
2025 REFORMS
Privacy Compliance
For Practice Owners
Lazarus
LEGAL
consultmed

2025 REFORMS

Privacy compliance for Practice Owners

Before & after the 2025 Privacy Act reforms

Presented by:

LAZARUS LEGAL

consultmed

What is the Privacy Act
and why it applies to you?

The **Privacy Act 1988 (Cth)** sets national rules for how personal information must be handled.

From 2025, **all practices must comply**, regardless of size or revenue.

This includes:

- **How you collect and use patient information**
- **How you secure records**
- **How patients can access or correct their data**
- **What you must do if something goes wrong**

Your practice will soon be covered by the Act and expected to meet its standards.

LAZARUS LEGAL

consultmed

The APPs and the role of the OAIC

The **Australian Privacy Principles (APPs)** are the 13 core rules under the Privacy Act. They require you to:

- **Collect data only when necessary and with informed consent**
- **Secure all patient records**
- **Respond to access and correction requests**
- **Limit data sharing to lawful, documented cases**
- **Train staff and document your processes**

The **Office of the Australian Information Commissioner (OAIC)** enforces these rules.

The APPs and the role of the OAIC

The OAIC can:

- **Investigate your practice**
- **Handle patient complaints**
- **Issue fines up to $50 million for serious breaches**

If a breach occurs, the OAIC is the authority that will review your actions.

Under the 2025 reform proposals, all practices are expected to come under the Privacy Act for the first time, removing any current exemptions.

The 13 Australian Privacy Principles (APPs)

1. **Open & Transparent Management** – Entities must have an up-to-date Privacy Policy and manage personal info transparently.
2. **Anonymity & Pseudonymity** – Individuals must have the option to interact anonymously or via pseudonym, where lawful and practicable.
3. **Collection of Solicited Info** – Collect only necessary personal info, by lawful and fair means.
4. **Unsolicited Info** – Destroy or de-identify unsolicited personal info if not lawfully collectible.
5. **Notification of Collection** – Take reasonable steps to notify individuals about the collection and handling of their info.
6. **Use & Disclosure** – Use or disclose personal info only for the primary purpose (or secondary if permitted).
7. **Direct Marketing** – Personal info must not be used/disclosed for marketing unless specific conditions are met.
8. **Cross-border Disclosure** – Take reasonable steps to ensure overseas recipients comply with the APPs.
9. **Government Identifiers** – Restrict use/disclosure of government-issued identifiers (e.g., Medicare numbers)
10. **Data Quality** – Ensure personal info is accurate, up-to-date, and complete.
11. **Data Security** – Protect info from misuse, loss, and unauthorised access; destroy or de-identify when no longer needed.
12. **Access** – Individuals have a right to access their personal info, subject to lawful exceptions.
13. **Correction** – Take reasonable steps to correct inaccurate, incomplete, or outdated personal info.

LAZARUS LEGAL

consultmed

Key Changes at a Glance for Small Practices

Area	Before 2025	After 2025 Reforms
Legal Coverage	Practices earning under $3M were generally exempt from the Privacy Act	All medical practices must now comply, regardless of size
Privacy Policy	Not legally required	Must publish a privacy policy that aligns with the Australian Privacy Principles
Data Security	No legal obligation to secure records	Must implement reasonable security measures, including encryption and access logs
Consent Requirements	Often implied or outdated	Must obtain clear, up-to-date, and informed consent before collecting or sharing

As of May 22, 2025, the removal of the small business exemption from Australia's Privacy Act 1988 has not yet been enacted into law. While the government has agreed in principle to this reform, it remains under consideration and has not been passed by Parliament.

