

A person is shown from the side, wearing a dark suit jacket and a light-colored shirt, using a silver laptop. Their hands are on the keyboard. The background is a blurred office setting with a plant. Overlaid on the image are several glowing white icons: a padlock, a brain with circuitry, speech bubbles, a globe, gears, and two human figures. These icons are connected by thin white lines, suggesting a network or data flow.

# Cybersecurity, Informed Consent, Privacy & my health app

Peter Mullen – Digital Health Officer

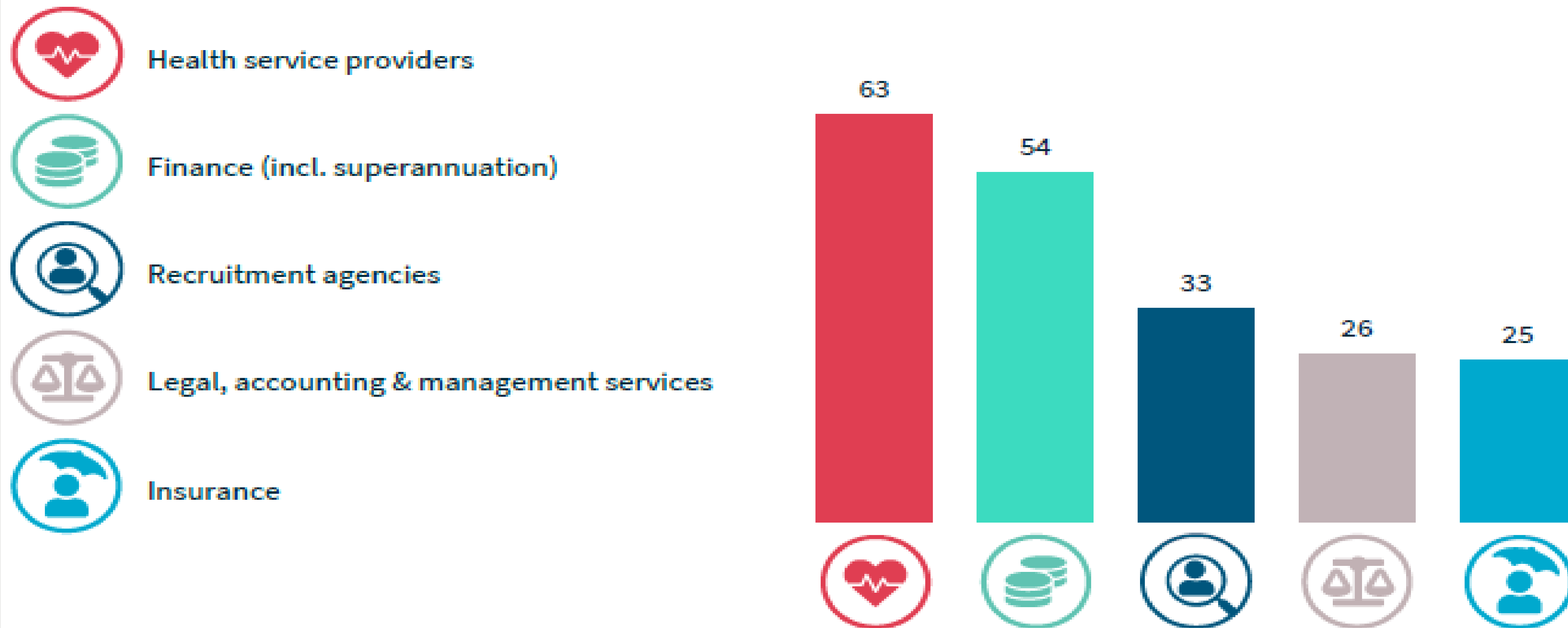
## CYBERSECURITY & DATA SECURITY

### Data Security – Is your data secure?

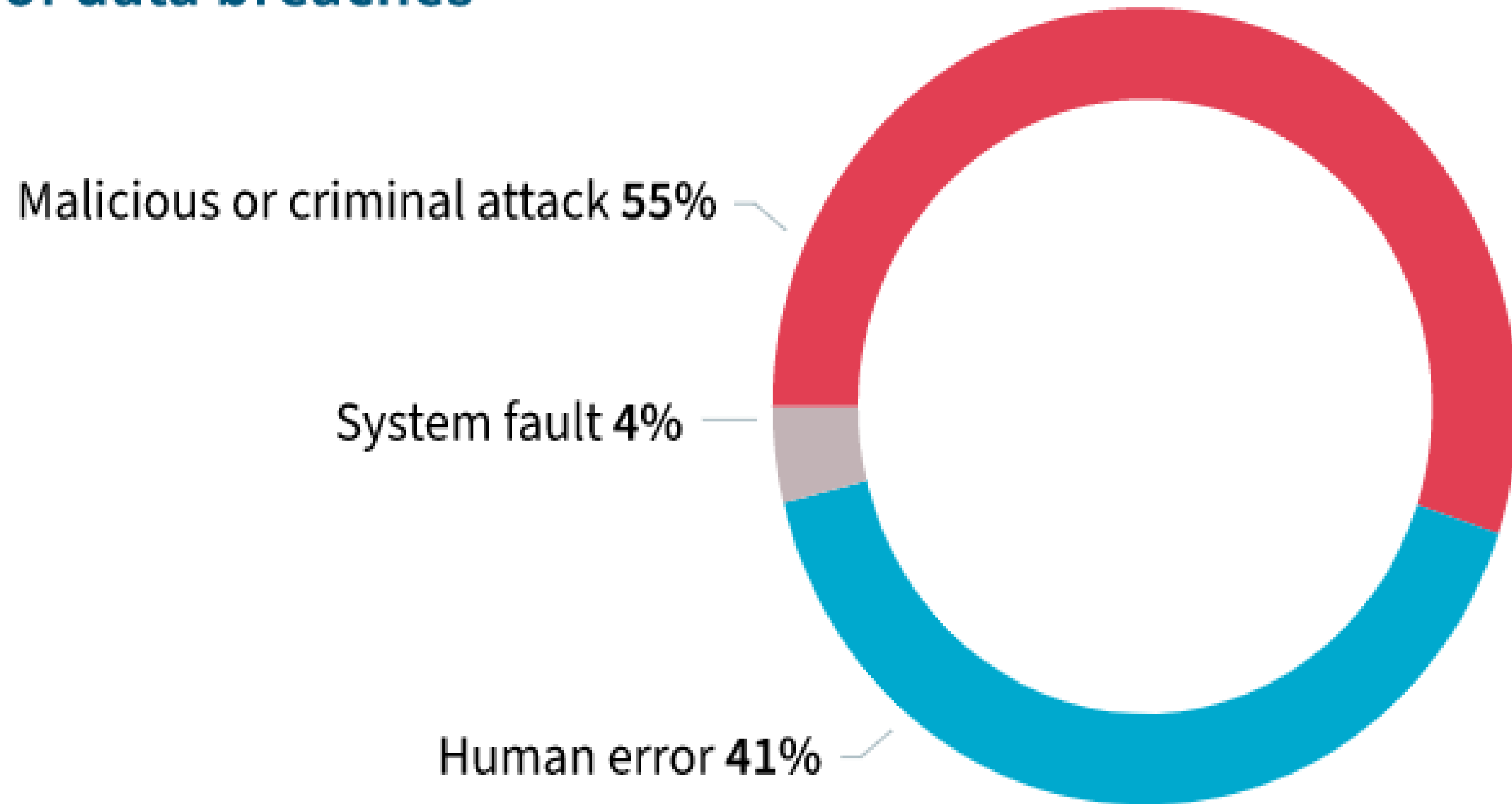
Who is the threat and why health industry data?



