

HR + Tasmanian GP & Allied Health Leaders Conference

Cybersecurity and Artificial Intelligence (AI)
Know your obligations and risks



Cheryl Wood
Risk Adviser, Avant

Friday 14 June 2024

1



Agenda

Cybersecurity

- Overview of best practices to avoid a cyber incident
- What to do if an attack occurs
- The steps required following an attack

Artificial Intelligence (AI)

- AI scribing tools issues



2

2


Cyber security



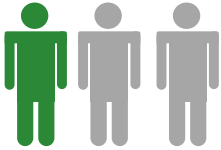
Avant
By doctors for doctors

3


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



4

4

Types of cyber attacks

5

5

Australian Cyber Security Centre




[Home | Cyber.gov.au](#)

6

Passwords



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



statista

<https://www.statista.com/chart/26298/time-it-would-take-a-computer-to-crack-a-password/>

7

7

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

<https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>

8

8

More on back-ups



3 copies ideal



Working files



Cloud



Hard drive

9







Human factors matter



10

10

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

11

11

Policy and process documents – cyber



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

12

12

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

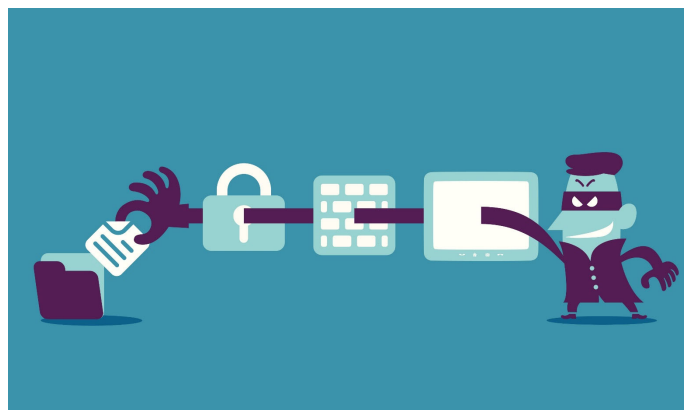


This is the primary way attackers compromise computers

13

13

If you are attacked



14

14

Should we pay the ransom?



Generally, the advice is not to pay

15

15

Can we still see patients?




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

16

16



After an attack

17

17

Cardiology group

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.

18

18

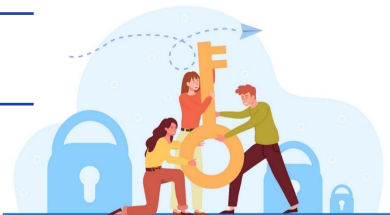
Key messages



Employ experts to help


Policies and procedure

You need ongoing vigilance and training




19

Artificial Intelligence (AI)



20



Case scenario


Dr Summer works in a busy GP practice – five GPs, one practice nurse, two reception staff and a practice manager

Dr Summer often runs late – the practice has received many complaints


Dr Summer's notes are not the best

Practice manager has heard about a new AI scribing tools at a conference "DocNoteMaster"







She suggests Dr Summer try it out as it might be useful for the practice



21



Artificial intelligence based scribing tools – issues

-  Consent
-  Privacy
-  Accuracy
-  Product terms and conditions
-  Quality and safety "medical grade"
fit for purpose
-  Due diligence and governance

22

Key points

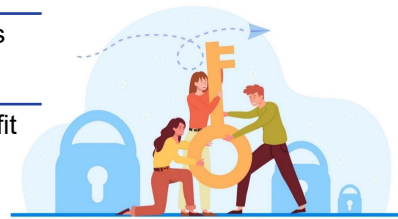


There are lots of potential benefits of using AI documentation tools in your practice

Do your due diligence – take your time!

Check the notes for accuracy – whatever is produced is a draft

Monitor use in your practice to ensure it is fit for purpose and meeting its objectives



23

Resources:

Cybersecurity

<https://avant.org.au/aer/cyber-collection>

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

<https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>

<https://www.statista.com/chart/26298/time-it-would-take-a-computer-to-crack-a-password/>

Artificial Intelligence (AI)

<https://avant.org.au/resources/using-chatgpt-to-help-with-paperwork-could-breach-patient-privacy>

YouTube Webinar

Medico-legal issues (incl AI) <https://www.youtube.com/watch?v=q5x2sjA-jMY>



24

Important notices

General disclaimer

The case discussed in this article/publication is based on a real case. Certain information has been de-identified to preserve privacy and confidentiality.

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.



Avant insights & resources

