create the account.

a. Permissions

Before learning how to add accounts, it may be helpful to understand permissions. Each user of the MI Trauma Registry is assigned three sets of permissions: facility, user group, and report writer permissions.

- All records in the MI Trauma Registry are associated with a facility. **Facility permissions** specify for which facilities a user can view, create, or edit records. A user may be assigned more than one facility. Only a System Administrator can assign multiple facility permissions to a single user.
- The **User Group** specifies the level of access to the Patient Registry module (the data-entry side) of the ImageTrend software. Table 1 lists the user group names (column A), a brief description (column B), and type of access for the software modules (columns C-F).
- The **Report Writer Group** specifies the level of access to the Report Writer module. Report writer groups are automatically assigned to specific user groups, but can be changed on a case-by-case basis. Table 1, column E lists the report writer group names in Italics and type of access for these groups.

Permissions are assigned to users at the time of account creation, but can be changed at any time by users with Facility Administrator or State Administrator (sometimes called System Administrator) permissions. Facility Administrators may assign Facility Administrator, Facility Staff, Peer Review, and Data Upload permissions. Only State Administrators may assign State Administrator or Regional Trauma Coordinator privileges.

Table 1: Groups and Permissions		Permissions by module, tabs, and sub-tabs						
A. User Group	B. Description	Patient Registry					E. Report Writer	F. Administration
		C. Data Exchange	D. Facilities					
			Staff	Users	Setup	Incidents		
Data Upload	This group is designed for third party vendors for uploading data.	View, edit, and add*	No access	No access	No access	No access	No access	No access
Peer Review	This rarely assigned user group is only able to view incidents with status marked as “requires review” for up to 14 days after creation. They cannot see patient identifiable information.	No access	No access	No access	No access	View only “requires review”	No access	No access
Facility Staff	This is the most common user group that is assigned. Users in this group can perform data entry and upload data. They cannot delete records or perform administrative functions.	View, edit, and add*	View all	View all	No access	View, edit, and add all	*Facility Staff:* View, edit, and add all	No access
Facility Administrator	Users in this group can perform the same functions as Facility Staff, but also have the ability to perform administrative functions for their hospital(s). These include account management and facility settings.	View, edit, add, and delete*	View, edit, add, and delete all	View, edit, and add all	View, edit, add, and delete all	View, edit, add, and delete all	*Facility Staff:* View, edit, and add all	No access
Regional Trauma Coordinators	These users have the ability to view incident records, but not to modify the records. It is reserved for the SOM Regional Trauma Coordinators.	View*	View all	View all	View all	View all	*Regional Trauma Coordinators:* View, edit, and add all	No access
State Administrator	This group is given full rights to the application. Only MDHHS staff have this level of access to the program, which allows for password resets, troubleshooting data uploads, and other administrative functions	View, edit, add, and delete all	View, edit, add, and delete all	View, edit, add, and delete all	View, edit, add, and delete all	View, edit, add, and delete all	*State Administrator:* View, edit, add, and delete all	View, edit, add, and delete all

*All users except the State Administrators can only access data uploads initiated by themselves. Only the State Administrator can see uploads initiated by other users.

b. Adding New Users

The workflow for a Facility Administrator to add a new user is listed below.

1. Obtain information about the user (if needed) and a signed User Agreement.
    a. Information needed includes:
        - Name
        - Title/Position
        - Email
        - Work Telephone
        - Work Address
        - If the user wants to be a primary contact for the patient registry

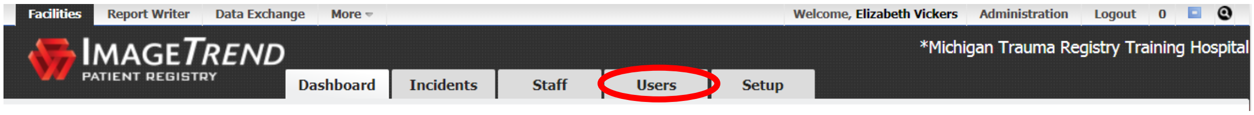
    b. If a user is requesting access to multiple facilities, additional information is requested, including:
        i. Valid User Agreement listing all facilities on the signature page OR a separate User Agreement for each facility, and
        ii. Email permission from authorizing staff at each facility for this person to access the data in ImageTrend.

    c. After obtaining the User Agreement(s), review the User Agreement for completeness. Tips for completeness include:
        - All fields must be filled out and complete. Any forms with incomplete or missing fields must be corrected.
        - An authorizing supervisor must sign the form- you may not be your own supervisor.
        - Signatures must not be typed. The form may be signed with an ink pen or via a program that allows insertion of an electronic signature (such as Adobe).
        - All signatures require dates on the same line.
        - All three pages of the User Agreement must be sent back, not just the signature page.

