

Cyber security, data breach and electronic communication with patients

Ruth Crampton and Cheryl Wood

Agenda



Cyber

Demonstrate the immediate action required if a cyber threat is suspected



Data breach

Discuss the OAIC mandatory data breach requirements



Digital communication

Explain the appropriate preparation and planning required for digital communication



Emailing patients

Identify key risks and how to minimise them when emailing patients

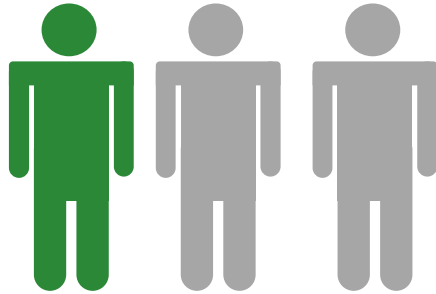
Agenda



Cyber

Demonstrate the immediate action
required if a cyber threat is
suspected

Why cyber security



Only a third of Australian Healthcare organisations embed cyber security and awareness training into their policies and procedures



Cost in excess of 3
Billion dollars
\$3,500,000,000

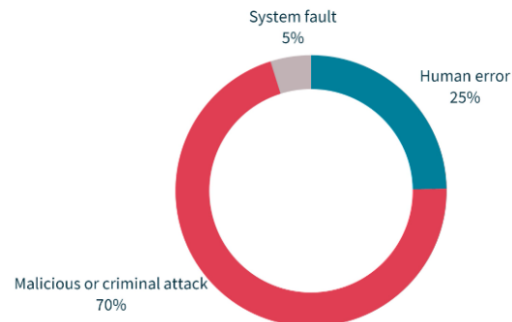
<https://www.digitalhealth.gov.au/>

58%

Breached when
patch available



Sources of data breaches



Use passphrases for better security

Change your passwords to passphrases to keep your accounts and data secure.

[Learn more](#)



Get alerts on new threats



Report a cybercrime or cyber security incident



Become a partner



Information Security Manual

Latest alerts and advisories

[View all alerts and advisories](#) →

31 MAR 2023

Alert rating: Medium ⓘ

Supply chain compromise of 3CX DesktopApp

The ACSC is aware of a reported supply chain compromise affecting the 3CX DesktopApp, allowing malicious actors to conduct multi-stage attacks against users of the legitimate software. Australian users of affected versions of 3CX DesktopApp should...



29 MAR 2023

Alert rating: High ⓘ

High Severity Vulnerability present in Microsoft Outlook for Windows

The Australian Cyber Security Centre (ACSC) is aware of a Microsoft Outlook for Windows vulnerability. All Australian organisations using all versions of Microsoft Outlook for Windows should apply the available patch immediately.



20 MAR 2023

Advisory

2023-03: ACSC Ransomware Profile – Lockbit 3.0

The Australian Cyber Security Centre (ACSC) is aware of Lockbit 3.0 which is the newest version of Lockbit ransomware. It is used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia....



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

	Lowercase letters only	At least one uppercase letter	At least one uppercase letter + number	At least one uppercase letter + number + symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org



Essential 8 best practices (ASCS)

- 1 Application control
- 2 Patch applications
- 3 Configure Microsoft Office macro settings
- 4 User application hardening
- 5 Restrict administrative privileges
- 6 Patch operating systems
- 7 Multi-factor authentication
- 8 Daily back-ups

More on back-ups

3 copies ideal



Working files



Cloud



Hard drive

Human factors matter



Plan for the unexpected

- Fire, flood, earthquake other disasters can strike at any time. Be prepared for this to happen at any time.
- There are two parts to this process:
 - 1 have backup systems in place
 - 2 have a sound recovery plan

Cyber Security Policy

- Set out best practice for cyber safety such as password management, use of devices off site
- Outlines education required for staff
- Requirements for back-up systems, how often they are backed up and tested
- Regulations about white-listing apps
- Guidelines for administration privileges and staff access to which data

Cyber Response Plan

- Immediate actions if attack suspected
- Contact details for IT providers
- Roles of responsibilities for staff if attack confirmed
- Process for notification of patients
- Instructions on how and when to access back up data
- Contact details for media support, insurance etc

How to recognise you are under attack

- Typical symptoms include:
 - system will not start normally (blue screen of death)
 - system repeatedly crashes for no obvious reason
 - internet browser goes to unwanted webpages
 - anti-virus software appears not to be working many unwanted advertisements pop up on screen
 - cannot use mouse



