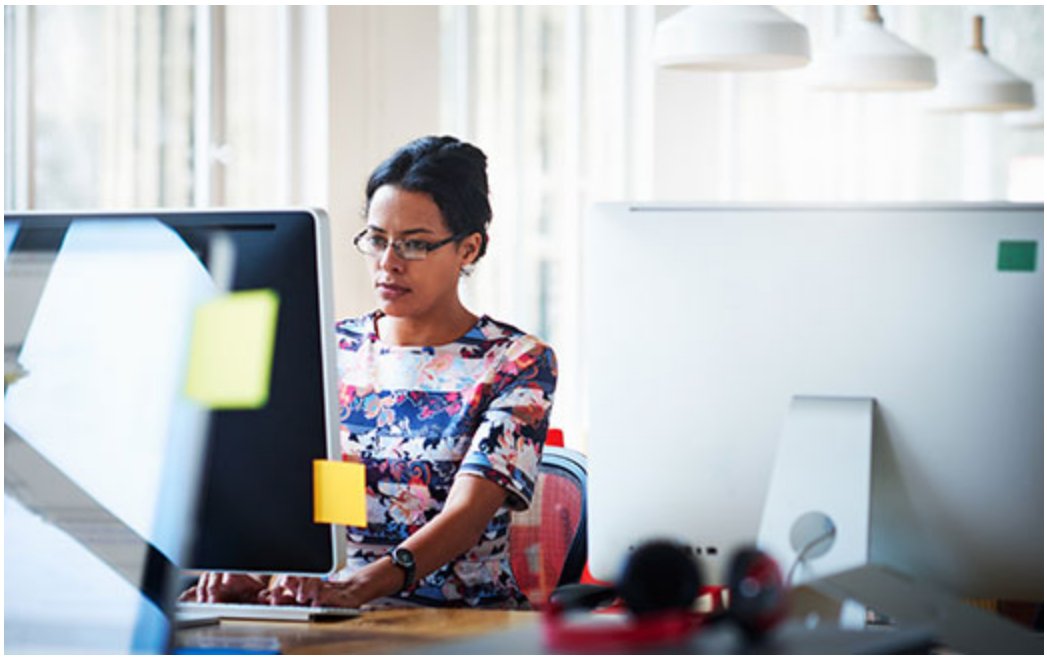
Who is managing your secure provider portal account?

Sign in – Secure Provider Portal



We encourage you and your staff to access the Blue Cross® Blue Shield® of Arizona (BCBSAZ) secure provider portal at azblue.com/providers. Each provider organization may set up an account and then create as many additional user accounts as needed.

Encourage your billing team to avoid common PHI security errors.

Your designated “account administrator” plays an important role in keeping your portal account safe. To ensure HIPAA compliance and avoid the risk of protected health information (PHI) exposure, this person should be one of your employees, not a representative of a billing company.

Who is your account administrator?

Your organization’s portal account is overseen and managed by your account administrator. If you’re not sure who holds this responsibility, you can go to “Practice Management > Account Management > My User Account.” You’ll see the name of the person who can make changes to your account. If your account is managed by someone with an “office manager” user role, you can ask that person for the name of the account administrator. For a comprehensive report on your account, contact us at .

Updates to the portal terms and conditions

We have updated the portal terms and conditions for more clarity pertaining to provider responsibilities. Here is the updated excerpt from the “Security” section of the agreement:

G. Access to azblue.com interactive web applications, as described in these terms and conditions, shall be available only to, and used only by, authorized individuals. Authorized individuals are:

- The organization’s designated account administrator to whom BCBSAZ has granted access. This person must be an employee of the organization (not a representative of a third-party billing service).
- The individuals that the account administrator has authorized on behalf of the organization.

  Note: The “financial manager” user role may only be assigned to an employee of the organization (not a representative of a third-party billing service).

Any account administrator shall have and maintain adequate and appropriate policies and procedures for authorizing access and protecting information available through the azblue.com interactive web applications.

Organizations may not assign the portal account administrator role/responsibility to a third-party billing service representative. Likewise, the financial manager user role may not be assigned to a third-party billing representative. Non-compliance with these requirements may result in termination of usage rights.

Why certain account roles should be assigned only to your employees

Although you are welcome to give your third-party biller access to your organization’s account, you may not assign them as the overall administrator for the account, or for the office manager or financial manager user roles.

The account administrator and office manager user roles hold the following responsibilities on behalf of your organization:

1. Authority to assign tax IDs to your account (the tax IDs in your account should be limited to those associated with your organization and not include tax IDs of other organizations that a third-party biller may be working with in addition to your company)
2. Authority to set up unlimited user roles for your organization (you must only create user accounts for your employees and specific third-party billers working with your organization—not for other billing company staff who are not working with your organization)

Note: When you’re assigning the financial manager role to someone who already has a portal user account, you must create a new, additional user account.

The “financial manager” role holds authority to make EFT changes for your organization.

All three of these user roles may only be assigned to your employees.

Account audits

We review portal accounts to ensure compliance with HIPAA requirements and assess risk of PHI exposure. If we determine that an account is at risk of exposing PHI, we may delete the account.

Reminder: All account users must have their own login credentials

Please ensure that all account users have their own unique username that is not shared by others in your organization. For security reasons, sharing login credentials is prohibited by the terms and conditions of the portal registration agreement.

If a user is no longer part of your practice or no longer needs to access the portal, please delete the user account from your account profile.

Questions?
If you have questions about your portal account, please reach out to your provider liaison or call Provider Partnerships at 602-864-4231 or 1-800-232-2345, ext. 4231.

Our members can take a digital ID card with them wherever they go with the MyBlue AZ℠ mobile app.