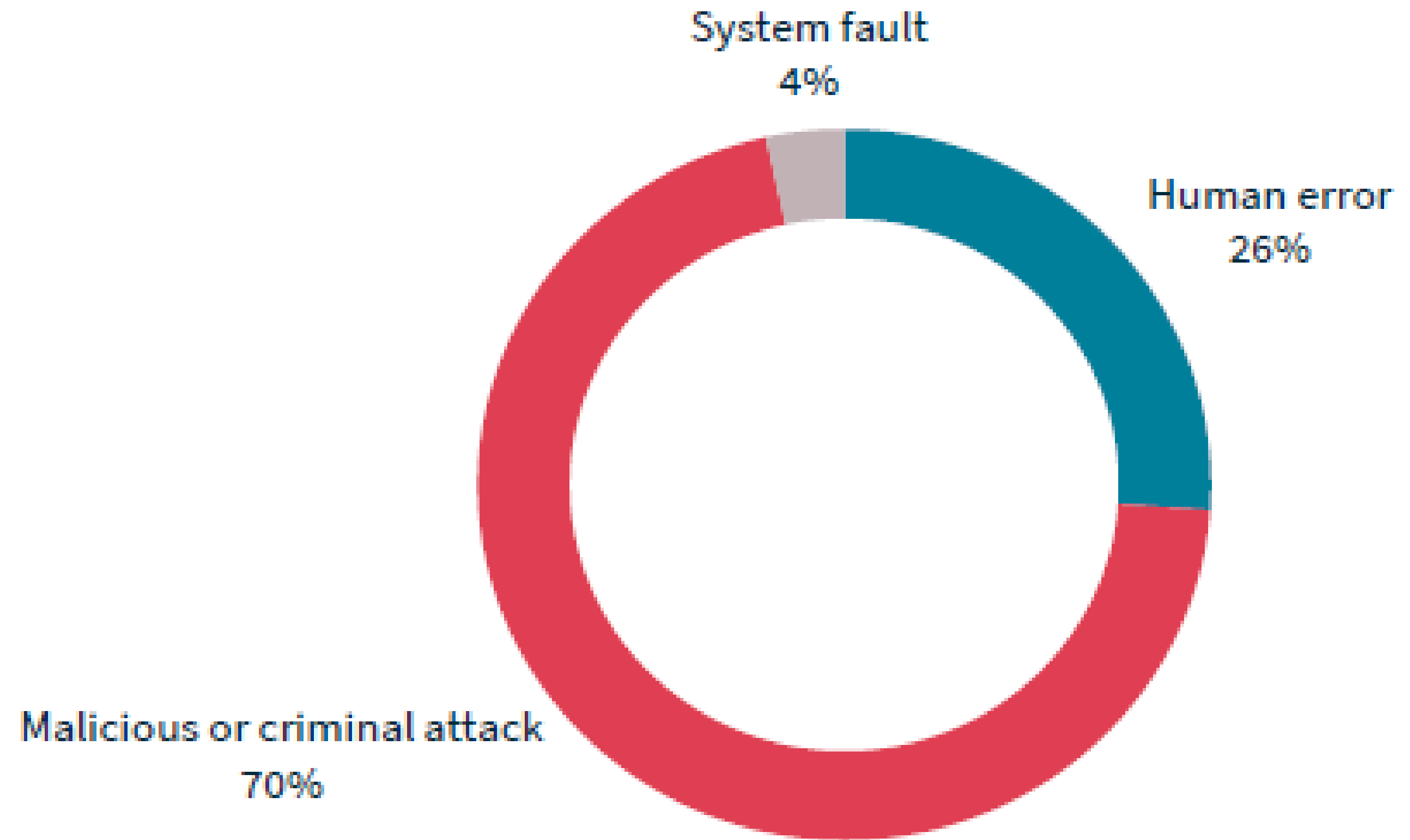
## Top 5 sectors to notify data breaches



## Sources of data breaches



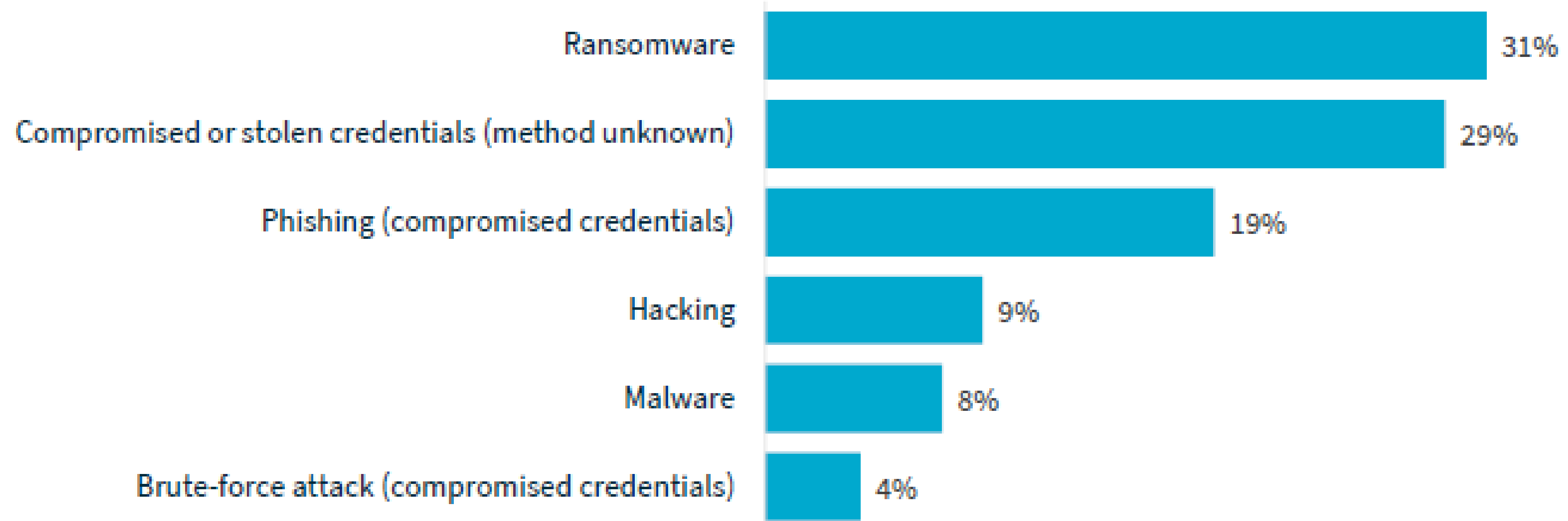
## Sources of data breaches



## CYBERSECURITY & DATA SECURITY

**42% of all data breaches resulted from cyber security incidents  
(172 notifications)**

Cyber incident breakdown



# CYBERSECURITY & DATA SECURITY

## Data Security – Is your data secure?

Common cyber threats

### #1 Compromised Credential Attacks

- Phishing
- Malware
- Brute Force Attack
- Compromised or stolen credentials

Mitigated by

- Staff training
- Web filtering
- Email filtering
- Strong password policies
- Multi factor authentication
- Business continuity and disaster recovery plan



**+ HELP NET SECURITY**

## TOP 10 MOST COMMON PASSWORDS IN 2022

Rank	Password	Time to crack it
1	password	< 1 Second
2	123456	< 1 Second
3	123456789	< 1 Second
4	guest	10 Seconds
5	qwerty	< 1 Second
6	12345678	< 1 Second
7	111111	< 1 Second
8	12345	< 1 Second
9	col123456	11 Seconds
10	123123	< 1 Second

SOURCE:  NordPass®



# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



> Learn how we made this table at [hivesystems.io/password](https://hivesystems.io/password)

## CYBERSECURITY & DATA SECURITY

### Passphrase Security – Is your data secure?

#### 2022

- HnEcCpHn (8 Characters – 22 Minutes)
- Gr33nFr0g\$\$ (11 characters – 400 yrs)
- T3rr!b!eCoFF33 (14 characters – 200m yrs)
- Be5Tpresent@tionevR (19 characters – 7qd yrs+)