This is the primary way attackers compromise computers

If you are attacked

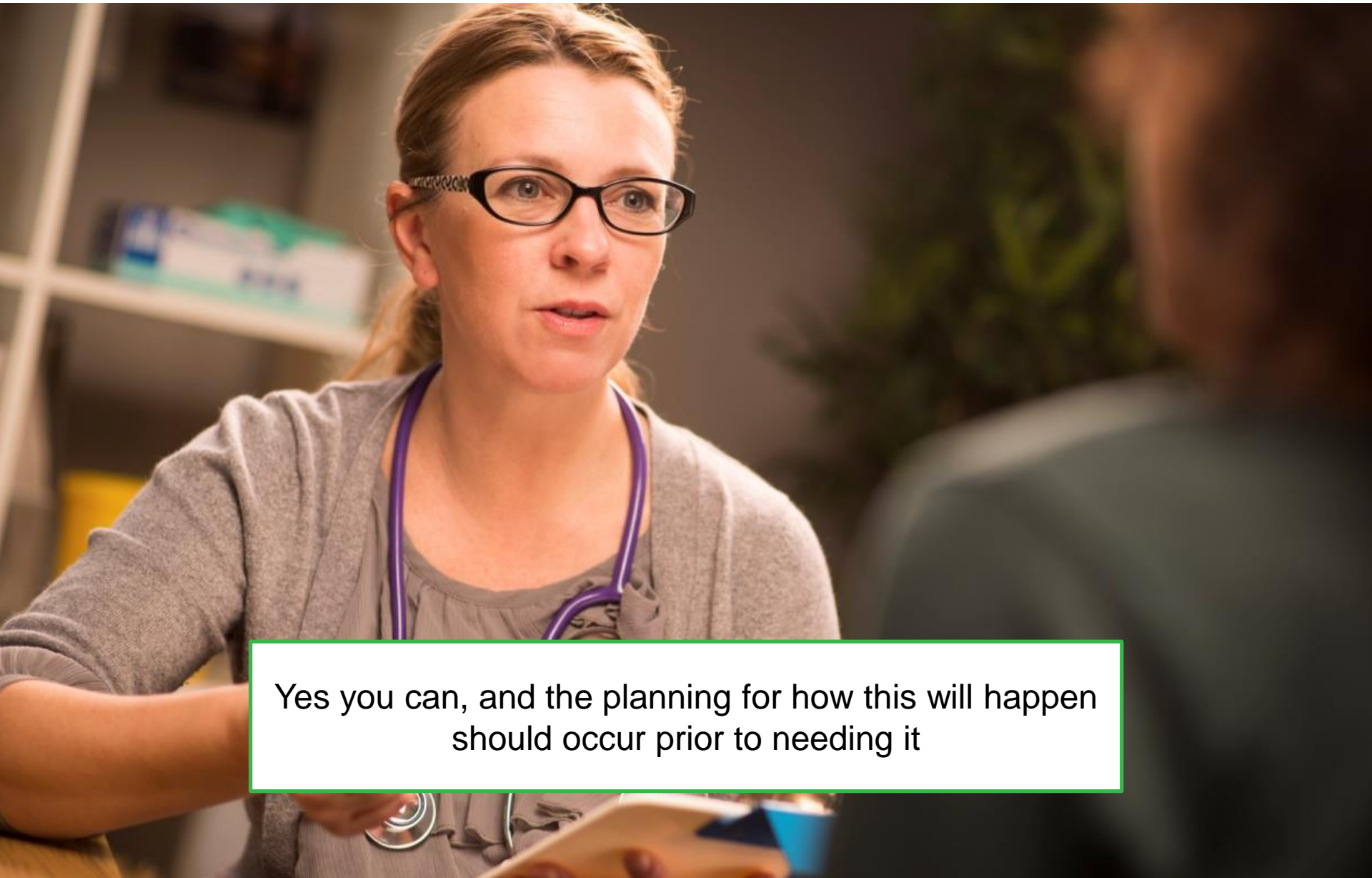


Should we pay the ransom?



Generally the advice is not to pay

Can we still see patients?



Yes you can, and the planning for how this will happen should occur prior to needing it

After an attack



DATA
BREACH

Agenda



Cyber

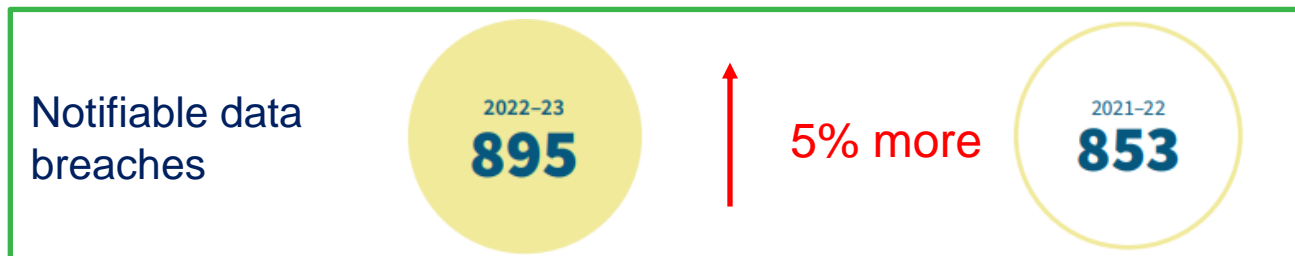
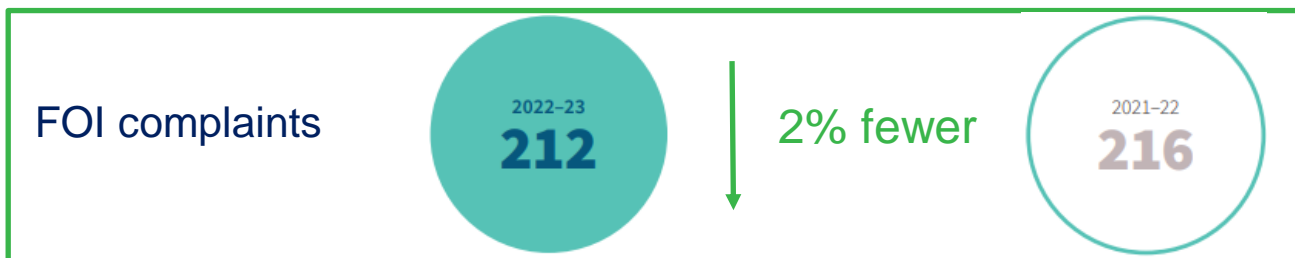
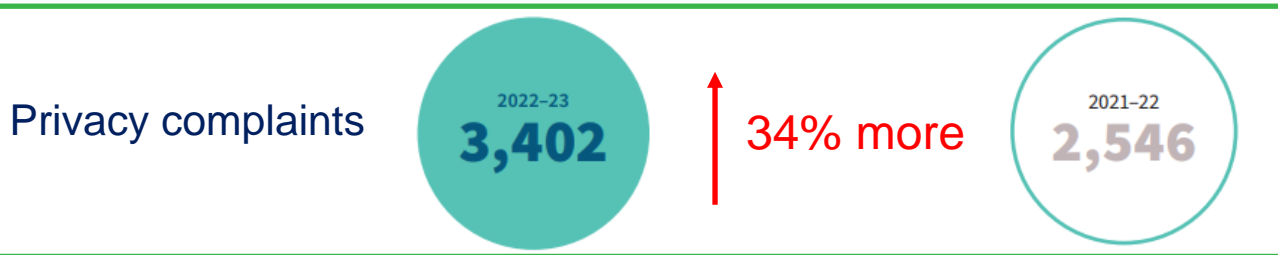
Demonstrate the immediate action required if a cyber threat is suspected



