HotDoc | CPD WEBINAR

Privacy: Key Obligations, How Medical Practices Can Comply & Preparing for Upcoming Reforms

HOSTED BY

Ella Cannon Partner

CIE Legal

CERTIFIED LEARNING PROVIDER cpd home AMA 2026

Thursday 27th August

12:30pm AEST

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.

HotDoc

Housekeeping

- This session is being recorded & will be sent to you 4-6 hours after this session has concluded along with the resources.
- Pre-submitted questions will be addressed at the end of today's session, we will do what we can to address additional questions submitted during the LIVE webinar
- In the "related content" you'll find our further feedback form.
- Your certificate of attendance will be accessible at the 40 min mark, you can access via the  certificate icon on your console.
- Have a play around with the console/ icons on your screen for an interactive experience.
- Please take some time to complete our feedback survey to let us know what you thought of today's session.

HotDoc

CIE Legal

Privacy: Key Obligations, How Medical Practices Can Comply & Preparing for Upcoming Reforms

Ella Cannon
Partner

Agenda

1. Setting the scene
2. Key privacy obligations
3. Recent and proposed privacy reforms
4. Common privacy risks in healthcare
5. Questions?

Setting the scene

Ella Cannon

Partner

Why privacy matters

- **Potential penalties**
  - Serious interference with privacy (tier 3) – up to $50M
  - Interference with privacy (tier 2) – up to $3.3M
  - Low-level breach (tier 1) – up to $330,000
- **Statutory claims**
  - Tort for serious invasion of privacy
  - Individuals can now bring direct action against a party for intrusions on their seclusion
- **Patient trust / satisfaction**
- **Avoiding complaints / reputational damage**
- **Professional obligations**

Australian privacy laws: current landscape

- **Federal**
  - Privacy Act 1988
  - My Health Records Act 2012
  - Healthcare Identifiers Act 2010
  - Consumer Data Right

- **State/Territory:**
  - Privacy laws or principles that apply to State/Territory public sector
  - Health records legislation in NSW, Vic and the ACT that also extends to the private sector

- **Broad conceptual alignment, with jurisdictional-specific nuances**

Australian privacy laws: proposed reforms

CIE Legal

- **Privacy Act Review Report 2023:**
  - 116 specific recommendations for reform
  - Proposed material change, aligned conceptually with the GDPR and other foreign equivalents

- **Government Response:**
  - Agreed to 38 reforms; Agreed in principle to 68 reforms
  - Noted 10 reforms

- **Tranche 1 reforms (POLA, 2024)**
  - Implemented 23 of the original proposals
  - Created statutory tort, increased penalties and regulatory powers, mandated Children's Online Privacy Code, includes mechanisms to enable future change

- **Expectation:**
  - Tranche 2 reforms to be released….?
  - No State/Territory equivalent current, but similar change in future

Key obligations

Ella Cannon

Partner

Defining our terms

- **Personal information**
  - Regulated by the Privacy Act.
  - Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not, and whether recorded in material form or not.

- **De-identified information**
  - No longer identifiable, and not reasonably capable of re-identification.
  - Not regulated by privacy laws.

- **Health information / Sensitive information**
  - Regulated by the Privacy Act and State/Territory health records legislation.
  - Definition varies between jurisdictions, but generally:

  Health information is any information or opinion, whether recorded or not, that:

    - identifies an individual or could reasonably identify them, and
    - relates to their physical or mental health, disability, the health services they have received or will receive, or **other information collected in providing or managing healthcare;** or
    - Is otherwise intrinsically connected to their health (such as genetic information, or their wishes regarding future health services).

Privacy Policy

CIE Legal

You must have and make available a Privacy Policy, setting out:

- your name and contact details;
- the kinds of personal information you collect (and how you collect it)
- the purpose(s) of collection, use and disclosure
- how they can seek access or correction, or make a complaint (usually refer to Privacy Policy)
- any overseas recipients and if so, their locations
- a description of any automated decision-making [new obligation; awaiting guidance]

Collection

Collection of health information must be:

- **Reasonably necessary** for your functions and activities

- Collected in a way that is **lawful and fair** (not unreasonably intrusive)

- Collected either with the individual's **consent**, or if collection is:
  - required or authorised by law
  - *necessary to provide a health service* to the individual, and collected in accordance with rules of health/medical bodies that deal with professional confidentiality
  - information about a third party, which is *necessary to enable the family social, or medical history of a patient* to be collected
  - necessary to *lessen or prevent a serious threat to life, health* or safety (or public health or safety) and consent is impractical
  - required for law enforcement/investigations
  - necessary for *approved research, statistical analysis or public health purposes* if certain requirements are met (ethics approval, public interest considerations etc)
  - covered by another prescribed exception

Collection notifications

CIE Legal

You must take such steps (if any) as are reasonable in the circumstances, to notify individuals (or otherwise ensure they are notified) of certain matters, including:

- your name and contact details
- the fact that you have collected their personal information
- the purpose(s) of collection
- how the information will be used / disclosed (including the types of entities you usually disclose information to)
- how they can seek access or correction, or make a complaint (usually refer to Privacy Policy)
- any overseas recipients and if so, their locations

Use and disclosure

If personal information was collected for a particular purpose (*the **primary purpose***), you must not use or disclose the information for another purpose (***secondary purpose***), unless an exception applies...