#### 2023

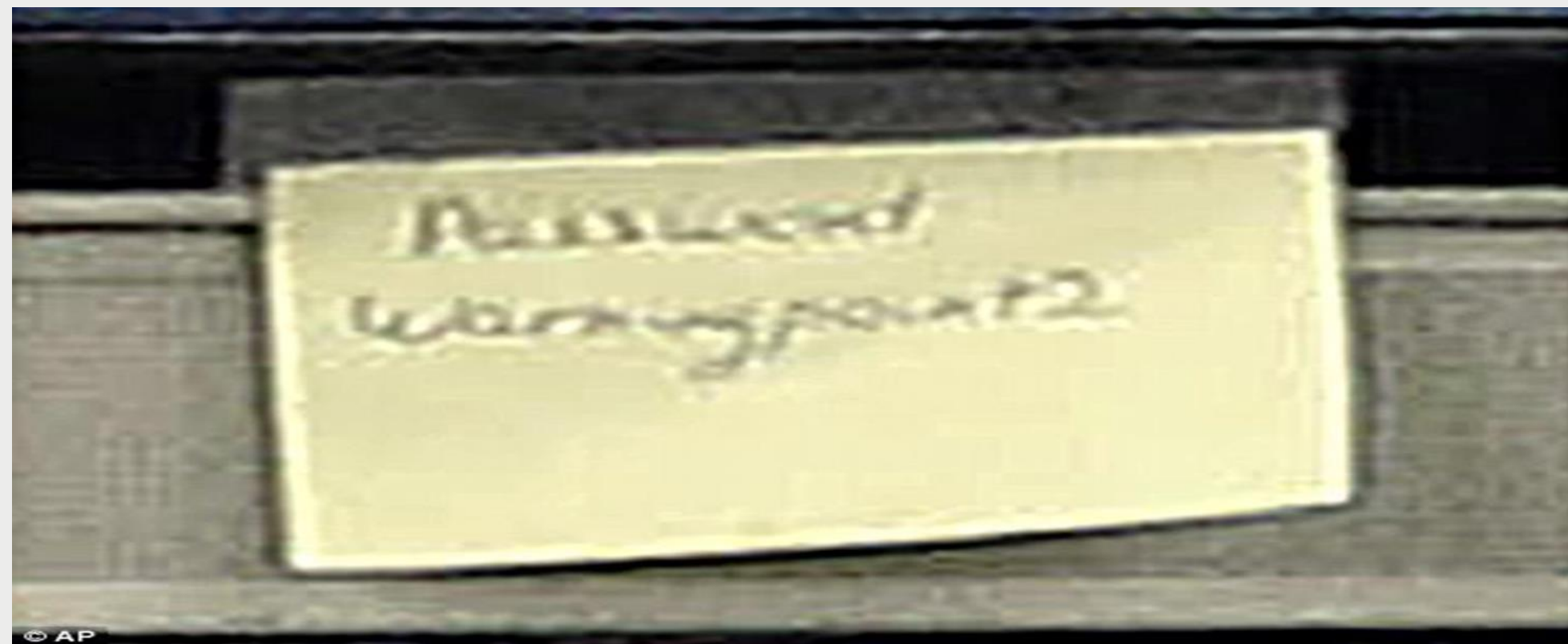
- HnEcCpHn (8 Characters – 28 Seconds)
- Gr33nFr0g\$\$ (11 characters – 3 years)
- T3rr!b!eCoFF33 (14 characters – 1m yrs)
- Be5Tpresent@tionevR (19 characters – 26tn yrs+)

# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



› Learn how we made this table at [hivesystems.io/password](https://hivesystems.io/password)



# CYBERSECURITY & DATA SECURITY

## Data Security – Is your data secure?

### #2 Ransomware

Ransomware is a type of malware designed to prevent or limit access to a user's system by locking the screen or files until a ransom is paid.

#### Mitigated by

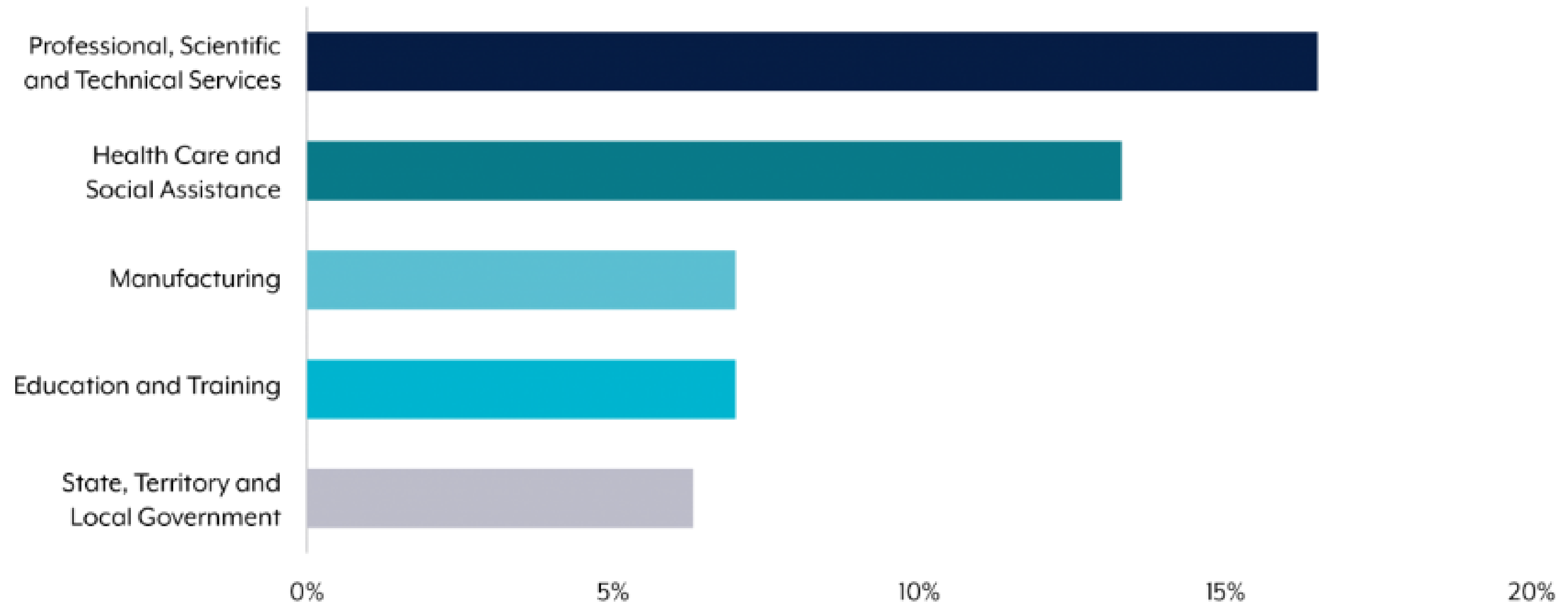
- Staff training
- Web filtering
- Email filtering
- Application whitelisting
- Business continuity and disaster recovery plan



Image Source: Adobe Stock

## CYBERSECURITY & DATA SECURITY

Figure 8: Top five reporting sectors for ransomware-related cyber security incidents





# Secure Remote Desktop Protocol



## Password protection

Require a password to use RDP

## Behind VPN

Require VPN to use RDP

## Multi-factor authentication

Secure VPN, RDP, and associated email addresses with MFA

## Limit login attempts

Cap the number of login attempts via RDP

## CYBERSECURITY & DATA SECURITY

### User permissions

- Do they allow staff to work effectively within their job scope?
- Who requires administrator level access & who doesn't?

### Software

- Keep all software up to date and running on the latest version.
- Don't unduly delay software upgrades (CMS/OS/BIOS/Drivers).

### Backups

- Are they done daily and stored offsite?
- Cloud storage vs Physical Drive.
- What is backed up?
- Secondary Server.
- Have you tested your data recovery from your backup?