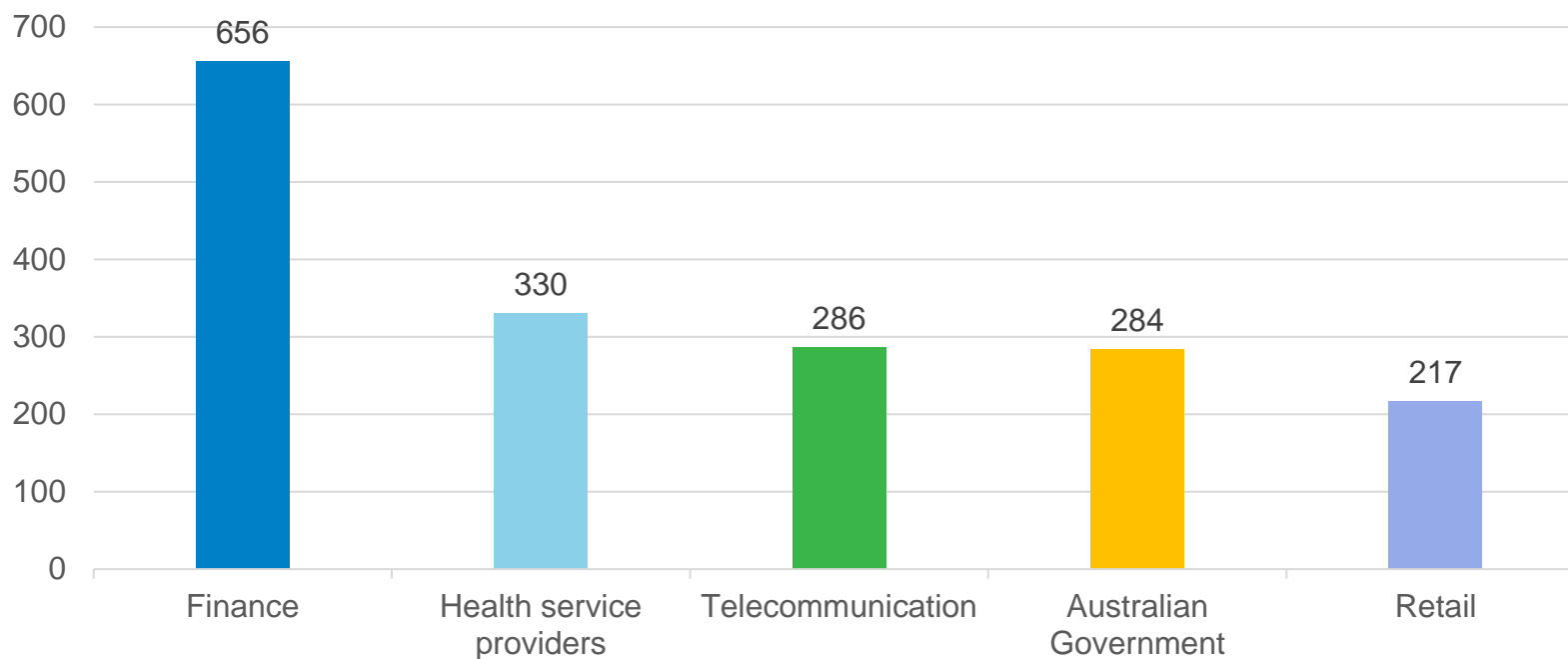
Data breach

Discuss the OAIC mandatory data breach requirements

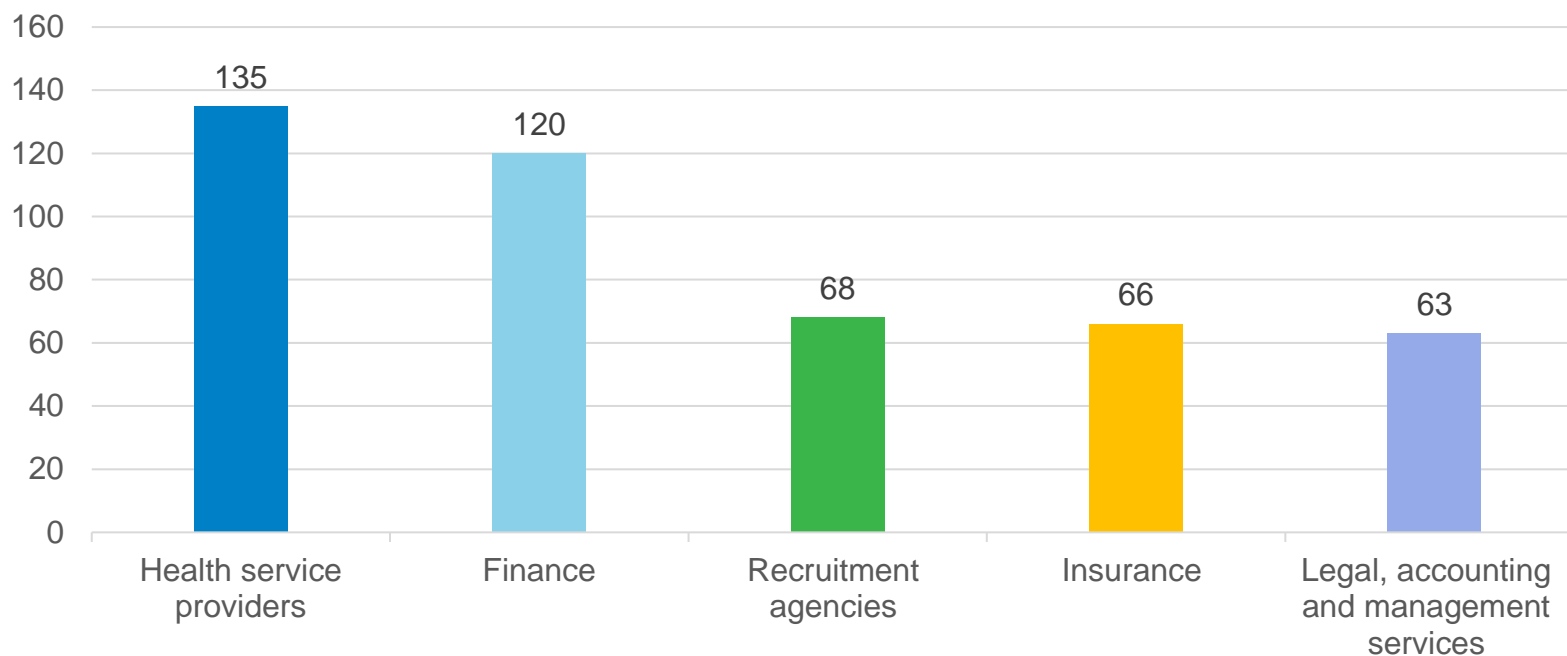
OAIC Annual Report 2022-23



Top 5 sectors by privacy complaints received

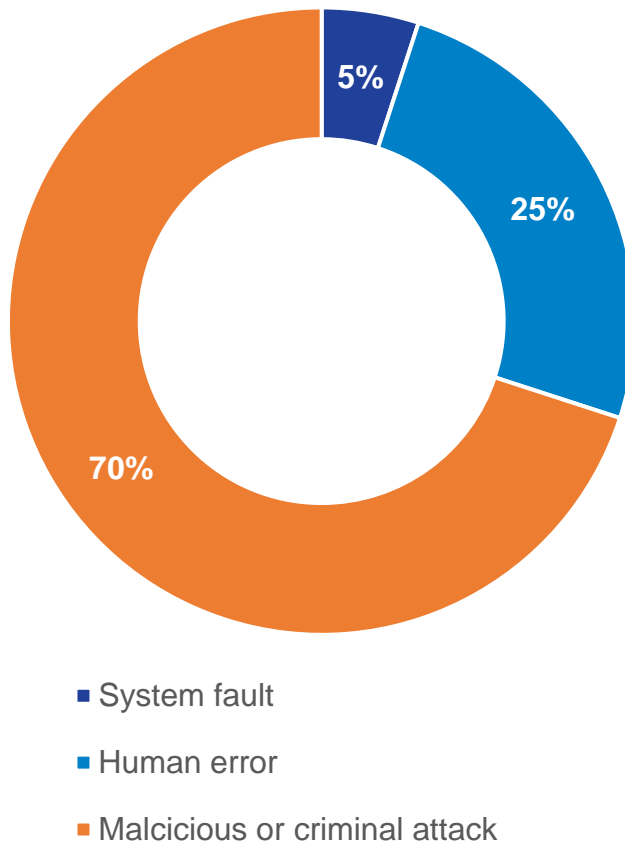


Top 5 sectors by data breach complaints received

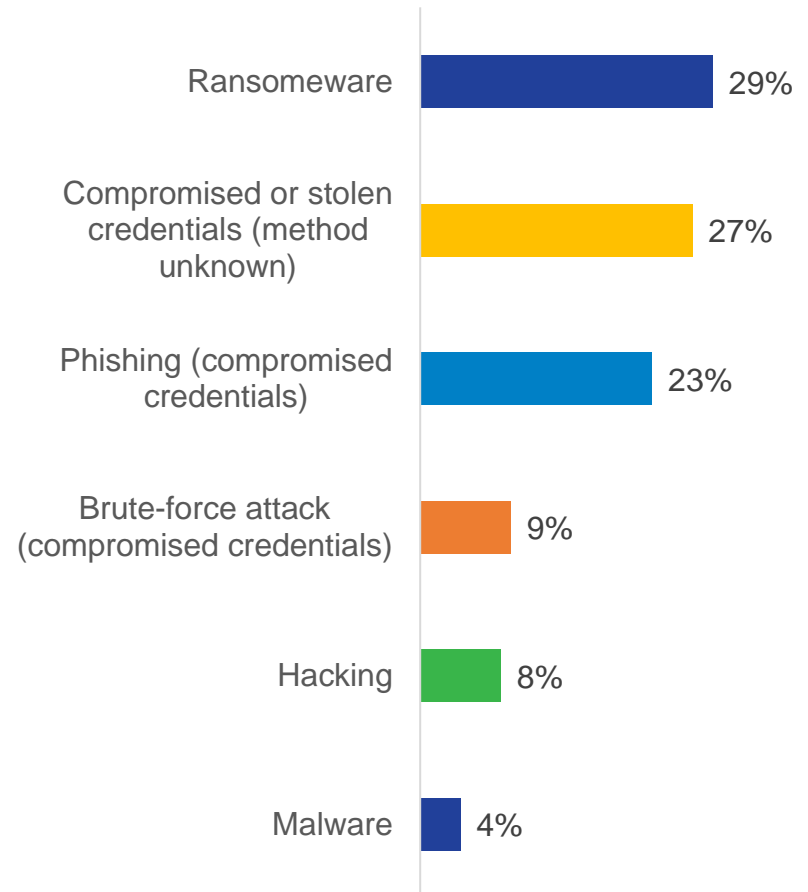


Notifiable data breaches report

Sources of data breaches



Cyber incident breakdown



Example – privacy breach



PRIVACY

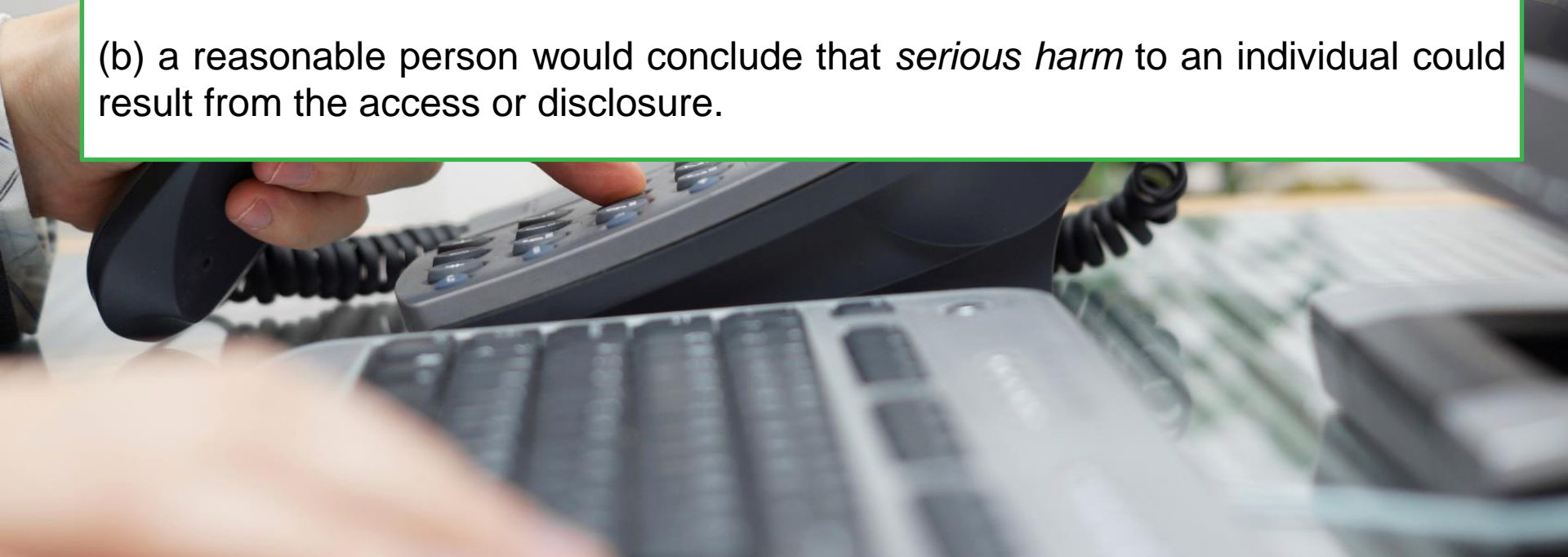
The word "PRIVACY" is displayed in large, bold, white capital letters. The letter "V" is highlighted in orange. The text is centered over a blue background featuring a large, faint circular graphic with several interlocking gears of different sizes. In the background, there are also faint, out-of-focus silhouettes of people.

What is an 'eligible data breach'?

(a) either:

- i. there is unauthorised access to, or unauthorised disclosure of, information held by a health provider; or
- ii. information is lost in circumstances where there is likely to be unauthorised access to or unauthorised disclosure of information; and

(b) a reasonable person would conclude that *serious harm* to an individual could result from the access or disclosure.



What is not an 'eligible data breach'?

If an entity takes remedial action:

- (a) prior to any serious harm occurring from a data breach
- (b) prior to any unauthorised disclosure, access or loss of information
- (c) after information is lost, accessed or disclosed, but before that access or disclosure results in any serious harm to an individual



If a breach occurs you are required:

