Australian Government
Department of Health
Therapeutic Goods Administration

Cyber security for your medical device

Some medical devices can connect to the internet, communicate with a phone, or send information to other people. Your device may also connect through other methods, such as USB or Bluetooth.

These digital features make your medical device more useful, but have cyber security risks you need to understand and manage.

Questions to ask about your medical device

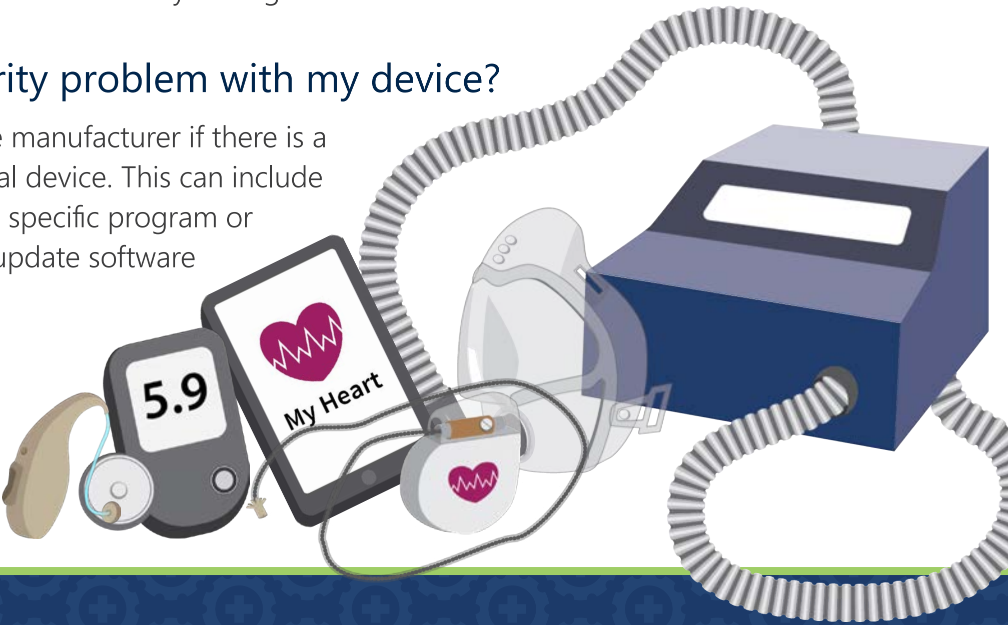
Ask your doctor or the manufacturer of the medical device these questions:

- What are the cyber security risks associated with use of my device?
- What are the default security settings?
- What happens to the security of the device if I change the default settings?
- When and how does this device connect to the internet (for example, home wifi, mobile networks or public wifi)?
- What information is collected and stored on the device or my smartphone, where does it go, and who has access to it?
- How can I tell if a device has been hacked or compromised and who should I talk to if this is suspected?
- What do I need to do to maintain the security of my device (for example, updates)?
- If the device connects to another product, such as my smartphone or computer, do I need to check any settings, such as password settings and connectivity settings?

What if there is a cyber security problem with my device?

You will usually receive an alert from the manufacturer if there is a cyber security problem with your medical device. This can include your computer, smartphone, tablet, or a specific program or app. The manufacturer may ask you to update software or change your password.

If you become aware of a cyber security problem with your medical device, follow the manufacturer's instructions, seek further information from the manufacturer, or consult your doctor.



For more information see
www.tga.gov.au/medical-device-cyber-security-consumer-information

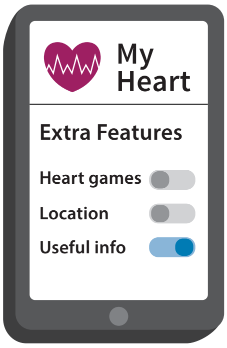
7 ways to help keep your devices cyber secure

Be careful when away from home

Avoid connecting to public networks. If you must connect to a public network, minimise sending or receiving sensitive information.

Only use features you need

Turn off features you do not use, or use rarely. You should speak to your doctor before turning off any features.