Image Source: Adobe stock



Image Source: Adobe stock



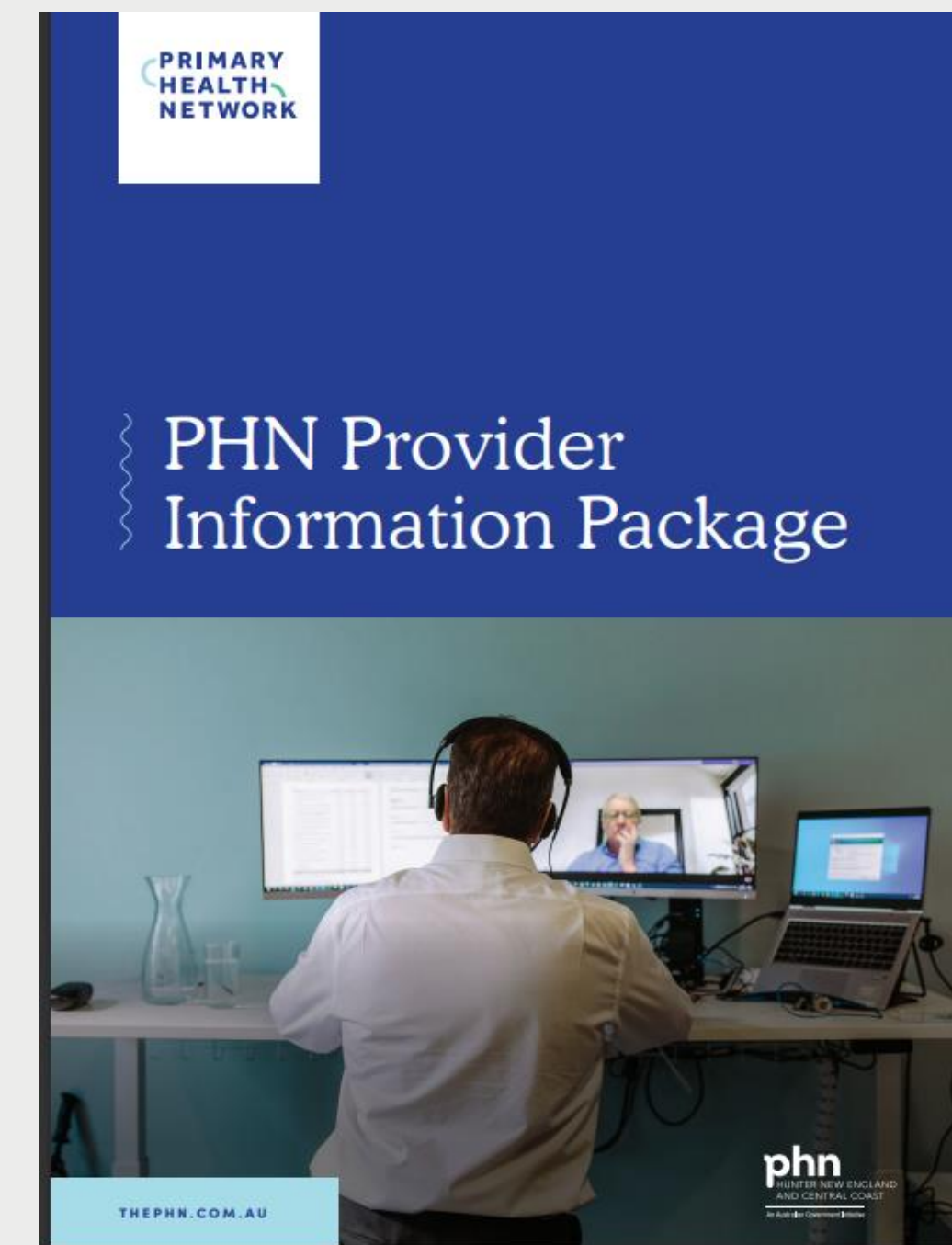
## CYBERSECURITY & DATA SECURITY

### Policies & Procedures

- Digital Health Access Policy (PHN Commissioned Service Providers)
- Privacy Policy/ My Health Record Security & Access/Secure Messaging/Social Media/Email & Internet/Data Records/Password Policy
- Does what you say you do in your Policies & Procedures Manuals match what you actually do day to day?

### IT Consultants/Suppliers

- Do you use an IT supplier or do you do it yourself?
- Do your IT consult with you or do the work and send an invoice?
- Do you or your manager know your IT administrator passwords?
- Does your IT Consultant work for you or do you work for them?



## CYBERSECURITY & DATA SECURITY

### Scenario 1:

#### Break in and theft of IT hardware (server &/or hardware) - On premise server and clinical management system

- Purpose of theft (Data theft/ransom/fraud)
- Prevention - Practice Security and IT storage (alarm system/monitored alarm system/key access/server storage (locked room with deadlock or under a desk).
- Password access – 40% of respondents in the GP HTDCS stored passwords on paper, in notebooks or a word document.
- SLA's with ITMSP – replacement IT hardware and/or operating environment time/data recovery time/what is backed up/where is the backup stored (is it password protected and/or encrypted)? Can ITMSP do what they say they can do? Has it been tested?
- What is the likely downtime and what would be the impact of that downtime? Business Interruption Insurance coverage?
- Who to advise Police/ITMSP/PHN/Insurance/Staff/OAIC.



Image Source: serverguys.com.au

## CYBERSECURITY & DATA SECURITY

### Scenario 2:

#### Break in and theft of IT hardware – Cloud based server and clinical management system

- Actual theft of IT equipment – Hardware
- Purpose of theft (Data theft/ransom/fraud)
- Prevention - Practice Security and IT storage (alarm system/monitored alarm system/key access)
- Password access – 40% of respondents in the GP HTDCS stored passwords on paper, in books or a word document
- SLA's with ITMSP – Replacement IT hardware time/data recovery time/what is backed up/where is the backup stored (is it password protected and/or encrypted). Can ITMSP do what they say they can do? Has it been tested?
- What is the likely downtime and what would be the impact of an that downtime? Business Interruption Insurance coverage?
- Who to advise Police/ITMSP/PHN/Insurance/Staff/OAIC.



Image source: Adobe Stock

## INFORMED CONSENT

“Importantly, consent is not just about getting a signature on a form, rather it is about a process of shared decision-making. As another colleague recently put it: “The thing we need to understand about informed consent is that it’s about the conversation, not the form. It’s not about a tick list to ensure you’ve disclosed every conceivable risk, it’s about understanding the patient and what is materially relevant to them and working through that with the patient.””

Source: [avant.org.au](http://avant.org.au)

### Consent needs to address three aspects:

- Capacity — who can give informed consent?
- Disclosure — what information do patients need?
- Voluntariness — are they giving consent freely?



# INFORMED CONSENT

## Capacity

Having decision-making capacity means that a patient can:

- understand the facts involved;
- understand the main choices;
- weigh up the consequences of the choices;
- understand how the consequences affect them; and
- communicate their decision.

## Disclosure

A clinician needs to discuss a procedure or proposed treatment and provide information in regard to any associated benefits and risks as they relate to the patient.

## Voluntariness

A patient must be free to make a decision in regard to a procedure or treatment without undue pressure or influence.



## INFORMED CONSENT & PRIVACY

### Children/Minors

When can a child or minor provide consent?

- The law presumes competence for capacity at age 18 and in South Australia age 16.
- However, before reaching 18 years of age (16 in SA) a child can be deemed a 'mature minor' which is referred to as Gillick Competent.
- When deciding if a child is Gillick competent a clinician should consider the child's age, the nature of the proposed treatment/procedure and their understanding of this including possible effects or side effects.

### Medicare

- At age 14 parents no longer have access to their child's Medicare claims history online.
- Children can have their own Medicare card at age 15.



## INFORMED CONSENT & PRIVACY

### My Health Record

- A parent or guardian will have control over a child's MHR until they turn 14. After that time a child who can prove to the ADHA that they are a mature minor can have control over their own MHR.
- At age 14 the child's parents and guardians are automatically removed from their MHR.
- Children can give access to their MHR to a parent or guardian.

### Clinicians and My Health Record

- Do you need a patient's consent to access their MHR?

### Patient control of their My Health Record

- What control does a patient have over their MHR?