- To assess
- To notify OAIC if criteria met
- To notify affected individuals



Example: security of practice IP



5 best practice tips from OAIC

Employee training

Preventative technologies and processes

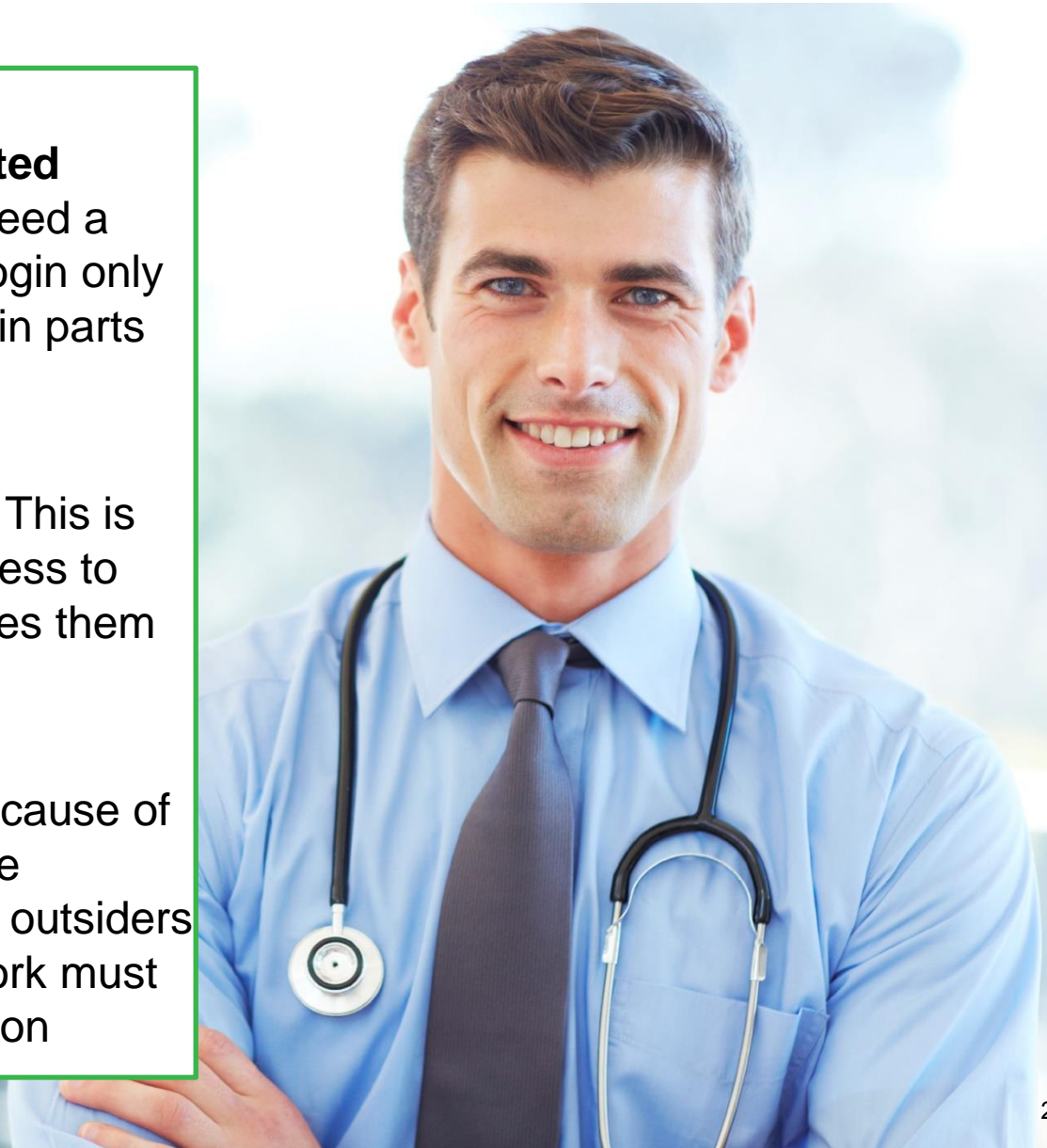
Preparation

Assessment of harm

Post-breach communication

Control access to your system

- **Control access to protected health information.** You need a system so an individual's login only gives them access to certain parts of your system
- **Control physical access.** This is controlling not only the access to files but securing the devices themselves
- **Limit network access.** Because of the sensitivity of health care information tools that allow outsiders to gain access to the network must be used with extreme caution



Communication after a breach



Responsive



Empathetic



Accountable



Competent



Transparent

[HOME](#)[CARDIOLOGY ▾](#)[ABOUT](#)[OUR TEAM](#)[CONDITIONS](#)[PROCEDURES](#)[CONTACT US](#)

HEART SPECIALISTS |

25 February, 2019

wishes to advise all our patients that the cybersecurity incident we experienced in late January has been resolved. The data has been decrypted and our systems have been restored. Once again we would like to emphasise that patients' privacy has not been compromised or breached. No information left our computer system - it was encrypted so that no one could see it, even ourselves. We would like to thank all our patients for their understanding over this period.

Established over a decade ago,

has

the best cardiologists at your service.



Cyber security - what you need to know

Summary:

With so much of our personal and work lives connected to the internet the risk of experiencing a cyber incident is always increasing. Our resources provide a guide to minimising the chances of a cyber incident and planning so you know what to do if an incident occurs.

Practices GPs Specialist

Documentation & medical records

Landing Pages

Technology

05 / 08 / 2019

Cyber security resources



Preventing a cyber incident

Steps to minimise the chances of a cyber attack

Factsheet: Steps to protect your practice from a cyber incident

Video: Being aware of cyber security

eLearning: Module 1: Preparing to manage privacy and security risks



Under attack...

Don't panic. Get the right team together. Confirm the facts.

Factsheet: Responding to a cyber security incident

eLearning: Module 3: Responding to a data breach or security incident



After the event

Lessons learned. Is there a notifiable data breach?