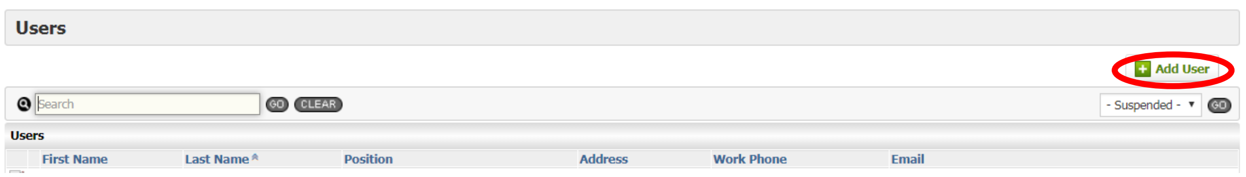
    d. Send the completed User Agreement(s) to the MDHHS Trauma Section within 10 days of account creation. **The MI Trauma Registrar may inactivate newly created accounts if the User Agreement is not provided**. The completed User Agreement may be sent via:
        - Email (preferred), to StateTraumaRegistrar@Michigan.gov, or
        - Fax, to (517) 335-9434

2. Sign in to the MI Trauma Registry at https://www.mi-emsis.org/patientregistry/. This will bring you to the Dashboard for the last facility that you accessed. Make sure that you are at the right facility.

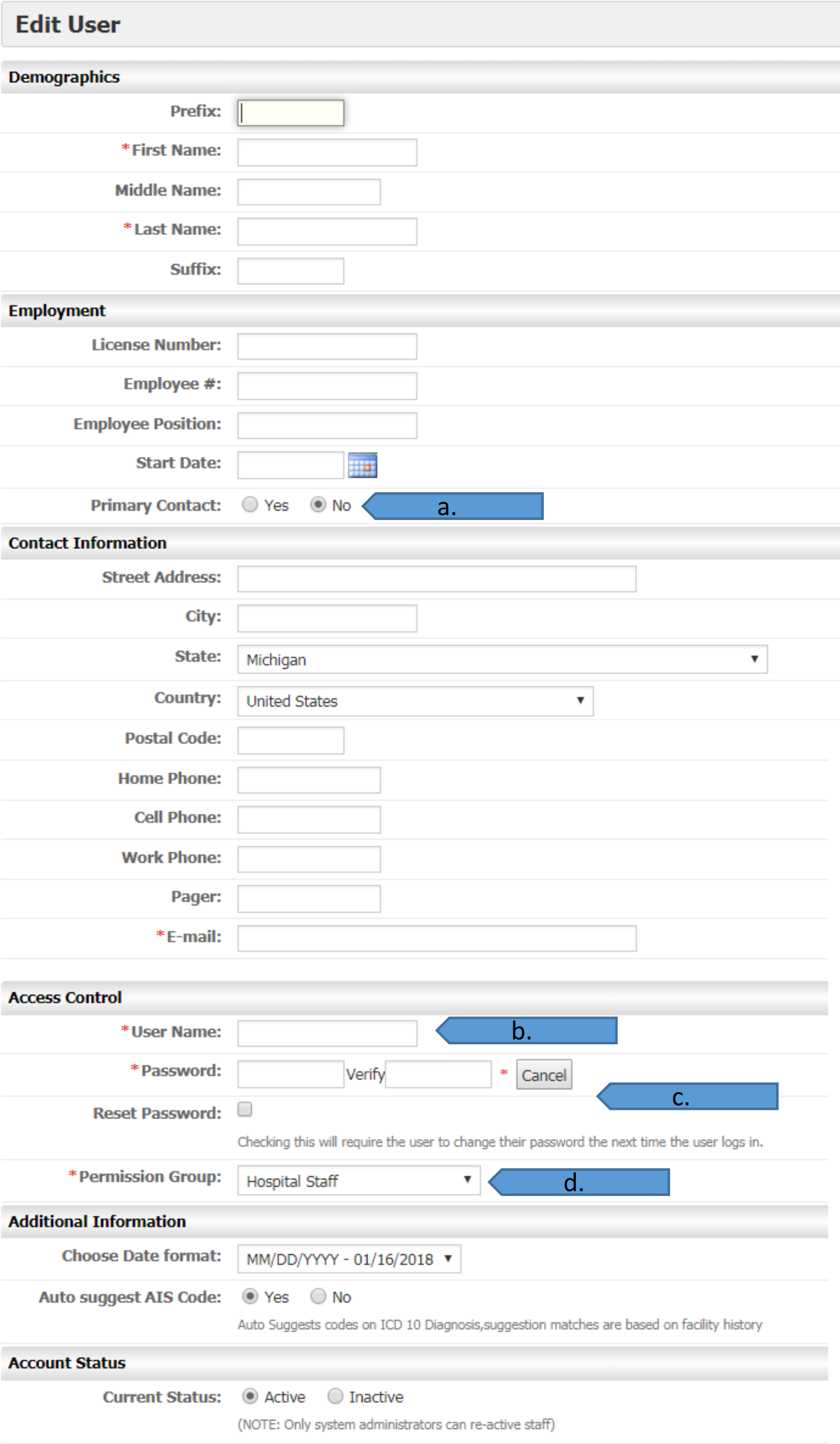
3. Open the user list for that facility by clicking on the "Users" tab.