Use and disclosure - exceptions

Exceptions permitting use or disclosure for a **secondary purpose** include where:

- the individual **consents** ; or
- the individual would **reasonably expect** such use/disclosure, and the secondary purpose is related to (or for health information, **directly related** to) the primary purpose; or
- another **specific exception** applies – such as:
    - necessary to lessen or prevent a serious threat to life, health or safety (or public health or safety) and consent is impractical
    - required for law enforcement/investigations (e.g. locating a missing person)
    - necessary for approved research, statistical analysis or public health purposes if certain requirements are met (ethics approval, public interest considerations etc)

Retention

State/Territory health records legislation requires health records to be retained:

- for 7 years from the *last date of service*; or
- in the case of a child, until that child turns 25.

If you sell, relocate or close down your practice (or die), notification and management obligations kick in, e.g.

- must give patients reasonable notice and information about access/transfer
- continue to securely manage until lawfully transferred to another practice or the retention period expires
- continue to comply with access and transfer requests

All other personal information must be destroyed or de-identified once it is no longer needed.

Access and correction

CIE Legal

Individuals have a right to access the personal and health information you hold about them

- Respond within required timeframes (30 days under the Privacy Act; sooner where State/Territory health records laws require)
- Verify identity, then give access in the form requested where reasonable. You can charge a reasonable fee, if preferred.
- Refuse only on limited grounds (e.g. serious threat to health, unlawful or privileged) and give written reasons

Individuals can seek correction of their information

- Correct information that is inaccurate, out-of-date, incomplete, irrelevant or misleading, and notify others you have shared it with
- If you decline, note the requested correction on the record and give written reasons

Practical guidance

- Keep a documented access and correction procedure aligned with both the Privacy Act (APPs 12 and 13) and applicable State/Territory health records Acts
- Where jurisdictions differ, apply the standard most protective of the individual

Security / Data breaches

- **Security obligation:** You must take reasonable steps to protect the personal information that you hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
  - Health information = expectation of more robust security

- Reasonable steps includes **technical and organisational measures** [new requirement], e.g.
  - **technical** : encryption; MFA; secure password policies/managers; role-based access controls; organization approved devices and platforms
  - **organisational** : review vendor security commitments; data mapping; training; data breach response plans; audits and compliance reviews

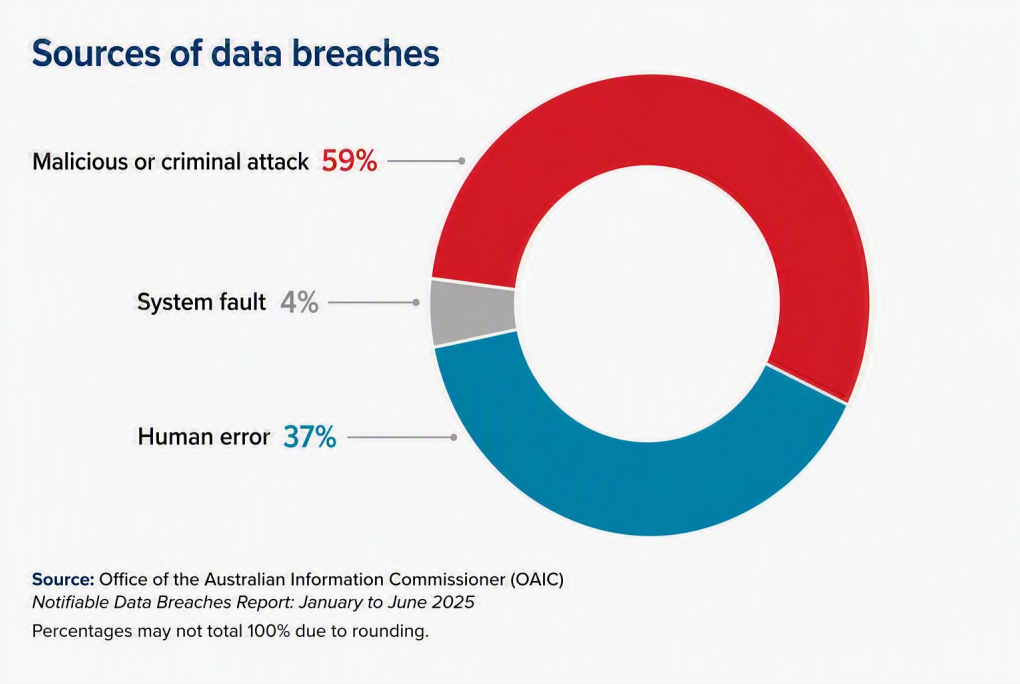
- **If a data breach occurs,** you must:
  - assess whether it constitutes an 'eligible data breach' within 30 days (at the latest); and
  - if an eligible data breach has occurred, make notifications to the OAIC and affected individuals.

