

CORC Security Tips



To: All CORC Users
From: CCORP and OSHPD
Subject: CORC System User ID and Password Security

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

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

The CORC System allows a total of ten (10) active user accounts per hospital. The 10 users may include up to seven Hospital Users plus an additional three users may have the role to act as User Account Administrator (UAA) for your hospital. The UAA is responsible for maintaining current user information for all users at a hospital. UAA's can:

- Create hospital user accounts
 - Grant user roles (i.e. access to various CORC functions)
 - Assign hospital contacts (Primary Data Contact, Secondary [optional] and Administrator/CEO)
 - Change passwords for hospital users
 - Unlock hospital user accounts
 - Inactivate hospital user accounts (staff that leave or no longer need access)
 - Maintain hospital user accounts (update profile info such as name, address, phone number, e-mail, etc.)
-

Frequently Asked Questions:

Q: I can't remember my password and my account is locked. Do I contact CCORP?

A: **It depends.** The UAA is the central contact for hospital CCORP 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 hospital, and need help with your individual account, you will need to contact OSHPD to change your password or unlock your account; 2) if your hospital has more than one active UAA, a UAA can obtain assistance from another UAA with changing their password and unlocking their account; and, 3) all other users that are not a UAA should contact their UAA for assistance with account related questions and issues.

Q: Someone with CORC access left our hospital but gave me her 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 CORC. 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 CCORP. Please allow 48 hours for CCORP 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 hospital is not left stranded without any users/UAA's (see the FAQ above). If you are listed as a Primary Contact and/or CEO/Administrator, assign another user as the Primary Contact and/or CEO/Administrator, so the hospital 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.

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