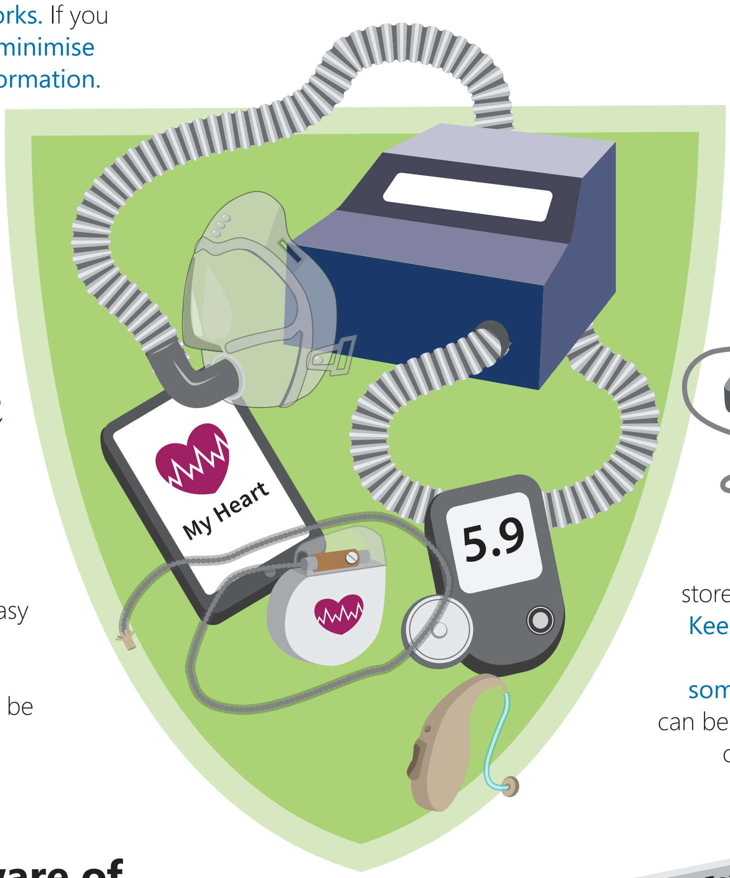

My Heart

Extra Features

Heart games ○

Location ○

Useful info ●



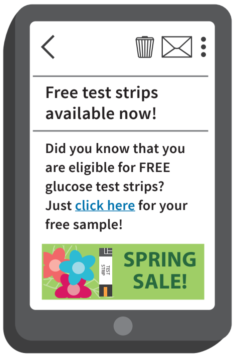
horsecupstarshoe

Use passphrases

Use a unique hard-to-guess passphrase as your password.
A passphrase is a phrase that only you are likely to know and that is easy for you to remember, but hard for someone else to guess.
It's recommended that passphrases be made up of at least 4 words.

Use backups and protection

Your medical device might store valuable data for your healthcare. Keeping up-to-date backups of your data can help you recover it if something does go wrong. This copy can be on a USB stick, external hard drive or a reputable online cloud service.


Free test strips available now!

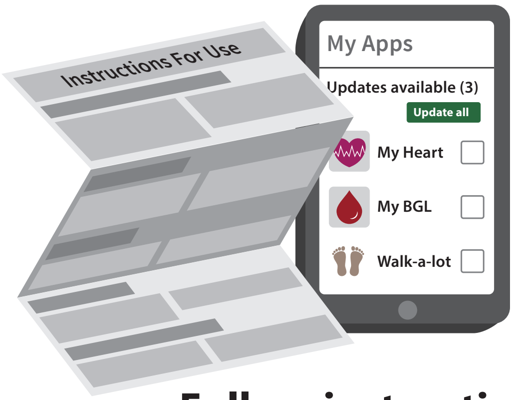
Did you know that you are eligible for FREE glucose test strips? Just click here for your free sample!

SPRING SALE!

Be aware of suspicious messaging

Hackers might try to obtain sensitive information from you or harm your device by imitating electronic messaging from your doctor or device.

Do not respond to or click on links in any suspicious message you receive.



My Apps

Updates available (3)

Update all

My Heart □

My BGL □

Walk-a-lot □

Stay up-to-date

Keep your device up-to-date with the latest security software. This will help prevent unauthorised access, and help protect against new cyber security problems.

Security Update available

Download and apply

Follow instructions

Read the information provided with your medical device and new information provided by the manufacturer or your doctor, including its instructions for safe use and maintenance.