# PRIVACY

## Legislation

Privacy Act 1988 was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than \$3 million, and some other organisations handle personal information.

The Privacy Act covers some small business operators (organisations with an annual turnover of \$3 million or less), including:

- a private sector health service provider — an organisation that provides a health service includes:
- a traditional health service provider, such as a private hospital, a day surgery, a medical practitioner, a pharmacist and an allied health professional
- a complementary therapist, such as a naturopath and a chiropractor
- a gym or weight loss clinic
- a child care centre, a private school and a private tertiary educational institution



## Privacy Act 1988

No. 119, 1988

### Compilation No. 96

**Compilation date:** 21 September 2023

**Includes amendments up to:** Act No. 73, 2023

**Registered:** 10 October 2023



# PRIVACY

## Privacy Policy

- Your Privacy Policy should outline how you collect, treat patient data and who has access to it.

## Right of access to information collected – Patient

- Patients have a right to their own health data or file under the privacy legislation.
- This includes reports from 3<sup>rd</sup> parties

## Right of access to information collected – 3<sup>rd</sup> Parties

- 3<sup>rd</sup> Parties have **no** right to anyone's data (including My Health Record) without a valid authority.
- 3<sup>rd</sup> Parties includes employers, insurance companies, law enforcement agencies, partners/spouses, children and parents (depending on the age of the child).
- Valid authority from a patient can be written or verbal.
- My Health Record does have a 'break glass' condition



*Privacy and managing  
health information in  
general practice*



## PRIVACY

### Right of access to information collected – 3<sup>rd</sup> Parties

- In NSW a Power of Attorney/Enduring Power of Attorney does not provide for access to health information.
- In NSW an Enduring Guardianship appointment only provides for access after the individual loses capacity.
- Access without consent can occur via subpoena, summons, when legislatively required or in certain emergency situations such as the 'Break Glass' feature in the MHR.



## PRIVACY

### Data Breaches

#### What are Notifiable breaches?

- A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and the OAIC when a data breach involving personal information is likely to result in serious harm.

#### What is the process to follow after a data breach

- [OAIC - Notifiable data breaches](#)
- [Data breach preparation and response](#)



Australian Government

Office of the Australian  
Information Commissioner

## Data breach preparation and response

A guide to managing data  
breaches in accordance with the  
Privacy Act 1988 (Cth)

oaic.gov.au

PRIMARY  
HEALTH  
NETWORK

my health app



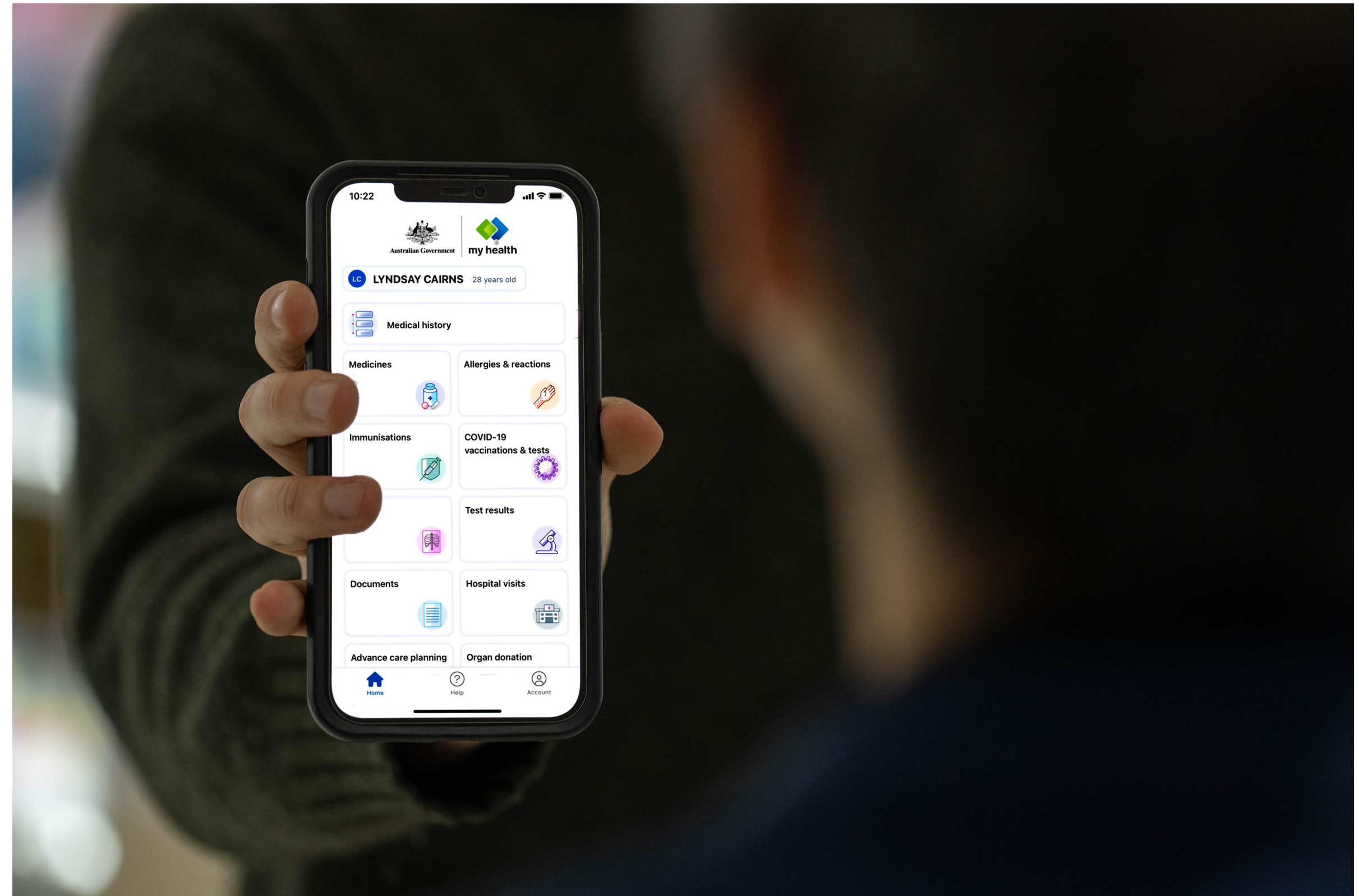
## WHAT IS THE MY HEALTH APP?

my health lets you view key health information that you, your healthcare providers or representatives have uploaded to My Health Record.

Before you can begin you'll need:

1. a myGov account already linked to My Health Record and
2. to have accessed My Health Record at least once through a web browser

To download the app search for “my health gov” in the Apple App Store or Google Play Store”. Once downloaded, follow the prompts and start exploring!

