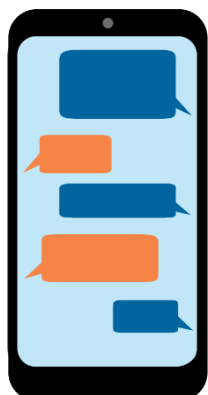


# Virtual Health: Our Virtual Care Chat App



**Virtual health** allows you to see, hear, talk to, and chat with your healthcare team from your home.

You can use a smartphone, tablet, or personal computer with a web camera and microphone.

You need to be able to connect to the internet through cable, Wi-Fi, satellite, or cellular data. You are responsible for costs related to this connection.

## Using virtual health, you can...

- ✓ **Get access** to healthcare providers and services.
- ✓ **Work with** your healthcare provider from home to plan your care.



## Can I contact my care team without using the chat app?

Yes, you can always contact your healthcare team by phone or email.

## Can I contact a specific person of my care team using the chat app?

Not at this time. When you send a message, everyone on your care team can see it. Any one of the care team could then reply to you.

## How does the chat app work?

- This app allows you to chat with people on your care team any time during our service hours.
- We need your email address so that we can email you to invite you to join a chat conversation. The email includes a link to the chat conversation.
- After we have started a chat conversation, you can send messages to us and we can send messages to you.
- The chat stays open until you are no longer a patient with the care team. If you change to a new care team and that team is also using this app, then a new chat might be started.
- Once you are no longer a patient with the care team using the chat app, we save the whole chat conversation and place it in your health record.
- If you feel the chat app isn't working for you for any reason, you can opt out at any time. In the email that invited you to join the chat, there is an "opt-out" link. All you have to do is click the link. If you prefer, you can call us and let us know you no longer wish to use the chat app.

## Virtual Health: Risks of Using Technology

### How is my privacy protected?

There are risks to using this type of technology to send personal information.



We will not send personal information by email unless we have to. We will do what we can to confirm that any personal information we send is being received by you and only you, but it is never possible to be 100% certain who we are communicating with outside of a face-to-face visit.

Be assured that we adhere to the *B.C. Freedom of Information and Protection of Privacy Act* for everything related to your virtual health visits.

Only those healthcare providers involved in your care are allowed to see or hear your personal health information.

We do not record your virtual health visit. We ask that you do not record it either.

Your virtual visit is very secure (encrypted). Unfortunately, we cannot guarantee that the visit will not be transmitted outside of Canada. This is because of the way this technology works and where the application company is located.

### Are there risks to communicating electronically?

Yes, unfortunately there are.



- Your information could be requested, viewed, changed, or deleted if you allow computer programs, applications, or people access to your device or email account.
- Your information could be at risk if it is stored on a device infected with a computer virus or malware (malicious software usually installed without your knowledge).
- Third parties can intercept electronic communications.

For more on how we care for your information, see '[Caring for Your Information](#)' under 'Risks of using technology' online by:

- searching '[Virtual Health Tools](#)' on [fraserhealth.ca](http://fraserhealth.ca)
- clicking the links above
- scanning this QR code



### How can I protect my privacy?

Please note that we cannot control what happens to your information once it is stored:

- on your device
- by your telecommunications provider
- by software or application providers
- by other applications that might have access to your messages

You are responsible for the security of your own computer, tablet, smartphone, and email service.

### Tips to help protect your privacy:

- ✓ Protect your passwords! Someone could pose as you by sending us a request from your device or email account.
- ✓ Delete emails and texts you no longer need.
- ✓ Download computer software and applications (Apps) from trusted sources (Google Play, Apple App Store).
- ✓ Set permission controls on your device so applications do not have access to your text messages and emails.
- ✓ Set limits on what other information you permit your Apps to access.
- ✓ When using Wi-Fi, use a secure Wi-Fi network. Try not to send personal information while using public Wi-Fi.
- ✓ Use antivirus software on your devices. Regularly scan your devices for viruses and malware.
- ✓ If you share your computer screen with your healthcare provider, make sure they cannot see anything you want to keep private.

### Not sure how to do some of these things?

Ask a person you trust to help you set up your device so it is secure.