LAZARUS LEGAL

consultmed

Key Changes at a Glance for Small Practices

Area	Before 2025	After 2025 Reforms
Breach Notification	No requirement to report data breaches	Must notify OAIC and affected individuals within 30 days of an eligible breach
Referrals & Sharing	Often via unsecured email or fax with no process	Must use secure systems and clearly document sharing procedures
Staff Training	Not legally required	Staff must be trained on data handling and privacy obligations
Patient Rights	Limited enforceability for patients	Patients can access, correct, and complain about data handling via OAIC
Penalties	No serious consequences for non-compliance	Civil penalties up to $50 million for serious or repeated breaches

LAZARUS LEGAL

consultmed

Why the Privacy Act changed in 2025

The Australian Government has updated the Privacy Act to better protect personal data and address modern privacy risks. Key points include:

- **Drivers for Reform:** Increasing concerns about cyber threats, data misuse, and gaps in consumer protection prompted a comprehensive review.
- **Review Process:** A formal review of the Privacy Act 1988 was conducted by the Australian Government.
- **Final Report:** In 2023, the Attorney-General's Department published its final report, recommending 116 legislative changes.
- **Significant 2025 Reform:** One of the most impactful changes was the removal of the small business exemption.
- **Impact:** This means all businesses, including small healthcare providers, must now comply fully with the Privacy Act.

Why were small businesses previously exempt?

Historical Exemption

Since 2000, businesses with annual turnover under $3 million were mostly exempt from the Privacy Act.

Original Intention

The exemption aimed to reduce the regulatory burden for low-risk, small-scale businesses.

Outdated in Practice

Over time, the exemption became inappropriate, especially for sectors handling sensitive information.

Healthcare Spotlight

Even small healthcare providers routinely handle sensitive personal data like medical records and health histories.

LAZARUS LEGAL

consultmed

Removing the exemptions for small businesses

Uneven Protections

Previous exemptions meant small businesses weren't bound by the Privacy Act, leaving gaps in patient data protection.

No Legal Recourse

Many Australians had no way to challenge data misuse by smaller providers.

Falling Behind Globally

Australia's framework was no longer aligned with international privacy standards.

New 2025 Requirement

All entities handling personal data - regardless of size - must now comply with the Privacy Act.

LAZARUS LEGAL

consultmed

Common privacy risks for medical practices

1. Sending/receiving sensitive information via fax or unsecured email

The majority of practices send or receive fax or email correspondence including referrals, results, transfer of care summaries and other patient sensitive information. Email servers like Outlook or Gmail may encrypt in transit but do not protect attachments or ensure only the intended recipient can access them.

Risk: Failing to secure communications may breach APP 11 (data security), especially if a fax or email is misdirected or accessed by an unauthorised party.

What to do: Use platforms that verify recipient identity before access, for example, password-protected documents, MFA, secure links, or encrypted messaging systems.

LAZARUS LEGAL

consultmed

Common privacy risks for medical practices

2. Using practice systems without access control or audit trails

Many practices store patient files in cloud tools like G-drive, Dropbox, OneDrive or simply on practice desktops! The issue arises when access is not restricted by role, user activity is not tracked, or data is stored offshore without adequate safeguards.

Risk: You may be in breach of APP 11 or APP 8 (cross-border disclosure) if you cannot demonstrate security and control over where and how patient data is stored.

What to do: Confirm where data is hosted and require systems that log who accessed what and when. Remove shared logins and set access based on job roles, so that staff can only access the patient information needed for their duties.

Common privacy risks for medical practices

3. Outdated or inconsistent capture of patient consent

Some practices still use onboarding forms that have not been updated in years. These forms often do not cover newer systems like telehealth, online forms, or electronic correspondence (e.g. referrals, reports). Additionally, verbal or implied consent is usually not enough (depending on the clinical situation) to share sensitive data.

Risk: Consent must be informed and current under APP 3 and APP 5. If you use or share patient data for something not disclosed at the time of collection, the consent may not be valid.

What to do: Regularly review all patient-facing forms. Ensure they accurately describe current tools and data-sharing methods. Ensure that you have appropriately captured patient/carer consent to share medical information and sensitive data.

Common privacy risks for medical practices

4. Shared inboxes or generic system logins

It is still common practice for clinics to share email or messaging inbox access across admin staff, nurses, GPs for convenience. However, this limits traceability and verification of identity.