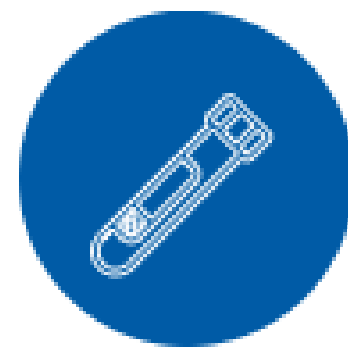


## WHAT INFORMATION IS AVAILABLE?

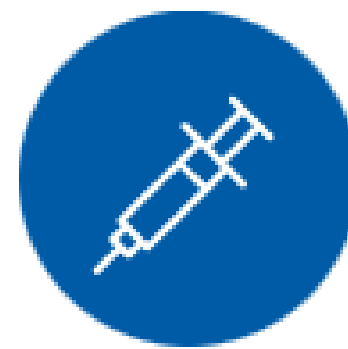
# Explore my health



View your  
medical history



Check pathology  
results, including  
Covid-19



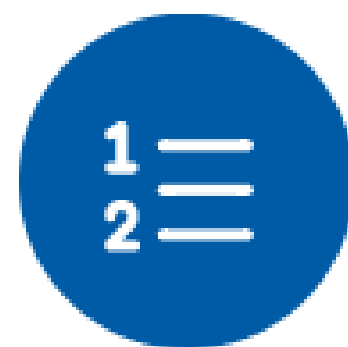
Manage  
vaccinations &  
immunisations



Track allergies &  
reactions



View hospital  
discharge  
summaries



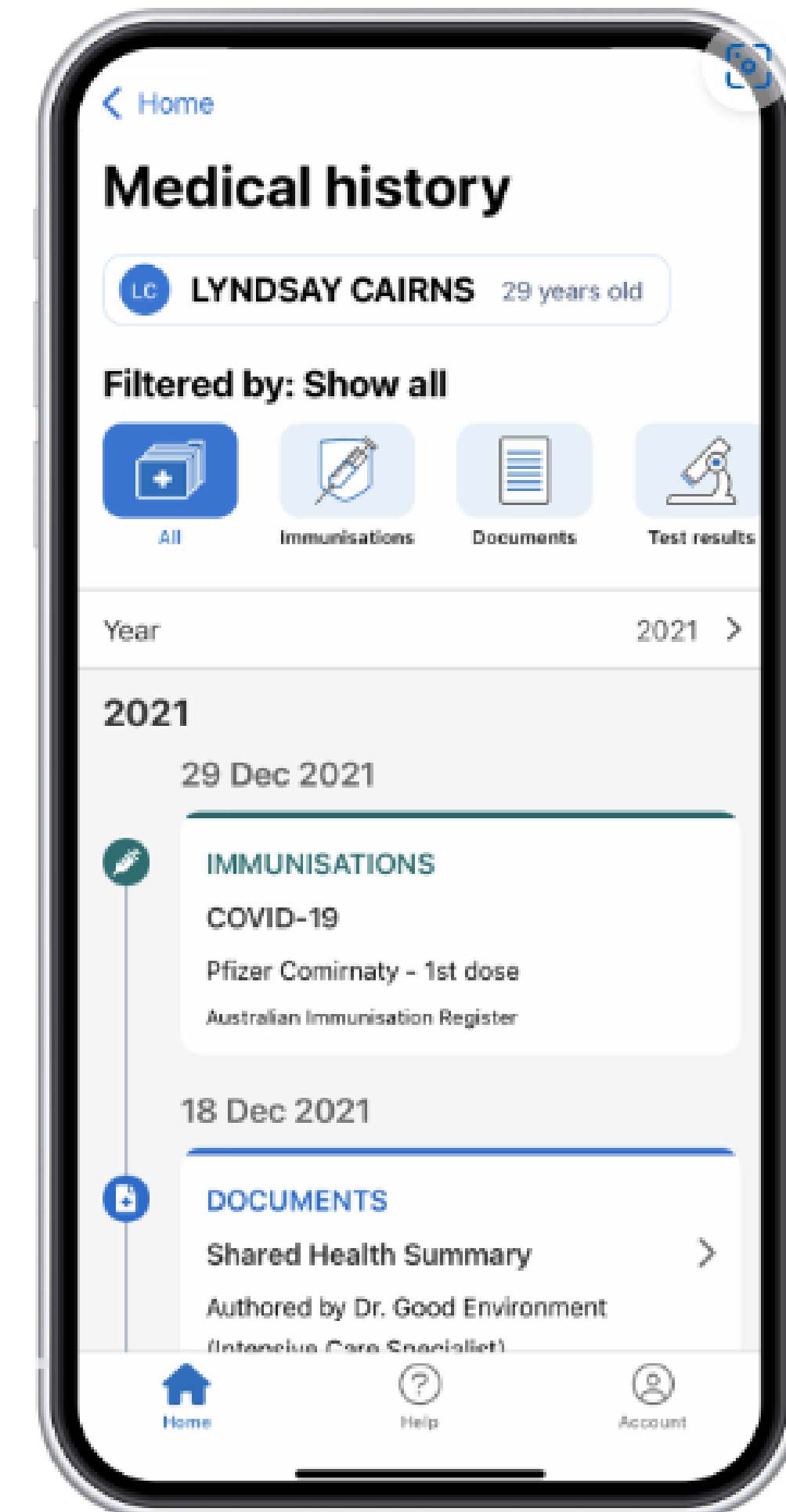
Keep track of  
care planning  
documents



View multiple  
records, yours &  
your family's



View medicine  
information



## IS MY INFORMATION SECURE?

my health has been built with your security in mind. Set up a secure 6-digit PIN in addition to your device's biometric security (e.g., fingerprint/Face ID). You can change your PIN in the account page of the app.

If you know or suspect your PIN has been compromised, or if you have any other concerns about the security of your my health app, you should change your PIN immediately.

my health will automatically log you out of the app if you haven't used it for 5 minutes.



## ACCESSIBILITY

The guidelines have three levels of accessibility (A, AA and AAA). The my health app aims to achieve level AA.

The Australian Digital Health Agency has a robust accessibility assurance process.

[Please visit the ADHA website to find out more.](#)

