Part II – Emerging dispute risks

The life sciences sector is undergoing rapid transformation driven by digital health technologies, AI and expanding global data ecosystems. These developments are creating new legal and regulatory risks that may give rise to future disputes.

The following chapters examine several of the most significant emerging risk areas affecting life sciences organisations in Australia, including privacy governance, AI regulation and insurance exposure.

2.1

Privacy risk in the life sciences sector

Rising enforcement and cyber risk in the handling of sensitive health data.

Lead author: Sonja Read, Partner

"Sensitive health data is no longer just a compliance issue for life sciences organisations – it is a legal, regulatory and cyber risk that demands governance at every level."

Sonja Read

Chapter summary

Privacy and data protection have become critical risk areas for life sciences organisations operating in Australia. Organisations in this sector routinely collect and process large volumes of highly sensitive information, including patient health data, clinical trial information and genetic data. As digital health technologies expand and data-driven research becomes more central to innovation, the regulatory, cyber and litigation risks associated with handling this information are increasing.

Recent developments have materially altered the risk landscape. Regulators are demonstrating a greater willingness to pursue enforcement action following privacy breaches, while cyber incidents affecting healthcare organisations have increased in both frequency and severity. At the same time, reforms to Australia's privacy laws have expanded regulatory powers and introduced new civil penalty pathways.

For life sciences organisations, sensitive health data must now be treated as a strategic risk requiring robust governance, cyber resilience and coordinated oversight across legal, regulatory, IT and commercial functions.

Introduction

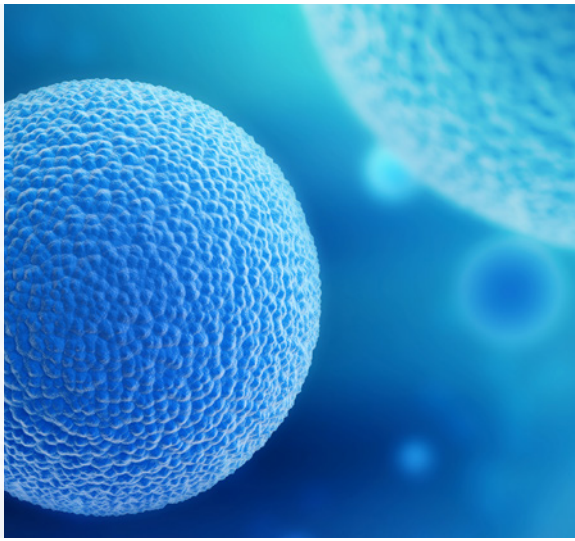
Life sciences organisations in Australia operate under heightened privacy obligations when handling health information. These organisations routinely collect and process highly sensitive data – including patient health records, clinical trial information and genetic data – often across complex networks involving healthcare providers, research institutions and global partners.

The handling of personal information is principally regulated by the *Privacy Act 1988 (Cth)* (the **Privacy Act**) and the Australian Privacy Principles (**APP**s). Recent reforms introduced through the *Privacy and Other Legislation Amendment Act 2024 (Cth)* have strengthened the regulatory framework, including new civil penalty regimes and a statutory tort for serious invasions of privacy. At the same time, regulators are adopting a more proactive enforcement posture, with the Office of the Australian Information Commissioner (**OAIC**) signalling increased scrutiny of how organisations collect, use and safeguard sensitive health information.

Against this backdrop, life sciences organisations must navigate an increasingly complex privacy landscape. This chapter examines the regulatory framework, recent enforcement trends and key compliance challenges, and outlines practical steps organisations can take to strengthen privacy governance.

According to respondents, the leading legal or compliance vulnerabilities over the next three years are:

- Product liability
- Regulatory
- Data, privacy and cyber



Legal framework

Health information is treated as a category of sensitive information under Australian privacy law and therefore attracts heightened protection. The handling of such information is governed primarily by the Privacy Act, which applies to all 'organisations'[44] that provide a 'health service'[45] and hold 'health information'. Unlike many commercial entities that deal primarily with general personal information, life sciences organisations routinely process sensitive health data and therefore operate under stricter privacy obligations.

The Privacy Act establishes 13 APPs, which regulate the collection, use, disclosure and security of personal information.[46] These principles apply to APP entities, including life sciences organisations, and are administered by the Privacy Commissioner within the Office of the Australian Information Commissioner (**OAIC**).

Under the Privacy Act, personal information is broadly defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable.[47] A subset of personal information is classified as sensitive information, which attracts a higher standard of protection.

