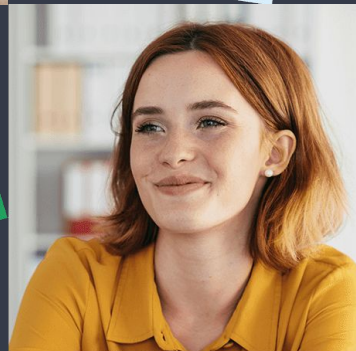
HotDoc

Security for Clinicians:

How to think about cyber security with analogies from healthcare

Thursday April 17



In the spirit of reconciliation, HotDoc acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community.

We pay our respect to their elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

Before we begin -

- This session is being recorded & you will be sent a link 4-6 hours after this session has concluded with the recording & resources
- Find all links to additional resources including the slides are in the “related content” section on your console/ screen
- Your CPD certificate will be accessible at the 40 minute mark, you can access via the certificate icon on your console
- Have a play around with the console/ icons on your screen, it’s an interactive experience

Who am I?

Tristan Lawrence
Head of Security & Privacy

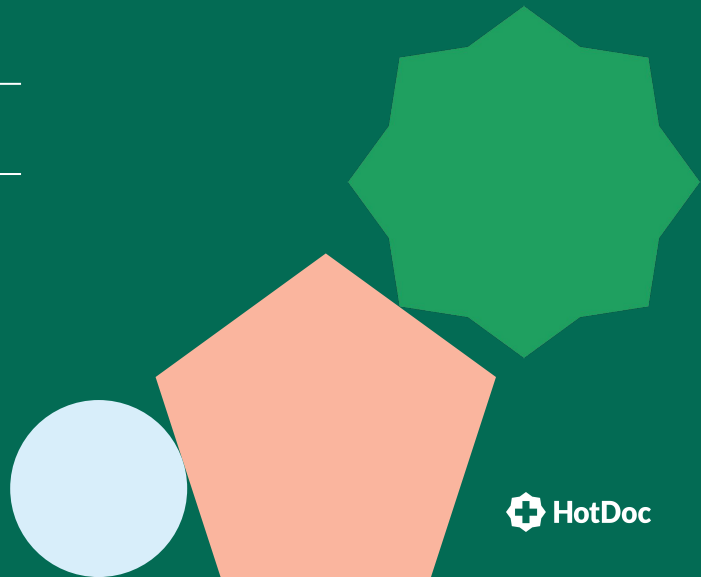
- 15 years of Cyber Security and Privacy Experience, from banks and Telecommunications companies down to small businesses
- Not a doctor, nor any medical training (beyond Level 4 first aid)
- Passionate about HotDoc's mission to enable the best healthcare experience for everyone in Australia, including allying with practices to increase trust

After today's presentation, I hope that you will

- Have some more information about the state of security and privacy in Healthcare, and
- Feel more confident managing security in your practice

Today's Agenda

1	Threats to Security & Privacy in Healthcare
2	Importance of Security to your Practice
3	Diagnosis & Risk Identification
4	A bunch of analogies
5	How to embed Security into your practice



HotDoc

Today I’m going to try and talk about Cyber and Privacy Risk like Clinical Risk

Essentially I’m trying to make security and privacy risk more accessible to practices.
I get good reviews, but I am not a doctor.
Please challenge me if the analogy is wrong or if you have other questions.

The first analogy to think about is that **cyber threats** are like **communicable diseases**.

Modern transport has increased the speed with which **diseases** can travel. This makes it harder to build immunity, and increases the diversity we are **exposed** to

Similarly, the internet has increased the speed with which **malicious actors** can access your practice too.

One could say that small businesses have a lower natural immunity and can't mobilise to defend against these threats

And this is backed up by the data.