Data breaches – lessons learned

CIE Legal

2025 saw the highest number of data breach notifications to the OAIC since the scheme commenced in 2018, the majority of which are caused by malicious or criminal attack

Cyber hacking remains the primary cause of data breaches reported to the OAIC. Of the 1,205 data breaches notified in 2025, the majority were attributable to malicious or criminal activity (716 notifications), with h[redacted], and accounting for 19% of the total or 225 notifications.



MHR and HI

CIE Legal

My Health Records Act 2012

- Register with the System Operator and meet participation, security and identity-verification requirements before using the system
- Opt-out: you may upload records to a patient's My Health Record unless they ask you not to (patients can opt out or set access controls)
- Access records only to provide healthcare; respect patient access controls and use "emergency access" only where permitted, recording why
- Maintain a written security and access policy, authorise and train staff, and notify the System Operator and OAIC of any breach

Healthcare Identifiers Act 2010

- Use Individual and Provider Healthcare Identifiers only for permitted purposes (identifying patients and communicating about their care)
- Match identifiers to the correct individual, keep them accurate, and protect them like other personal information

Reforms

Ella Cannon

Partner

Tranche 1 reforms

CIE Legal

Reform	Status
Updated Objects of the Privacy Act : reframed to recognise privacy as a public interest	✅ In effect
Enhanced OAIC Enforcement Powers : new search & seizure powers, compliance notices	
Tiered Civil Penalties & Infringement Notices : infringement notices up to $66,000 per contravention	
Security Uplift : "reasonable steps" clarified to include "technical and organisational measures"	
Emergency Declarations : enabling information sharing in declared emergencies	
Anti-Doxxing Criminal Offences : new offences for menacing exposure of personal data	
Streamlined Overseas Data Transfers : simplified mechanism (awaiting supporting regulations)	
Statutory Tort for Serious Invasions of Privacy : commenced on 10 June 2025; individuals can now sue directly	
Automated Decision-Making Transparency : from 10 December 2026, organisations using automated decision-making systems in particular ways will need to ensure their privacy policies reflect certain matters	⏳ Commences 10 Dec 2026
Children's Online Privacy Code : the Code will be in place by 10 December 2026	⏳ Due by 10 Dec 2026

Tranche 2 [No ETA]

To introduce a data controller v processor distinction:

- Data controllers:
  - The entity that determines **how** personal information is processed
  - More control = more direct compliance obligations

- Data Processors:
  - The entity that **processes** personal information on behalf of the Controller
  - Less control = less direct compliance obligations

Tranche 2 [No ETA]

- Stricter consent requirements
  - Improved quality of consent by requiring it to be voluntary, informed, current, specific and unambiguous
  - Express recognition of the ability to withdraw consent
- Expanded definition of personal information
  - Changing the word ‘about’ to ‘relates to’ – broadening scope
- Expanded individual rights [query if they will apply to health sector]
  - Right to erasure: right to erase relevant personal information held by an APP entity
  - Right to object: right to object to APP entities’ handling of relevant personal information

Tranche 2 [No ETA]

- Removal of small business exemption
- Restricting employee records exemption
- Minimum and maximum retention periods

Preparing for the reforms

- Data mapping – understand where your data is held / retention obligations / format
- Identify your data processors (PMS providers, HotDoc, AI tools?)
- Review, standardise and improve consent processes
- Prepare for more utilisation of individual rights
- Review or prepare retention and deletion frameworks
- Review and improve Privacy Policy and Collection Notices

Common privacy risks in health

Ella Cannon

Partner

Common risks (that you can fix!)

- **Privacy Policy out of date**

✔ Annual review and update

- **Inadequate consent provisions and collection notification for patient registration forms**

✔ Legal review and update

- **No process for dealing with access requests**

✔ Implement a policy and process

✔ Understand where health records are held

- **Lack of readiness for data breach**

✔Implement a policy (and template data breach report)

✔Know where to go for help

✔Ensure staff know how to escalate concerns

✔Check that basic security is applied (MFA where available, access controls, encryption)

- **No staff training or clear policies**

✔Regular staff training on Practice's privacy protocols

✔Phishing awareness

✔Implement a policy on data-handling generally

HotDoc | WEBINAR

Meet HotDoc's Document Assistant

Finally, A Reason To Enjoy Paperwork

HOSTED BY

Kiana Minkie

Product Marketer

Ruby Smith

Voice of Customer

Tues 1st Sep

12:30pm AEST

Questions?

Ella Cannon
Partner

+61 431 270 591

ecannon@cielegal.com.au

Thank You!

Medical Business Services

HotDoc