4. Add a new user by clicking on the green "Add User" box, on the top right.



5. This will open the User Information page. Add the new user's information to this page. Best practices for this page are listed on the next page. **Please fill out as much of the form as possible, not just the minimum required information.** This helps with maintaining the most current contact information.



Edit User

Demographics

Prefix:	
*First Name:	
Middle Name:	
*Last Name:	
Suffix:	

Employment

License Number:	
Employee #:	
Employee Position:	
Start Date:	
Primary Contact:	○ Yes ● No

Contact Information

Street Address:	
City:	
State:	Michigan ▾
Country:	United States ▾
Postal Code:	
Home Phone:	
Cell Phone:	
Work Phone:	
Pager:	
*E-mail:	

Access Control

*User Name:	
*Password:	Verify * Cancel
Reset Password:	□ Checking this will require the user to change their password the next time the user logs in.
*Permission Group:	Hospital Staff ▾

Additional Information

Choose Date format:	MM/DD/YYYY - 01/16/2018 ▾
Auto suggest AIS Code:	● Yes ○ No Auto Suggests codes on ICD 10 Diagnosis,suggestion matches are based on facility history

Account Status

Current Status:	● Active ○ Inactive (NOTE: Only system administrators can re-active staff)

(Continued from previous page- Adding New Users, Step 5)

a. At present, all active users will receive correspondence about the MI Trauma Registry. However, if primary contact is selected, this user will be the first person (or one of the first persons) to be contacted for facility-specific correspondence with the MI Trauma Registrar. A facility can have any number of primary contacts.

b. Usernames are typically assigned with last name and first initial.

c. Assign a temporary password meeting requirements and take note of it for later. Check the box for "Reset Password" so that the user can decide on their own password after the first sign-in.

d. Assign the appropriate permission groups, as described in section a. above.
   - MDHHS strongly recommends that only one user is given Facility Administrator privileges for security reasons. Most users will be assigned to the Facility Staff group.
   - Facility Staff report writer access is automatically assigned to all Facility Staff and Facility Administrator user groups. This can be removed, if needed, by selecting "no access".

e. Facility permissions for this user will automatically be assigned for the current facility. If a user needs permissions for multiple facilities, contact the StateTraumaRegistrar@Michigan.gov mailbox for assistance.

6. After all information has been added, click the "save" button on the bottom left of the form.
7. After the user account has been created, share the temporary password. The system will prompt the new user to choose their own password upon first sign-in.

5. Editing Users, Assisting with Login Issues, and Inactivating Accounts

a. Types of Account Lockouts

There are two type of account lockouts in the MI Trauma Registry- suspensions and inactivations.

A user account may become suspended due to:

- Too many incorrect password attempts,
- >120 days since login,
- System resets (uncontrollable), or
- Other unforeseen reasons.

If the user has been suspended, they will need to be unsuspended for a password reset to work. If a user has forgotten their password, it is best to allow them to reset it from the "Forgot your password?" link on the sign in page. This is the most secure way of resetting passwords. However, passwords may occasionally be reset manually if this link does not work.

Suspensions are different from inactivations, which require an Administrator to assign. Reasons for account inactivation include:

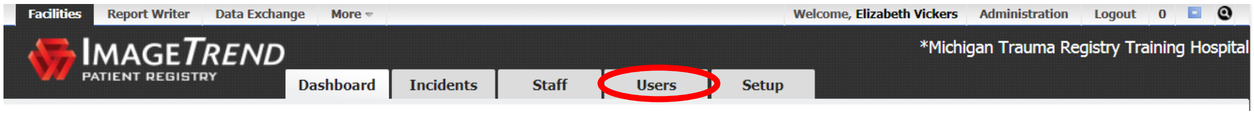
- The user is no longer working for a facility,
- They have not provided a User Agreement,
- The user is on temporary leave, and
- Other requests for inactivation.