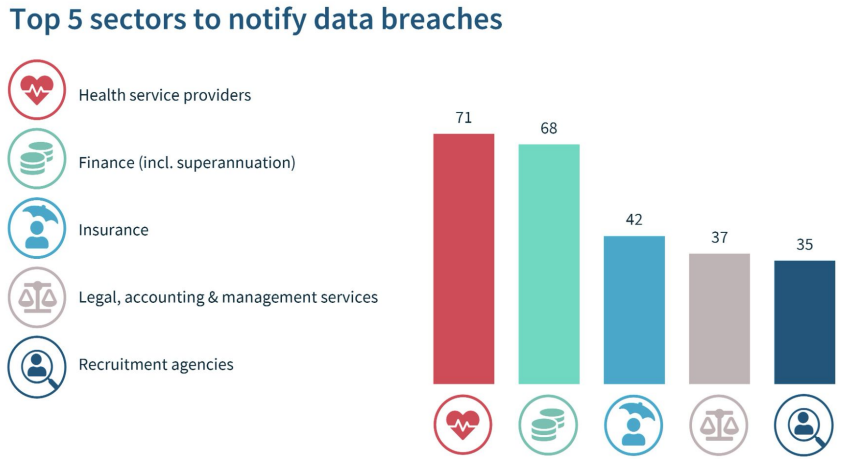
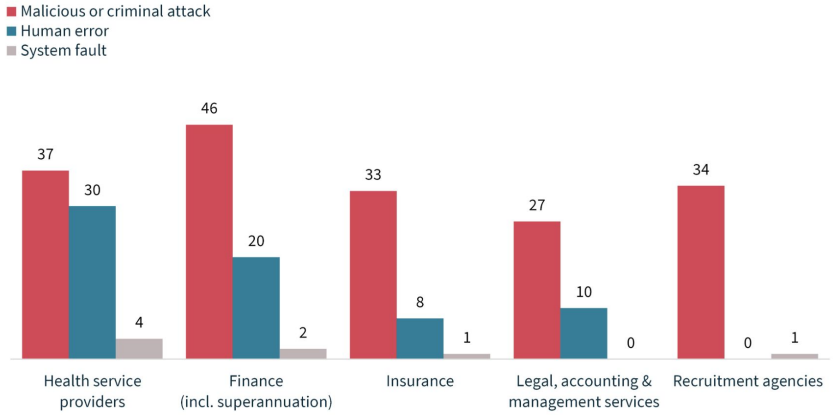


Chart 16 – Source of data breach notifications – top industry sectors

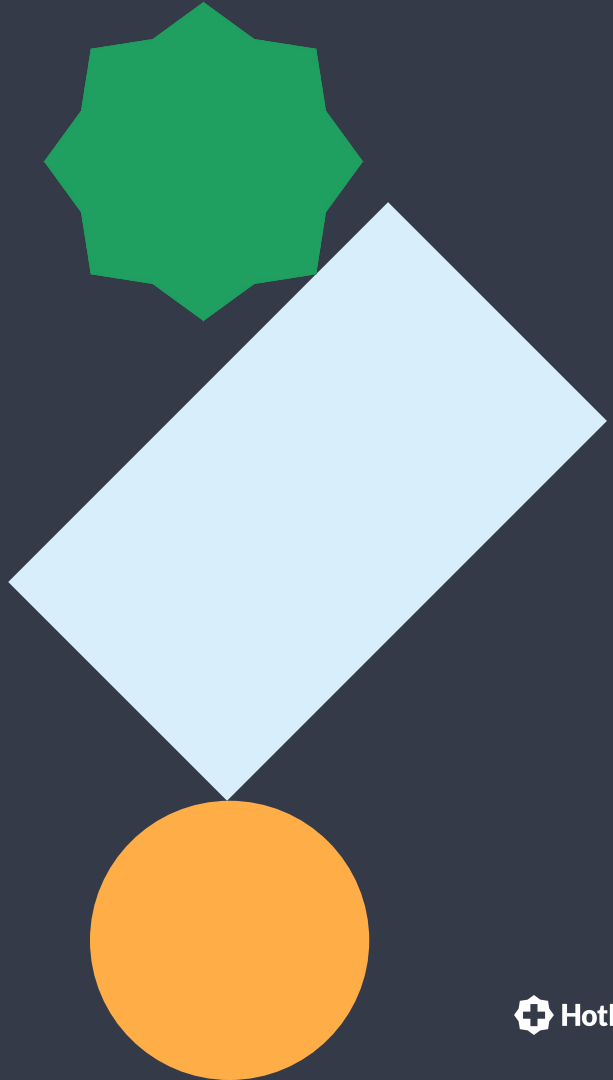


HotDoc

Let’s do a quick

~~risk assessment~~

Check up



HotDoc

How **‘fit’** are you, and ready to **resist a ‘communicable disease’?**

- Do you practice good **hygiene**?
- What’s your **immunity**?
- Do you **exercise** every day?
- Have you been **vaccinated**?
- Have you got a **good healthcare provider**?

You can do the same kind of assessment in the context of **“Cyber Defenses”?**

- Do you **patch** your systems?
- **Who** has **access** to your data?
- Have you got a **backup**?
- Have you **practiced** what you would do if you were compromised?
- Who do you **lean on** to help you with cyber?

HotDoc

If you were to get ‘sick,’ what would the short-term and long-term symptoms be?