Landing page: Data breaches: all you need to know



Cybersecurity checklist

Use this checklist to review the security measures in your practice

Factsheet: Cybersecurity checklist



Learn a bit more

Listen or watch for more information on cyber security

Article: 7 steps to avoiding a human data breach

Podcast: It happened to me: Cyber attack

eLearning: Module 2: Day-to-day privacy and security best practices



Common online threats

Explanation of cyber security terminology

Glossary

Agenda



Cyber

Demonstrate the immediate action required if a cyber threat is suspected



Data breach

Discuss the OAIC mandatory data breach requirements



Digital communication

Explain the appropriate preparation and planning required for digital communication

Policy and processes

- Cyber Security & Response
- Data breach
- Privacy
- Email
- SMS messaging
- Telehealth



Cyber Security Policy

- Set out best practice for cyber safety such as password management, use of devices off site
- Outlines education required for staff
- Requirements for back-up systems, how often they are backed up and tested
- Regulations about white-listing apps
- Guidelines for administration privileges and staff access to which data

Cyber Response Plan

- Immediate actions if attack suspected
- Contact details for IT providers
- Roles of responsibilities for staff if attack confirmed
- Process for notification of patients
- Instructions on how and when to access back up data
- Contact details for media support, insurance etc

Privacy Policy

- > Outlines staff behaviour and training
- > Patient electronic communication guidelines
- > Storage of patient data

Data Breach Response Plan

- > Advice on containment and assessment of data breach
- > Process on how to assess for harm
- > Who to notify – contact information
- > Outline of the information required for the notification statement

Patient Privacy Policy

- > Outlines collection, use and disclosure and security of patient information
- > Overview on how patients can access their medical records
- > How patients can make complaints about their privacy

Agenda



Cyber

Demonstrate the immediate action required if a cyber threat is suspected



Data breach

Discuss the OAIC mandatory data breach requirements



Digital communication

Explain the appropriate preparation and planning required for digital communication



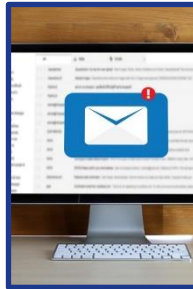
Emailing patients

Identify key risks and how to minimise them when emailing patients

Case study



Top cases of human error breaches



Personal information
sent to wrong recipient
(email) 42%



Unauthorised disclosure
(unintended release or
publication) 33%



Failure to use BCC
when sending email 6%

Have a clear policy

- Who can send
- What can be sent
- Who can it be sent to
- Address confirmation
- Consent confirmation
- Identify patient
- Document
- Password protection
- Defense building blocks – written system/training

Your policy and procedures manual should include:

- ☐ A statement as to when you and your team are willing to respond to email requests from patients (this will depend on the size of the practice and the ability to monitor emails and respond in a timely manner).
- ☐ What sorts of information will be sent by email and the level of protection required – encryption, secure messaging, password-protected attachments.
- ☐ If using passwords to protect a file outline the protocol on how that password is chosen and communicated to the patient.
- ☐ How you will confirm and document patient consent to communication by email.
- ☐ Steps staff need to take to avoid data breaches – checking email addresses, avoiding auto-complete text in addresses.
Refer to our article: [7 steps to avoid a human data breach](#)
- ☐ How you will ensure that electronic communications, including email and attachments, are retained, stored and destroyed in accordance with record-keeping requirements.
Refer to our factsheet: [storing retaining and disposing of medical records](#)
- ☐ Which staff are approved to send or reply to patient emails.
- ☐ Criteria for when patient emails must be referred to a doctor or other clinician for action.
- ☐ How you will respond to requests if you are unwilling to send information by email – whether because of practice capacity or because of the particular circumstances.

- ☐ When you will require confirmation of receipt, for example, for time-sensitive information.
- ☐ How you will manage and communicate about your use of practice email addresses – including auto-replies and ongoing monitoring of website email.
- ☐ Your policy if a data breach occurs via email with reference to your data breach policy.
See our information on [data breaches](#)
- ☐ Outline the exact wording for your practice privacy disclaimer to be included at the end of each email.

Disclaimer example

This communication is confidential and intended only for the individual or entity to whom it is addressed. No part of the email should be copied, disclosed or redistributed without [PRACTICE NAME'S] authorisation. If you have received this in error, please notify the sender of its incorrect delivery by reply email or phone [PRACTICE PHONE NUMBER].

Note: This email is only viewed once a day by a non-clinical staff member. Please do not send clinical queries via email.

Patient consent

1

Advise the patient about the risks associated with unencrypted email and confirm they still wish to have the information sent in that way.

2

Get patient consent in writing. If that is not practical, make sure you get the patient's verbal consent and document it in their clinical record.

3

If you have any concerns about their understanding and informed consent about the specific email, reconfirm details and consent with patient prior to sending.

Encryption

- Using encryption is the safest way to send an email and you should use it wherever possible.
- However, the OAIC does not insist that healthcare organisations use encryption as a minimum standard in all cases. Rather, you need to “develop procedures to manage the transmission of personal information via email”, recognising that email is not necessarily a secure form of communication.
- There are other ways to secure information i.e. encryption software



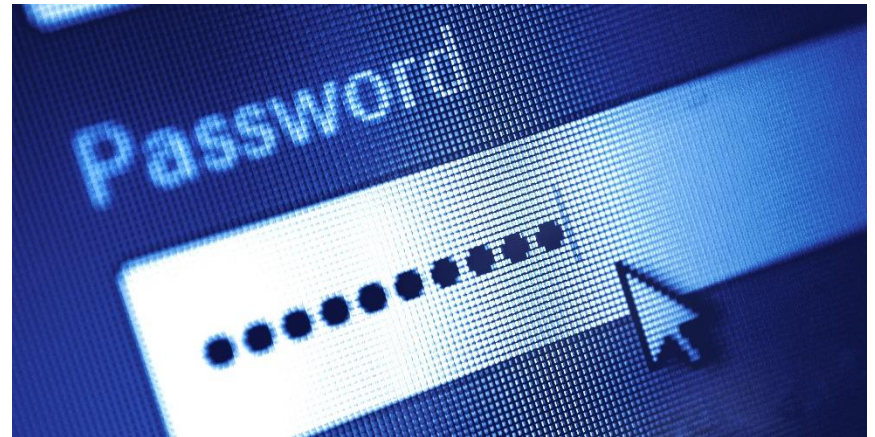
Check address before sending

- The OAIC consistently reports that private information being sent to the wrong recipient accounts for around one in 10 data breaches.
- Another emerging theme is errors involving auto-complete – where software programs default to recently or frequently used addresses.
- Other sources of error could involve misheard or mistyped email addresses, or accidentally using ‘reply all’.
- Patients may have more than one email address. They may not want information sent to a work or shared email for example, so make sure you check which address they want you to use.