Contact the State Administrator (StateTraumaRegistrar@Michigan.gov) if an account needs to be inactivated or reactivated.

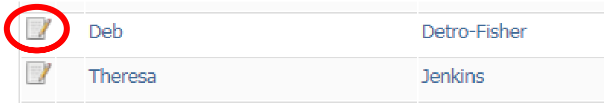
b. Editing the User Information Page

The User Information page can be used to update information in the MI Trauma Registry, restore account access, and remove account access for most users. However, if facility permissions need to be changed or revoked, contact the MI Trauma Registrar (StateTraumaRegistrar@Michigan.gov).

1. Sign in to the MI Trauma Registry at https://www.mi-emsis.org/patientregistry/. This will bring you to the Dashboard for the last facility that you accessed. Make sure that you are at the right facility.
2. Open the user list for that facility by clicking on the “Users” tab.

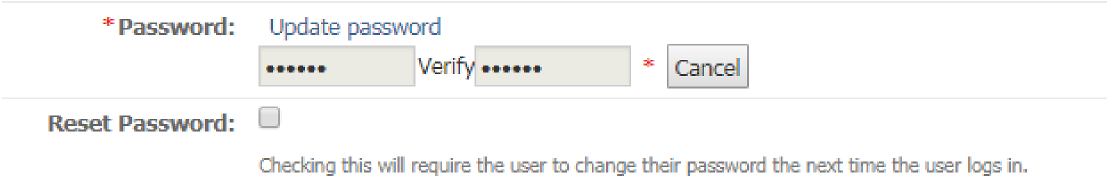


3. Open the Edit User Information page by clicking on the pencil and paper icon to the left of the user’s name.



✎	Deb	Detro-Fisher
✎	Theresa	Jenkins

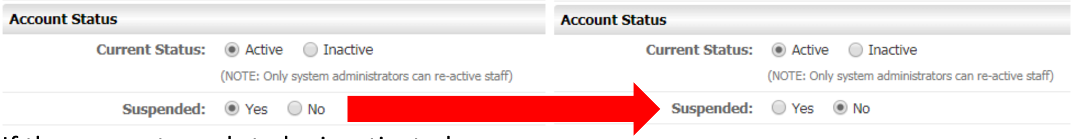
4. On the User Information page, make the necessary changes.
   a. If you are changing any information about the user, erase the old information (if needed) and type in the new information.
   b. If a password reset is needed, assign a temporary password following the steps below.
      1) Type the temporary password in both of the password boxes. Passwords must be at least 7 characters long and contain at least one number and one special character. Passwords cannot be reused.
      2) Click “Update Password” in blue.
      3) Check the “Temporary Password” box.



*Password: Update password
●●●●●● Verify ●●●●●● * Cancel

Reset Password: □
Checking this will require the user to change their password the next time the user logs in.

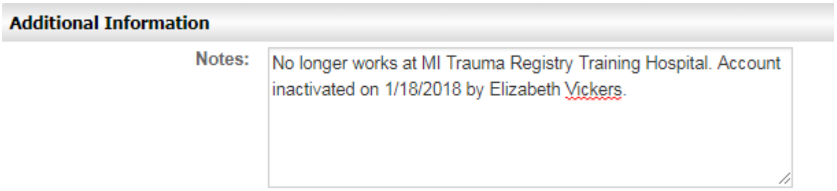
   c. If an unsuspension is needed: Locate the suspension status in the “Account Access” section. Unsuspend an account by selecting “No” on the “Suspended” line.



Account Status
Current Status: ● Active ○ Inactive
(NOTE: Only system administrators can re-active staff)
Suspended: ● Yes ○ No

Account Status
Current Status: ● Active ○ Inactive
(NOTE: Only system administrators can re-active staff)
Suspended: ○ Yes ● No

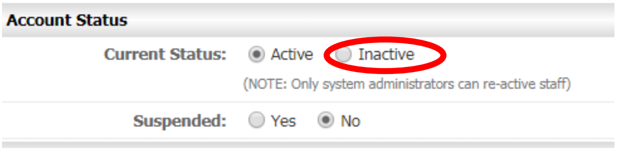
   d. If the account needs to be inactivated:
      1) Add a description of the account inactivation in the “Notes” section. This needs to include the reason for inactivation, the date of inactivation, and who inactivated the account (your name). DO NOT remove notes that are already present.



