









Keep office information **SECURE!**

MAY 2024

-  **Don't share user IDs.** Each employee who needs access should have an individual ID.
-  **Protect passwords.** The safest passwords are hard to guess, never shared and never posted where others can see them. Create unique passwords that use a minimum of eight characters and have a combination of words, numbers, symbols and upper and lowercase letters.
-  **Use separate Wi-Fi networks,** one for your practice and another for personal devices or guest use (for example, Practice, Practice Guest). Use separate passwords for each.
-  **Make sure laptops and desktops are secured** (cabled or stored in a locked drawer) when left unattended.
-  **Lock your workstation screens** when not in use.
-  **Maintain a safe, confidential and secure work area** regardless of work location. Follow additional safeguards to protect PHI by taking added precautions to prevent inadvertent disclosures, such as storing PHI in locked cabinets or in a locked room.
-  **We strongly encourage you to encrypt protected health information** stored on laptops to minimize the risk of a cyber security incident if a laptop is lost or stolen.
-  **Diskettes, thumb drives and other removable media** containing PHI should be **encrypted** before being removed from the office.

Revoke Availity® access when employees depart

To safeguard protected health information and comply with federal law, health care providers must revoke former employees' access to Blue Cross and BCN systems. Administrators must revoke former employees' access when they leave their positions.

If Availity access isn't revoked and the former employee inappropriately accesses PHI, the health care provider organization is responsible for notifying affected members of the information breach, which could be very costly.

Take the proper steps today

It's easy for an administrator to revoke Availity access when an employee leaves or no longer requires access.

To revoke user access in Availity:

- Log in to [availity.com](https://www.availity.com).*
- Select *Manage My Team(s)* (under your account name in the top right of the menu bar).
- Select *Organization (Customer ID)* If applicable.
- Search by team member's last name, first name, user ID or email address.
- Select the action menu > click *Deactivate User*.

Note: For users associated with multiple organizations, their access needs to be revoked for each organization, individually.

If you have any questions, contact an Availity Client Services representative at **1-800-282-4548** (800-AVAILITY) from 8 a.m. to 8 p.m. Monday through Friday.

Review access periodically

We recommend a review of your employees' access needs **every three months**. Large organizations might consider more frequent reviews depending on employee turnover or other operational concerns.

Availity® is an independent company that contracts with Blue Cross Blue Shield of Michigan and Blue Care Network to offer provider portal and electronic data interchange services.

*Blue Cross Blue Shield of Michigan doesn't own or control this website.