

Data Breach Response

My plan if personal information is lost, accessed or shared without authority

I take the security of your information seriously. This plan sets out what I will do if a data breach happens, in line with the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth) and guidance from the Office of the Australian Information Commissioner (OAIC). It is mainly a working guide for me and is shared here so you know what to expect.

What is a data breach?

A data breach is when personal information is lost, accessed or shared without permission. Examples include a lost laptop or phone, an email sent to the wrong person, or a hacked account.

My four steps

1. **Contain, immediately.** Stop further access: change passwords, sign out of devices, recall or ask for deletion of a misdirected email, and contact the provider involved (Halaxy, Google or Zoom).
2. **Assess, as quickly as possible and within 30 days.** Work out what information was involved, who is affected, and whether the breach is likely to cause serious harm (physical, psychological, emotional, financial or reputational). Health information is sensitive, so I will treat any breach of it with great care.
3. **Notify, as soon as practicable.** If serious harm is likely, I will tell the people affected directly, in plain language, with practical steps they can take. I will also notify the OAIC using its online Notifiable Data Breach form.
4. **Review.** Work out what went wrong, fix it, and update my practices and this plan.

Records I keep

I keep a confidential register of every breach or suspected breach, including what happened, my assessment and the actions taken, even when notification was not required.

Prevention

- Encrypted, password-protected computer and phone, with two-factor authentication on all accounts.
- Client records kept in Halaxy, with minimal detail in email or Google Drive.
- Software kept up to date, and old records securely destroyed when they are no longer required.

Useful contacts

- Office of the Australian Information Commissioner: oaic.gov.au, 1300 363 992
- Australian Cyber Security Centre (report cybercrime): cyber.gov.au, 1300 292 371
- IDCARE (identity and cyber support, free): idcare.org, 1800 595 160
- ProRisk, my professional indemnity insurer: 1300 468 730, newclaims@prorisk.com.au
- PACFA, for professional guidance: (03) 9046 2270