Additional Information

Notes: No longer works at MI Trauma Registry Training Hospital. Account inactivated on 1/18/2018 by Elizabeth Vickers.

2) Select "Inactive" in the "Account Access" section.



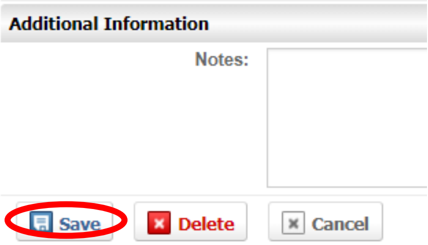
Account Status

Current Status: ● Active ○ Inactive

(NOTE: Only system administrators can re-active staff)

Suspended: ○ Yes ● No

5. When all necessary changes are made, click the "Save" button on the bottom of the page and the changes will take effect.



Additional Information

Notes:

If you have inactivated the account, this user will no longer appear on the user list for that facility and they will no longer be able to sign in. If this was done in error, contact the MI Trauma Registrar (StateTraumaRegistrar@Michigan.gov) to reverse the inactivation.

6. If needed, share the temporary password with the user. The MDHHS Trauma Section strongly recommends that you share the username and temporary password in different methods of communication (for example, send the username via email and share the temporary password over the phone). When they sign in, the system will prompt them to change the password to one of their choosing.
7. If needed, notify the MI Trauma Registrar (StateTraumaRegistrar@Michigan.gov) of any account inactivations.

6. Facility Administrator Responsibilities and Considerations

Facilities are allowed to manage their own user accounts so that the Trauma Registry can be an effective tool. However, this means that facilities have additional responsibilities related to their users and the security of the information contained within the Registry. Since Facility Administrators have privileges or account management, they are the users responsible for maintaining this information.

Facility Administrators will:

1. Add new users for the facility as necessary, with the appropriate level of access. This means that each person is only given access to what is necessary to perform their job functions. MDHHS strongly recommends only one Facility Administrator (person with the ability to create accounts) per facility.
2. Keep the user list and information about the users up to date in the MI Trauma Registry. This particularly includes deactivating accounts immediately after an employee leaves the facility or

when you become aware that the user no longer needs account access. ***This is a web-based application and can be accessed from any computer. Not removing user access to those who have left your facility leaves open the possibility of a patient data breach. MDHHS assumes no responsibility for disabling accounts for those who have left your facility or otherwise should not have access.***

3. Notify the MI Trauma Registrar of changes in staffing, especially in regards to primary contacts. Contact information stored in the MI Trauma Registry is used to notify facilities of late submissions; attempts to contact the facility will be escalated if a response is not received (see Policy for Data Submission and Missed Deadlines). MDHHS takes no responsibility for communications that do not reach the facility due to out-of-date contact information in the MI Trauma Registry.
4. If the Facility Administrator leaves, either:
    a. assign the new Facility Administrator the correct privileges and have that person inactivate the account, or
    b. contact the MI Trauma Registrar and request removal of account access.
5. Notify the MI Trauma Registrar and ImageTrend **immediately** of any suspected breaches in confidentiality from inappropriate user access, malware, or any other means that the facility becomes aware of.
6. Ensure that the appropriate legal representative for the facility has agreed to and completed the Data Use and Non-Disclosure Agreement and that this document is sent to the MDHHS Trauma Section.
7. Ensure that all users at the facility have agreed to and completed the User Agreement at the time that they are given account access and that these documents are sent to the MDHHS Trauma Section **within 10 days of account creation**.
8. Ensure that users at your facility are aware of and following current best practices for account security.

7. Best Practices for Account Security

Listed below are guidelines for all users in maintaining security of the information in the MI Trauma Registry. These guidelines are in addition to the practices listed in the User Agreement. Please share with your facility staff and ensure that they are adhering to these best practices.

1. Actively log out of ImageTrend when the program is not being used. Do not leave the ImageTrend website open on your computer while logged in.
2. Do not share your username or password with anyone.
3. Do not allow the internet browser to auto-fill your password on the sign-in page.
4. Do not store user names or passwords on the computer and delete any emails with password information.
5. Immediately report any malware, virus, or similar attacks to the MI Trauma Registrar and ImageTrend so that the system can be monitored for security threats.
6. Report a stolen computer to the Facility Administrator or the MI Trauma Registrar so that your account may be monitored and/or deactivated, as appropriate.

8. Questions or Feedback

The MDHHS Trauma team are happy to answer any questions or to consider any feedback about this document or the procedures described within. Please direct questions or feedback to the MI Trauma Registrar via email at StateTraumaRegistrar@Michigan.gov.