In cyber, it could be:

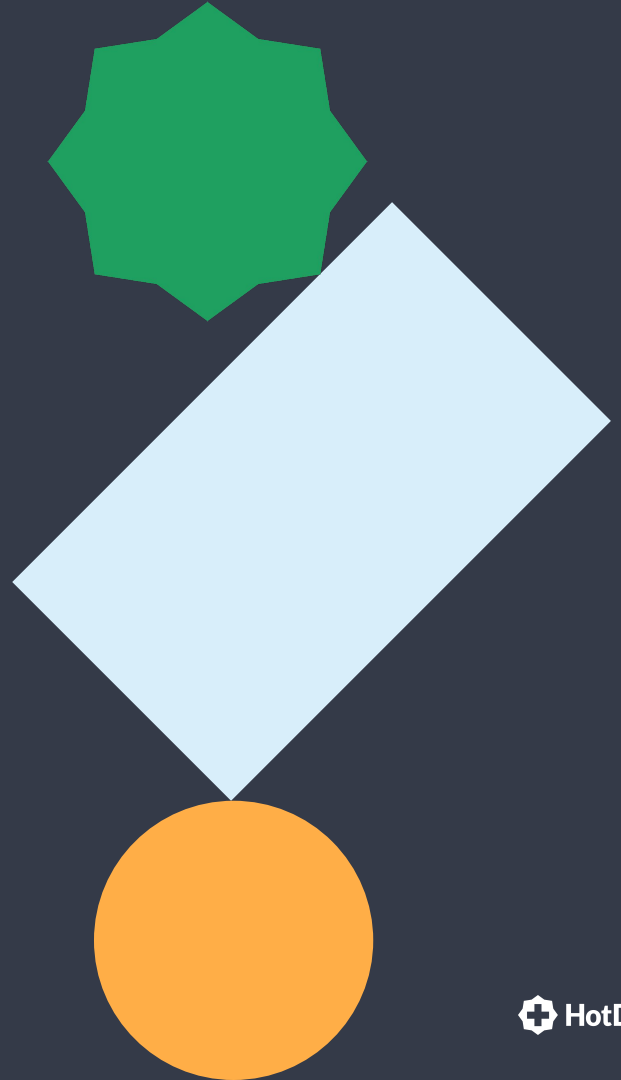
- Privacy Act Fines?
- Insurance Premium Increases?
- Brand Damage?
- Unable to operate?

HotDoc

Are you scared?
Don’t be!

Managing **Cyber risk** is like managing **Clinical risk** - there is an appropriate amount of mitigation, we just have to follow a process to be confident we have it right.

Some ideas....



Your IT systems and data are the **heart** of a modern practice. Ransomware or failures can **stop** it.

Think about:

- How long can you be without a heartbeat?
- What happens if you can't get on bypass or there's no defibrillator nearby?

What you can do:

- Keep fit
- Protect your heart
- Ask your IT provider
- Have a plan

RACGP: Information Backup

HotDoc

The **vendors** and **suppliers** you pick will be critical to your health or your security.

Think about:

- How do you decide to **trust** a Specialist you refer to?
- What could go wrong if I pick the wrong person?

What you can do:

- Ask questions
- Ask for referrals
- Ask for accreditations
- Monitor and govern

HotDoc

Hygiene and keeping your environment clean is key. Lock down all the ways something nasty can take root.

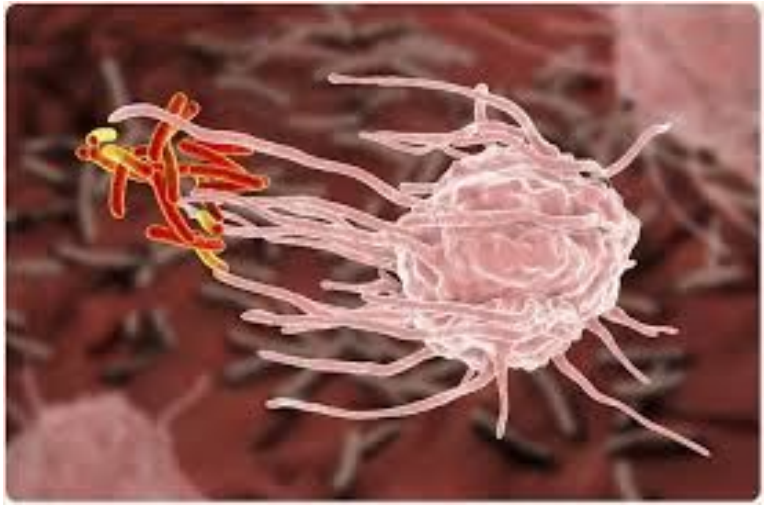
Think about:

- How do I make this normal?
- What could go wrong if I don't do this hygiene?

What you can do:

- Patching
- Good training
- Hard to skip
- Monitor and govern

ASD Ess.8: Application Control, Patching
RACGP: Securing your tech and network



Immune Response is all about identifying and responding to bad things once they get in.