This category includes health information, genetic information and certain biometric data.[48] Health information itself includes information about an individual's health or medical condition, information collected in providing a health service, and genetic information that may predict the health of the individual or their relatives.[49]

In addition to the Privacy Act, life sciences organisations operating across Australia may also be subject to State and Territory health privacy legislation, particularly in New South Wales, Victoria and the Australian Capital Territory.[50] While these frameworks broadly align with the Privacy Act, organisations conducting multi-site clinical trials, national pharmacy programs or digital health initiatives may need to navigate overlapping regulatory requirements.

Recent and upcoming reforms

The Privacy Act underwent significant reform in late 2024 through the enactment of the *Privacy and Other Legislation Amendment Act 2024 (Cth)* (**POLA Act**), commonly referred to as the 'tranche 1' privacy reforms. These reforms introduced a range of measures aimed at strengthening the protection of individuals' personal information and expanding the enforcement powers available to the Privacy Commissioner.

A number of the reforms commenced on 10 December 2024 when the POLA Act was enacted, with additional changes being progressively implemented through 2025 and 2026.

Several of these reforms are particularly significant for life sciences organisations, as shown in the table on the following page.

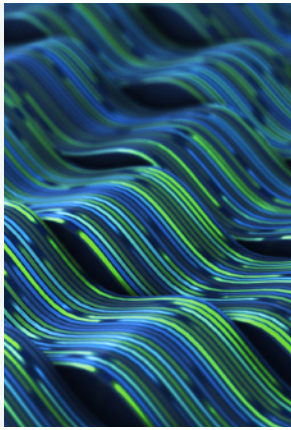
These reforms require organisations not only to update their privacy policies, but also to ensure that their use of automated systems aligns with broader expectations under the Privacy Act regarding transparency and fair handling of personal information.

In addition to these domestic reforms, the Privacy Act also has significant extraterritorial reach, which can affect international life sciences organisations conducting clinical trials or handling health data relating to individuals in Australia.

Surveyed health and life sciences leaders reported clinical trial data and patient medical records are the most frequently handled sensitive data types in their organisations.

90% of these organisations have undertaken a data audit and mapping process to understand data holdings and authorisations in the last three years.

75% of respondents are at least moderately concerned about OAIC scrutiny over the next two to three years.



Key reform	Implications for organisations
Expanded civil penalty regime	The POLA Act introduced a lower-tier civil penalty regime allowing the Privacy Commissioner to issue infringement notices for certain contraventions of the APPs, including failures relating to privacy policy transparency, anonymity options and direct marketing opt-out mechanisms. Breaches may attract penalties of up to 1,000 penalty units (approximately A$330,000) for bodies corporate. The reforms also introduced a mid-tier civil penalty regime for certain interferences with privacy, carrying maximum penalties of 10,000 penalty units (approximately A$3.3 million), and expanded the Commissioner's enforcement toolkit through the introduction of compliance notices requiring organisations to remedy contraventions of the Privacy Act.
Clarification of security and retention obligations	The POLA Act also strengthened the operation of APP 11, which requires organisations to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. The introduction of APP 11.3 clarifies that 'reasonable steps' include both technical and organisational measures designed to safeguard personal information. This clarification is particularly relevant for life sciences organisations that routinely hold large volumes of sensitive health data and are increasingly exposed to cyber threats.
Cross-border disclosure mechanisms	The reforms also introduced a mechanism allowing the Government to prescribe countries and binding schemes that provide privacy protections substantially similar to the APPs. This mechanism is intended to assist organisations when assessing whether personal information can be disclosed to overseas recipients in accordance with APP 8. The list of prescribed countries has not yet been finalised. However, the mechanism is likely to be particularly relevant for life sciences organisations engaged in: ■ international clinical trials; ■ global pharmacovigilance programs; and ■ cloud-based digital health platforms involving offshore data processing.
Statutory tort for serious invasions of privacy	A new statutory tort for serious invasions of privacy commenced on 10 June 2025. The tort provides individuals (but not corporations) with the ability to bring civil proceedings where their privacy has been seriously invaded, either through: ■ intrusion upon seclusion; or ■ misuse of private information. To succeed, a plaintiff must demonstrate (among other elements) that: ■ they had a reasonable expectation of privacy; ■ the invasion was intentional or reckless; and ■ the invasion was sufficiently serious that the public interest in protecting privacy outweighs competing public interests such as freedom of expression. Given the highly sensitive nature of health information, serious health data breaches may be particularly likely to satisfy the seriousness threshold under this tort.
Automated decision-making transparency requirements	Further reforms relating to automated decision-making (**ADM**) will commence on **10 December 2026**. These amendments introduce **APP 1.7** to **1.9**, requiring organisations to disclose in their privacy policies where automated systems are used to make, or substantially assist in making, decisions that could significantly affect an individual's rights or interests. Where such systems rely on personal information, organisations must disclose: ■ the types of personal information used; and ■ the types of decisions made or facilitated by the automated system. In the life sciences context, automated decision-making may arise in areas such as patient eligibility assessments, clinical trial screening, pharmacovigilance and digital therapeutics.