Risk: If a data breach incident occurs, you may be unable to identify who accessed or disclosed information. That is a red flag under OAIC investigations.

What to do: Provide and require staff to use individual logins for all administrative (e.g. staff email, SSO) and clinical systems (e.g. PMS) and revoke access immediately when someone leaves or changes roles.

Common privacy risks for medical practices

5. Mishandling access or correction requests from patients

More patients are exercising their right to see and correct their data. Some practices are slow to respond, unsure of the rules, or simply unaware this is enforceable.

Risk: APP 12 and 13 grant patients the right to access or amend their data. Failure to respond within 30 days may lead to complaints to the OAIC.

What to do: Assign responsibility within your practice and create a process for responding to access or correction requests quickly and lawfully.

Common privacy risks for medical practices

6. No documented privacy or data breach response plan

Many practices do not have a formal plan for what to do if data is lost, accessed improperly, or accidentally shared. Practices should have a strong privacy policy that outlines how data is stored, handled and protected.

Risk: Under the Notifiable Data Breaches scheme, you must notify affected individuals and the OAIC within 30 days of becoming aware of an eligible breach or improper handling of sensitive information.

What to do: Write a simple breach response plan outlining who investigates, who notifies, and how the incident will be documented and contained. Implement a formal privacy policy outlining how sensitive data is managed.

LAZARUS LEGAL

consultmed

Common privacy risks for medical practices

7. Use of AI tools (e.g. scribes, dictation, conversational or voice-AI apps)

AI tools, including LLMs like ChatGPT, Otter.ai, and other scribe platforms based on these models, are increasingly being adopted by clinicians. However, many of these tools may process or store sensitive data offshore, use data to improve their models, or worse, grant companies access to confidential patient information.

Risk: Entering identifiable patient information into these tools without consent may breach the Privacy Act, particularly around unauthorised use (APP 6) and offshore data handling (APP 8). Most public or free AI tools do not guarantee privacy compliance, and training on your data is often the default.

What to do: Practices should select AI tools that operate within secure, controlled environments where data is not used to train the models. They should also ensure that data is stored locally or in a way that complies with privacy regulations, and always obtain patient consent before entering any sensitive information.

LAZARUS LEGAL

consultmed

References

- Australian Attorney-General's Department, Privacy Act Review Report (2023)
- Office of the Australian Information Commissioner (www.oaic.gov.au)
- Privacy Act 1988 (Cth), Australian Privacy Principles (APPs)

For privacy compliance reviews, website updates, contract drafting, or risk mitigation strategies, visit **www.lazaruslegal.com.au**

LAZARUS LEGAL

consultmed

How Lazarus Legal can help your practice stay compliant

The Australian Government has updated the Privacy Act to better protect personal data and address modern privacy risks. Key points include:

Website Privacy Policy: updated to reflect the Australian Privacy Principles and current digital tools (e.g. telehealth, e-referrals, cloud storage)

Patient Consent Forms: including onboarding paperwork, telehealth consent, and treatment authorisations that meet the APPs

Terms and Conditions for Bookings or Referrals: to clarify service limitations, liability, and data sharing with third parties

Internal Data Breach Response Plan: a compliant framework outlining what your team must do within the 30-day response window

Email and Data Use Protocols: policies that govern email security, third-party systems, and secure messaging in daily practice

Privacy Complaint Handling Policy: documentation to demonstrate your clinic's ability to respond to requests under APP 12 and 13

LAZARUS LEGAL

consultmed

How Consultmed can help your practice stay compliant

THANK YOU!

Questions

Lazarus Legal
1/422 Oxford St, Bondi Junction
NSW 2022 Australia

T. (02) 8644 6000
M. 0412 442 414
mark@lazaruslegal.com.au
lazaruslegal.com.au

Consultmed
53 Wright Street
Adelaide, SA 5000 Australia

M: 0401 877 258
Vikram.palit@consultmed.co
consultmed.co

LAZARUS LEGAL

consultmed