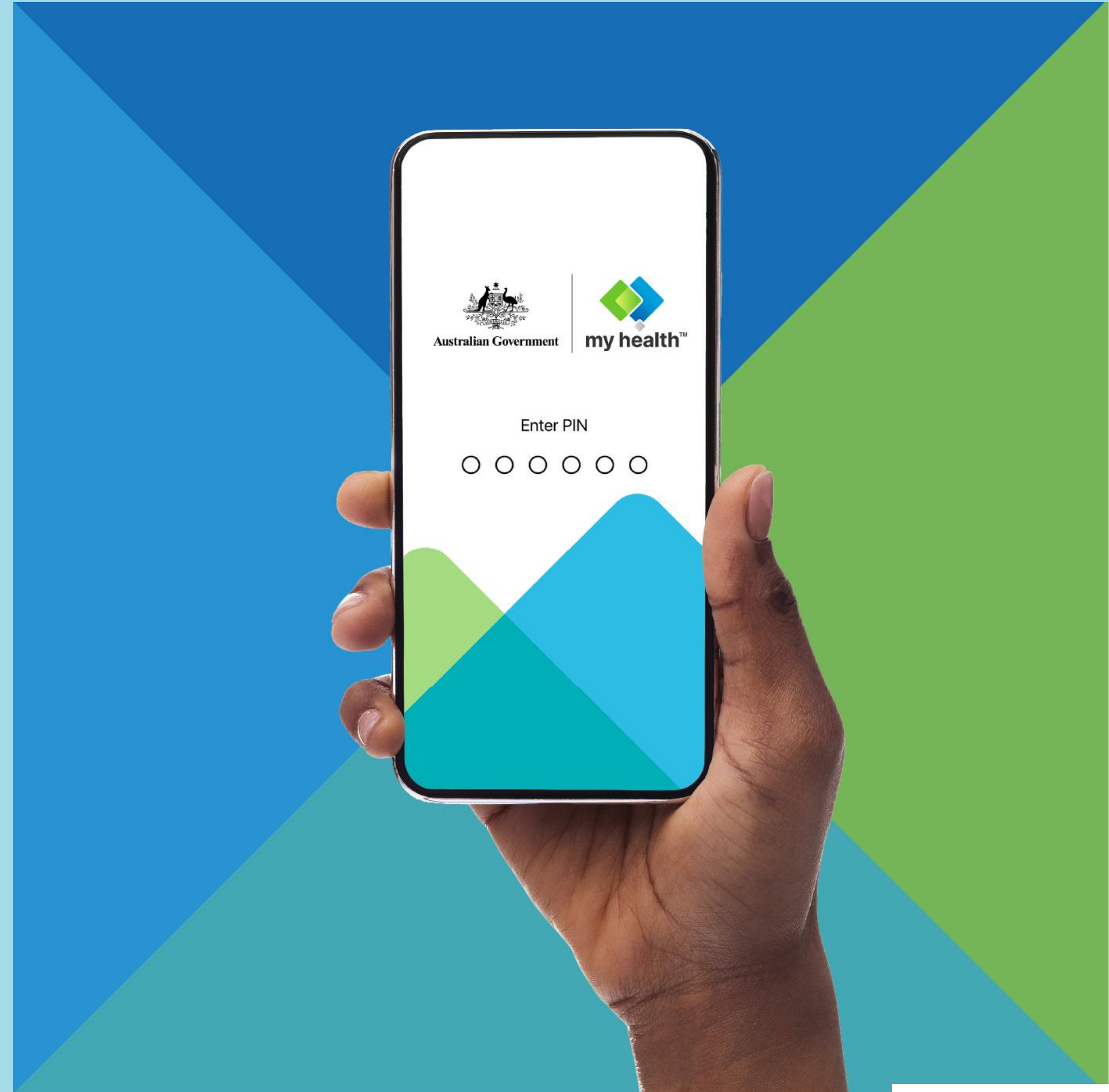
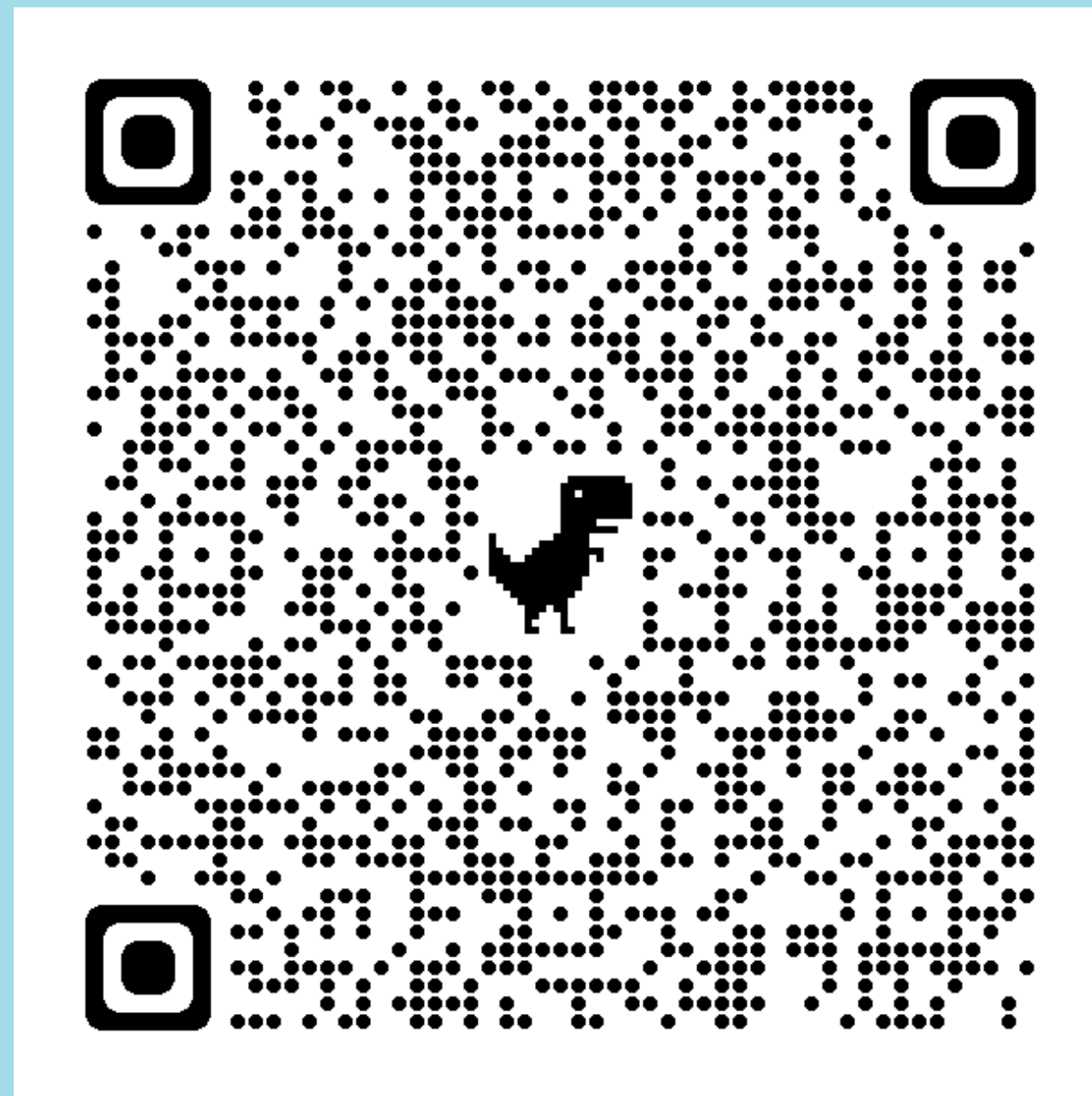




## ONLINE RESOURCES

[my health app – What is in my health app? – YouTube](#)

- <https://www.digitalhealth.gov.au/myhealth>
- Or use this QR code



## RESOURCES

### Australian Digital Health Agency

- <https://www.digitalhealth.gov.au/healthcare-providers>
- <https://www.digitalhealth.gov.au/healthcare-providers/training-and-support/cyber-security-training-and-support>
- <https://training.digitalhealth.gov.au/login/index.php>
- [Backups - Prepare for an emergency \(digitalhealth.gov.au\)](#)

### Australian Cyber Security Information Commissioner

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

### RACGP

<https://www.racgp.org.au/>

### Allied Health Professionals Australia

- <https://ahpa.com.au/>

### Avant

- <https://www.avant.org.au/>

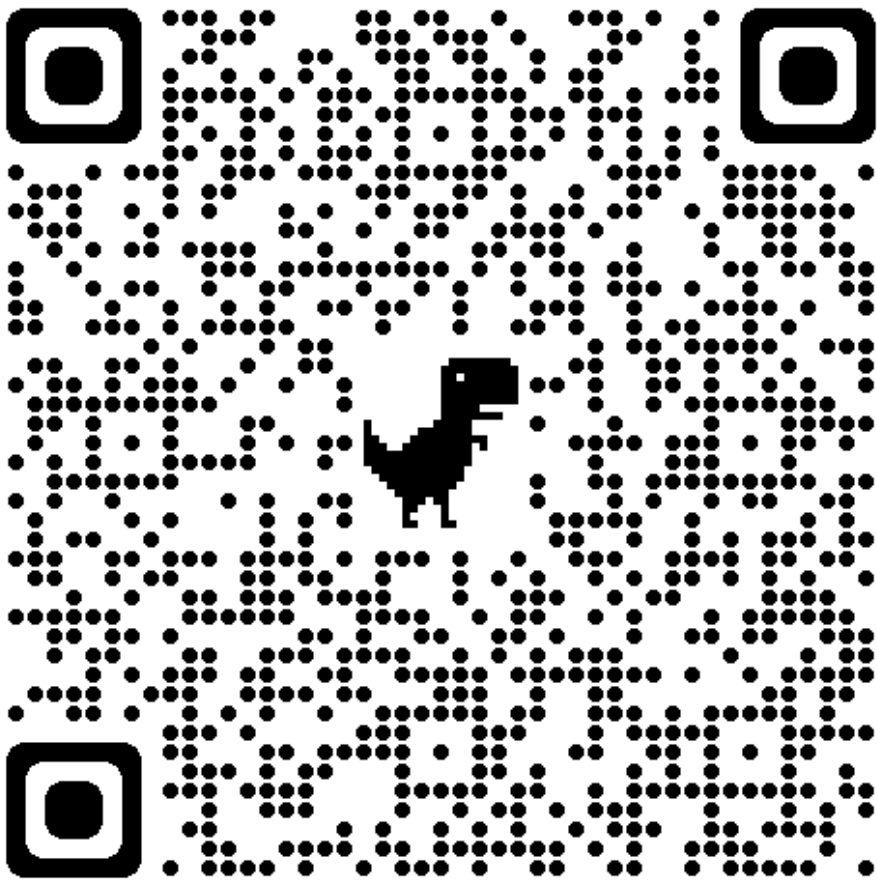
### Office of the Australian Information Commissioner