Think about:

- How can I identify bad?
- How do I stop it from spreading?

What you can do:

- Physical Barriers/Auth
- Detection and response to bad things being present
- identifying individuals (not sharing accounts)

RACGP: Authentication

HotDoc

Patient Consent is not just about to treatment, but also about what you do with their data.

Think about:

- Does the patient know what I'm going to do?
- Would they be surprised by the outcome?

What you can do:

- Privacy Policy
- Summarise so it's easy to access and understand
- consistency

RACGP: Privacy
OAIC

HotDoc

NOW a warning?!

Doing a once-off security and privacy risk assessment is not enough!

The answer:

Check-ups

and

fitness

and

vigilance

You could…

Schedule

- a regular reminder to review your risks
  - Individually
  - With the ‘control owners’
- tests of your security posture
  - A call from a patient who thinks your clinic has lost data
  - An ‘outage’ of a key system

Incorporate it into your normal processes, like

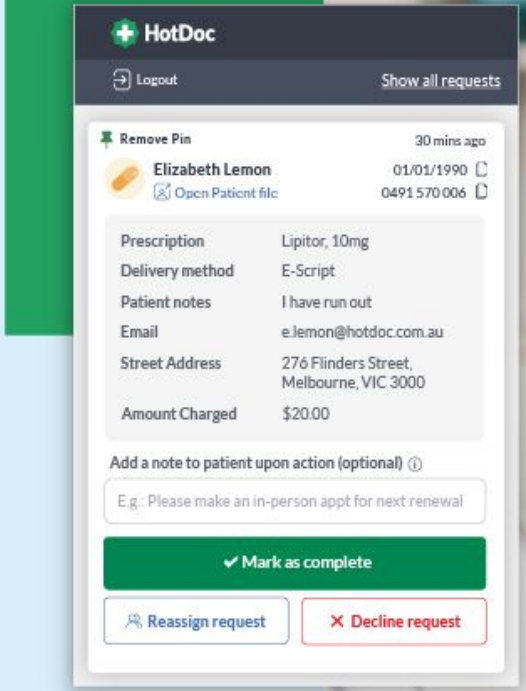
- ‘account discussions’ with your 3rd party providers
- Onboarding and offboarding staff

Quick Consults

Online healthcare from your regular doctor

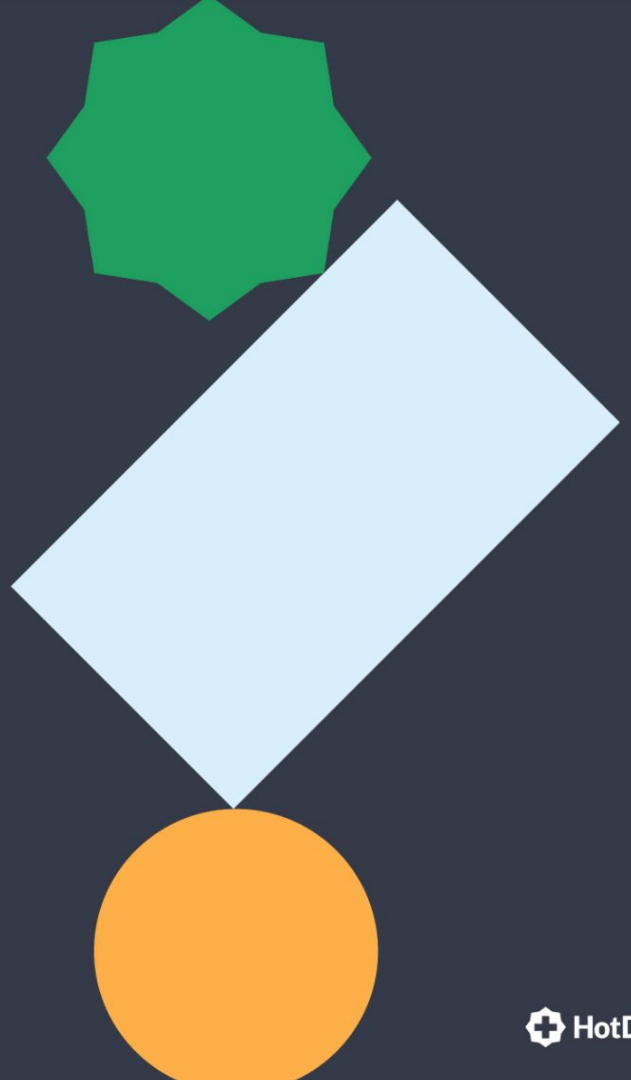
- Safe online care
- Increase earnings
- Flexible schedule

HotDoc



Book a Demo

Questions



Thanks for watching

Contact Us
info@hotdoc.com.au