Password protect sensitive information

- Your policy needs to address whether and how you will send particular types of information, for example results, prescriptions, or referrals.
- Some clinical or sensitive information should ideally be sent in a password-protected file. You will need to make this determination. In this case, make sure you take care to avoid including sensitive information in the body of the email.
- Your process also needs to include a protocol for providing the password (for example, phone the patient with the password).



Use a disclaimer

Disclaimer example This communication is confidential and intended only for the individual or entity to whom it is addressed. No part of the email should be copied, disclosed or redistributed without [PRACTICE NAME'S] authorisation. If you have received this in error, please notify the sender of its incorrect delivery by reply email or phone [PRACTICE PHONE NUMBER]. Note: This email is only viewed once a day by a non-clinical staff member. Please do not send clinical queries via email.

Double check C.A.N.D.O

STOP!!!!

Consent – pt or third party

Address – pt or third party

Name, DOB Address - all pages

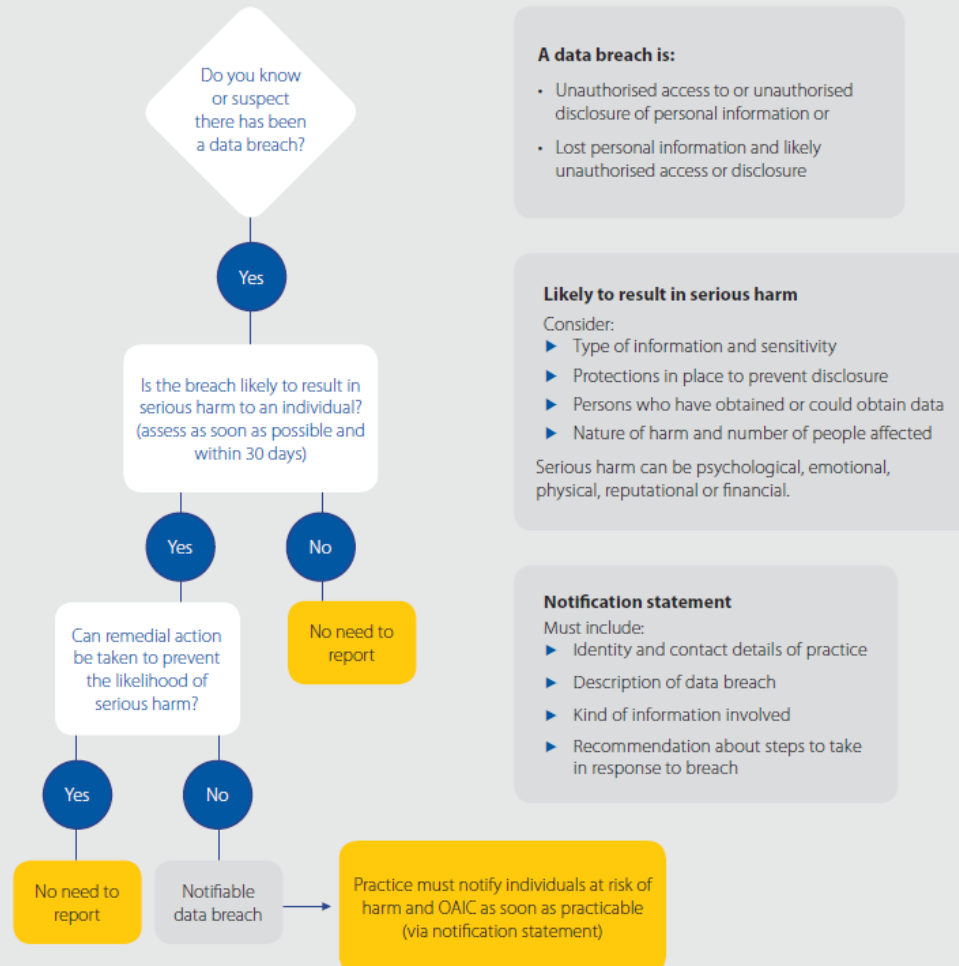
Document

Owner password



Notifiable Data Breach Scheme

From 22 February 2018, organisations covered by the Privacy Act 1988 are required to notify individuals likely to be at risk of serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner. Use the decision-making flowchart to assist you to determine whether to report a breach.



Documentation when emailing




- Policy
- Procedure
- Medical record
- Training
- Discussion

When is email inappropriate



Last words

- 
- > Employ experts to help
 - > Policies and procedure
 - > You need ongoing vigilance and training

Important notices

General disclaimer

The information in this presentation is general information relating to legal and/or clinical issues within Australia (unless otherwise stated). It is not intended to be legal advice and should not be considered as a substitute for obtaining personal legal or other professional advice or proper clinical decision-making having regard to the particular circumstances of the situation.

While we endeavour to ensure that documents are as current as possible at the time of preparation, we take no responsibility for matters arising from changed circumstances or information or material which may have become available subsequently. Avant Mutual Group Limited and its subsidiaries will not be liable for any loss or damage, however caused (including through negligence), that may be directly or indirectly suffered by you or anyone else in connection with the use of information provided in this document.