ACCURO

MOVING FROM A LOCAL SERVER TO ACCURO CLOUD

Frequently Asked Questions

When you transition to Accuro Cloud, you get enhanced data security through multi-factor authentication (MFA), and access to Cloud-only features like the **Accuro Admin Centre** and the **ACCUROgo** mobile companion app.

Accuro Cloud will improve Accuro performance, stability, and security while also lowering your IT costs.

What are the benefits of moving to a Cloud solution?

- Multi-Factor Authentication (MFA), which ensures that you, and only you, are logging in
- No more server hardware or software licensing costs
- Automatic updates, upgrades, and back-ups that don't interrupt your workflows
- Stronger security with detection monitoring that reduces your exposure to ransomware attacks
- Remote access to AccuroEMR from anywhere with an internet connection
- Scalable data storage that ensures you have room as your clinic grows
- 24-hour support and consistently reliable server up-times for better stability

Is this transition to Accuro Cloud mandatory?

Yes - this transition is mandatory and we are scheduling our local server clients to transition to Accuro Cloud throughout 2024.

Multi-factor authentication (MFA) is the new standard in security, and without it your patient data is at risk from hacking and ransomware. MFA is only available in a Cloud-based environment. Cloud computing also gives QHR Technologies greater agility in developing new product features and supporting our clients.

ACCURO

Will my data be safe? And where will it be stored?

Ransomware attacks disproportionately target local servers, and QHR invests in security systems that are more advanced than what most clinics can provide on their own. Your data will always be stored in Canada in a professionally managed co-location data center. Active data and backups are stored in a data center in Toronto, with a second backup stored in our Kelowna data center. In the not-too distant future, some or all of your data will be stored in Microsoft Azure Canada Central and Azure Canada East.

How quickly will I transition?

The timing depends on your availability and the readiness of your clinic, but at the moment we're scheduling moves about 4 to 6 weeks ahead. The process has a few steps, including contracting and actual migration with a short period of downtime. Enterprise clients will require special arrangements. We encourage you to schedule your transition as soon as possible.

How does implementation work?

1. You sign up today to schedule your transition.
2. Our sales team will contact you to outline your contract and determine which of your users are moving to the Cloud.
3. Once the contract is signed, it's handed over to the project team.
4. A project manager/IT coordinator will work with your clinic for a seamless transition.
5. You schedule the Cloud implementation, at which time your clinic may need to close for a short period.
6. You're up and running!

Does my clinic have to close during the transition?

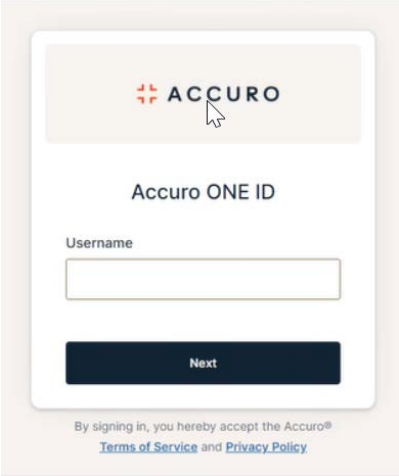
Yes, though for how long will depend on a few things, including clinic size, internet speeds, and the amount of data being moved.

Other things:

- Some clinics may require one-time, 3rd party IT support during the implementation process.
- Computers, printers, and fax machines are already configured for the Cloud, but we'll work with each clinic to determine whether those devices can stay connected to the clinic server if that's the preference.

How much will it cost?

Costs will vary by customer and may depend on clinic size. Our competitive costing structure encompasses your subscriptions, hosting, back-ups, updates, and access to advanced features like ACCUROgo and Accuro Admin Centre.



What does the user sign in experience look like?

Accuro ONE ID is a FREE single-sign on experience which also triggers multi-factor authentication (MFA). Every clinic will be able to choose the MFA options available to its users.

accuroemr.com/move-to-cloud/

ACCURO

Multi-Factor Authentication (MFA)

Is MFA mandatory?

If you use QHR's included identity management solution, your users do have to use MFA to log in to Accuro Cloud. MFA is an important security feature for protecting your data.

If your company uses federated identity management, however, you can set your own rules for identity management.

What types of MFA do you support or not support, and why?

We support a wide variety of MFA options, including one-time passwords (OTP), physical tokens such as Yubikey, MS Authenticator, Google Authenticator, or similar apps available for smartphones.

We encourage your users to use a password manager, such as 1Password or similar, and many password managers have OTP and/or authenticators built in.

We do not support MFA via SMS (text message on phones) or via email because they are not as secure as the methods we do support. Of course, if you use your own identity and access management system and federate it with our system, you can use whatever type of authentication you choose.

Recommended MFA Option – Okta Verify with a smartphone

If you are comfortable using your smart phone for authentication, Okta Verify is the choice we recommend for you.

To prove your identity with Okta Verify, you can either approve a push notification or enter a one-time code the first time you sign in to Accuro Cloud.

Other options for Multi-Factor Authentication without a smartphone

To help you decide which tool is right for you, we've done a breakdown of the various kinds of MFA tools with a short description of the pros and cons of each.

We've also created a decision tree that provides a quick visual of the decisions your clinic will need to make, and when to make them, along the path to Accuro Cloud.

A Security Key or Biometric Authenticator

The Security Key or Biometric Authenticator gives you the ability to pick computer authentication options that you might already be using in your clinic. Some common options are:

WINDOWS HELLO

This authentication method uses a biometric (fingerprint, iris scan, or facial recognition) or PIN. It is enabled for all Windows 10 and 11 users. Please see Windows Hello Setup for more information.

TOUCH ID (APPLE DEVICES ONLY)

Much like Windows Hello, Touch ID uses a fingerprint as a biometric to authenticate your account. Touch ID is only set up for iPhone, iPad, and MacBook Pro. See Touch ID Setup for more information.

YUBIKEY

This is a physical hardware device, similar to a USB Stick, and is used as a security token that allows users to add a second authentication factor. Please see yubico.com for more information.

What are the system requirements?

All of our computer, hardware, internet, and operating system requirements can be found here:

https://accuroemr.com/cloud-system-requirements This link is updated regularly.

Will my clinic continue to use the Citrix Receiver?

Yes. We typically recommend that you continue using the receiver wherever it was used prior. With Accuro Cloud, however, we have a new Preview option available that allows users to select 'Launch Accuro in Browser' using a web browser such as Google Chrome, Safari, or Microsoft Edge.