MIRCal Security Tip

To: All MIRCal Users
From: OSHPD - Patient Data Section
Subject: MIRCal User ID and Password Security

The following User ID and password security procedures follow industry best practices and should be adhered to in order to ensure data integrity and compliance with the HIPAA security rules.

Your User ID and password should be kept secure. For your own protection, **DO NOT SHARE YOUR USER ID AND PASSWORD**. Do not allow your facility's confidential data to be compromised by someone else using your MIRCal account. Day-to-day processes within MIRCal are logged and tracked for each action by means of your user account. The design of MIRCal allows multiple users from each facility to have access to their data. The person associated with a User ID is responsible for all actions within the MIRCal system attributed to that account. OSHPD retains the right to revoke user access if misuse is discovered.

MIRCal allows a total of ten (10) active user accounts per facility. Each facility must have at least one, and up to three, users whom the facility administrator has approved to act as their MIRCal User Account Administrator(s) (UAA). The UAA is responsible for maintaining current user information for all other MIRCal users at a facility. For instance:

- Creating user accounts
- Granting roles (access to various MIRCal functions)
- Assigning contacts (Primary, Secondary (optional), and Administrator)
- Changing passwords
- Unlocking accounts
- Inactivating user accounts (staff that leave or no longer need access)
- Maintaining user accounts (updating name, address, phone number, email, etc.)

Frequently Asked Questions:

Q: I can't remember my password and my account is locked. Do I contact my OSHPD analyst?
A: It depends. The UAA is the central contact for facility staff when handling user account related questions and issues. Three key points to keep in mind: 1) If you are the only active UAA at your facility, or a Designated Agent, and need help with your individual account, you will need to contact your OSHPD analyst to change your password or unlock your account; 2) if your facility has more than one active UAA, a UAA can obtain assistance from another UAA with changing their password and unlocking their account; 3) all other users that are not a UAA should contact their UAA for assistance with account related questions and issues.

Q: Someone left our facility but gave me their User ID and password to use. Is that ok?
A: No. The UAA should inactivate the account for the user that left, and create a new account for you.

Q: I only need temporary access to MIRCal. Can I use the User ID of one of our other users?
A: No. The UAA should create an account for you, then inactivate your account when you no longer need access.

Q: Our only UAA is about to leave and I will be her replacement. How can I get access?
A: Only OSHPD can grant the UAA role but the UAA can create a user account and grant other roles to you before they leave. Whoever will be performing the UAA role must complete and submit a User Account Administrator (UAA) Agreement form to OSHPD. Please allow 48 hours for OSHPD to process the request once it is received.

Q: I am a UAA and will be leaving soon. Can I inactivate my own account?
A: Yes. Before you inactivate your account, make sure that your facility is not left stranded without any users/UAAs (see the FAQ above). If you are listed as a Primary Contact and/or Facility Administrator, assign another user as the Primary Contact and/or Facility Administrator, so the facility will continue to receive correspondence from us. Lastly, when you no longer need access, go to the modify user screen, remove (deselect) your roles, change your user status to inactive, and apply the changes.

Q: I shared my User ID and password with someone already but no longer want them to use my account. Do I need a new account?
A: No. Once logged on, you should change your password using the "Change Password" link on the left side main menu. For security of your confidential data, do not share your User ID and password.

For a quick refresher on Maintaining Users (UAA role only), review our Training Module for User Account Administrators. Please share this information with the information security professional at your facility. Your facility may have additional security protocols that must be followed regarding User ID and password.

Rev. September 2018