- <https://www.oaic.gov.au/>



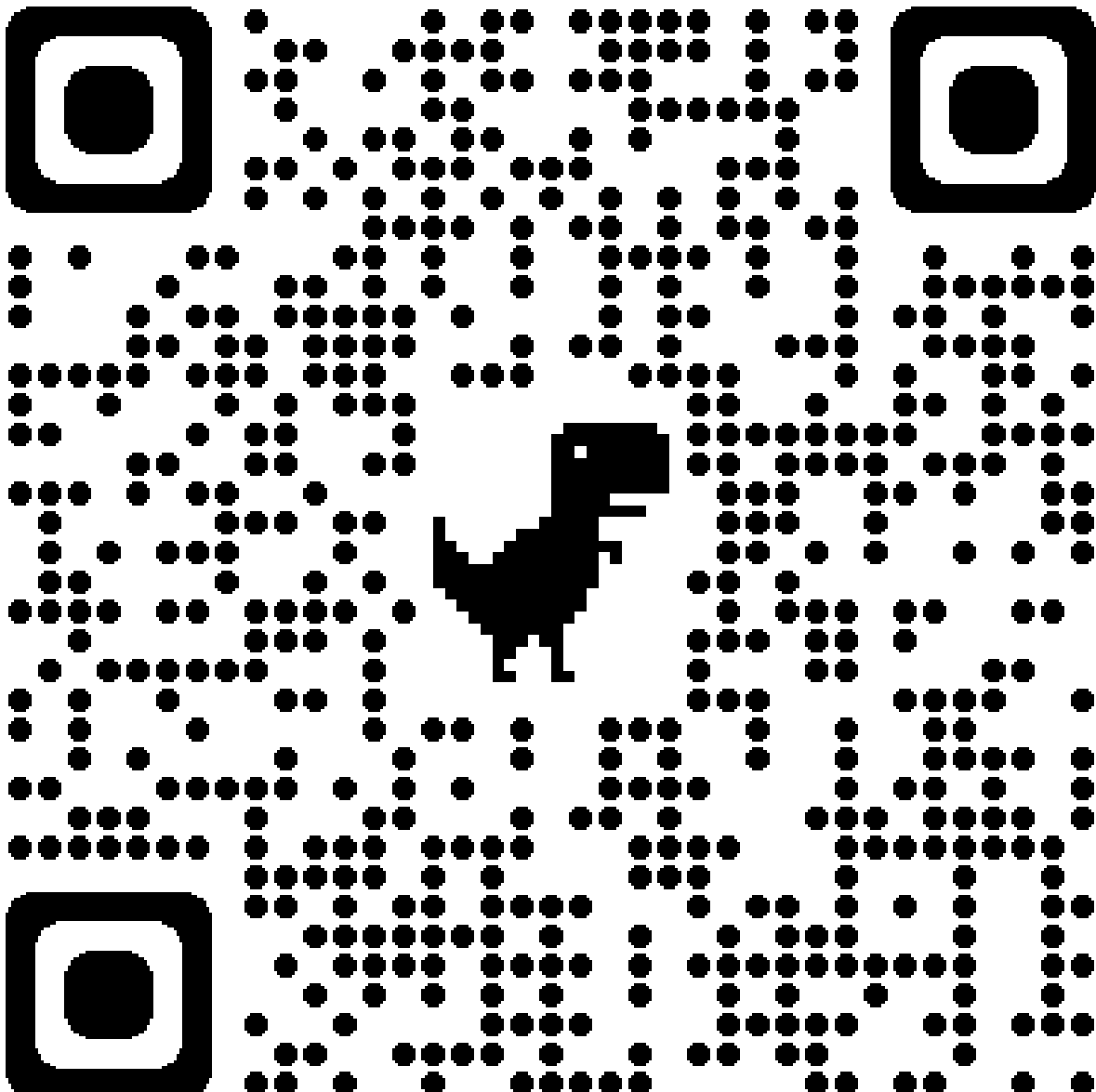
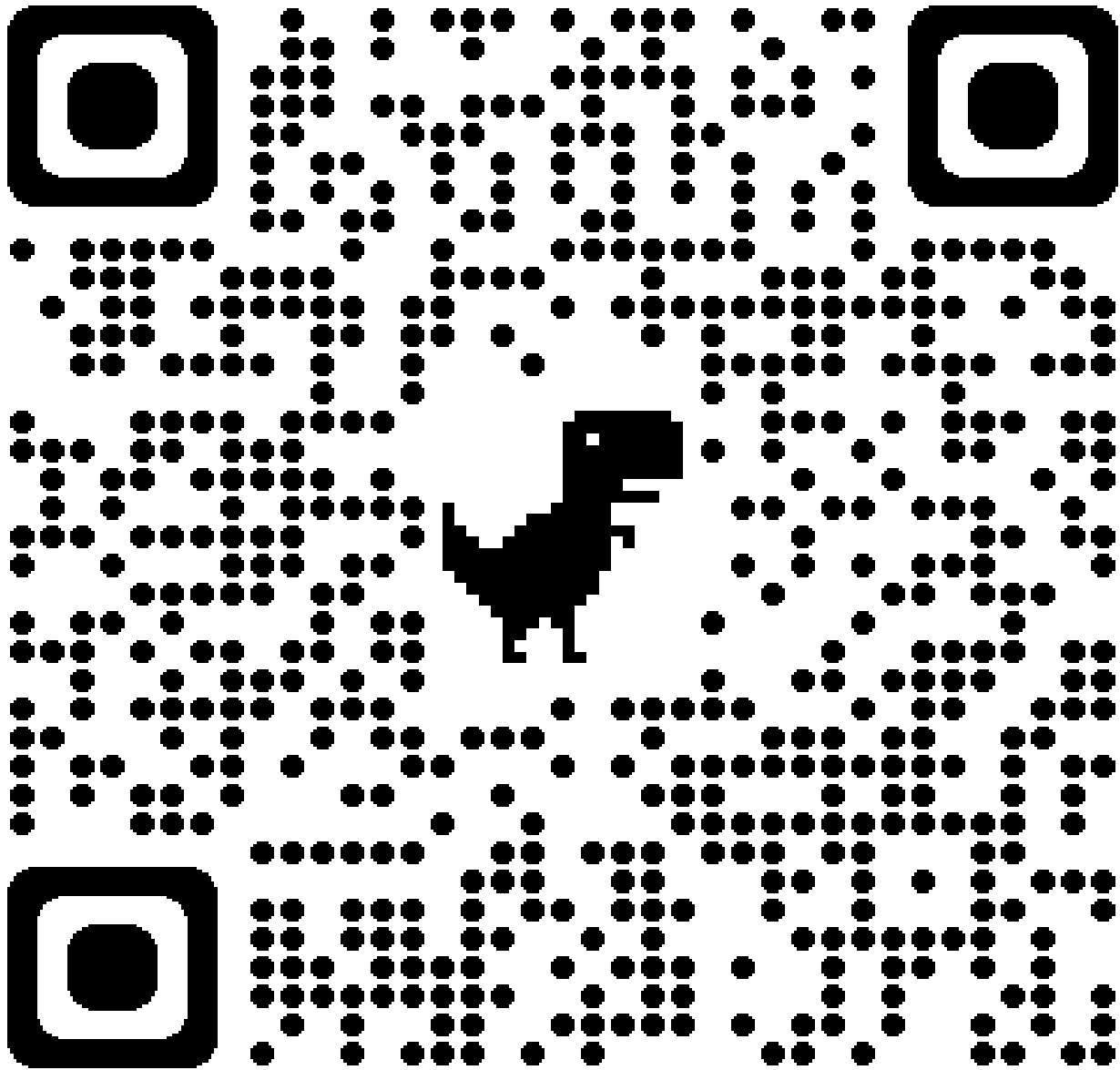
Image Source: Adobe Stock

RESOURCES



[Have I been pwned](#)

[See your identity pieced together from stolen data \(ABC\)](#)



[The PHN Digital Health Toolbox](#)

[The PHN Newsletter](#)

Q&A