Extraterritorial application of the Privacy Act

What constitutes an 'Australian link'?

International clinical trial sponsors and multinational life sciences organisations should be aware that the Privacy Act can apply extraterritorially to organisations with an 'Australian link' under section 5B. This means the Privacy Act may apply regardless of where an organisation is headquartered, incorporated or makes operational decisions.

An Australian link arises automatically where the entity is:

- incorporated in Australia;
- a partnership formed in Australia;
- a trust created in Australia; or
- an unincorporated association with central management and control in Australia.

Importantly, foreign entities that carry on business in Australia may also have an Australian link even where they do not maintain a physical presence in the country. The concept of 'carrying on business' is not expressly defined in the Privacy Act. Case law indicates that the test focuses on whether an organisation undertakes activities in Australia on a systematic or repetitive basis as part of its business operations.[51]

Activities likely to establish an Australian link

Judicial authority indicates that determining whether business is carried on 'in Australia' generally requires *some physical activity within Australia through human instrumentalities*, although the activity does not need to constitute the bulk of the organisation's business.[52] An organisation does not need to maintain an office in Australia for the test to be satisfied.[53]

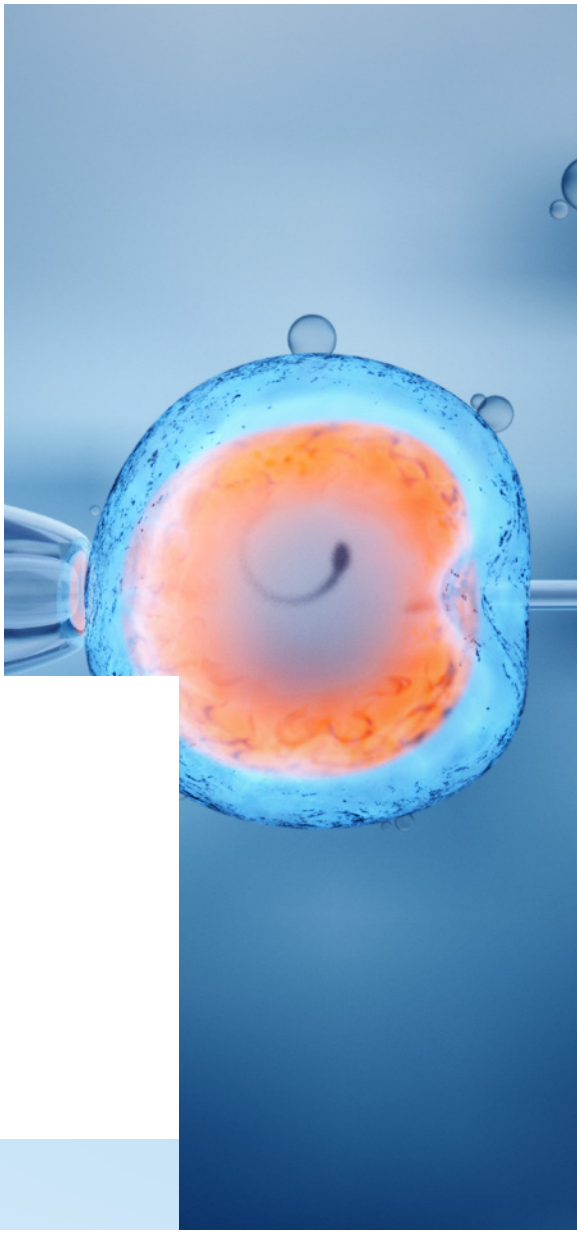
OAIC guidance indicates that an organisation may be considered to carry on business in Australia where it conducts commercial activities in Australia through employees, agents or digital platforms, or where Australian customers or participants form part of its business operations.[54]

Relevance for life sciences organisations

In the life sciences sector, a wide range of activities may establish an Australian link, including:

- establishing or contracting with Australian clinical trial sites;
- engaging Australian contract research organisations (**CROs**);
- recruiting Australian trial participants;
- collecting health information from Australian patients or trial participants (even if the data is processed offshore);
- maintaining ongoing commercial relationships with Australian healthcare providers or research institutions;
- making payments to Australian investigators or research sites; or
- using Australian participant data in global regulatory submissions.

As a result, multinational life sciences organisations involved in clinical trials, pharmacovigilance programs or global research collaborations may become subject to the Privacy Act even where their principal operations are located overseas.



Increased regulatory action

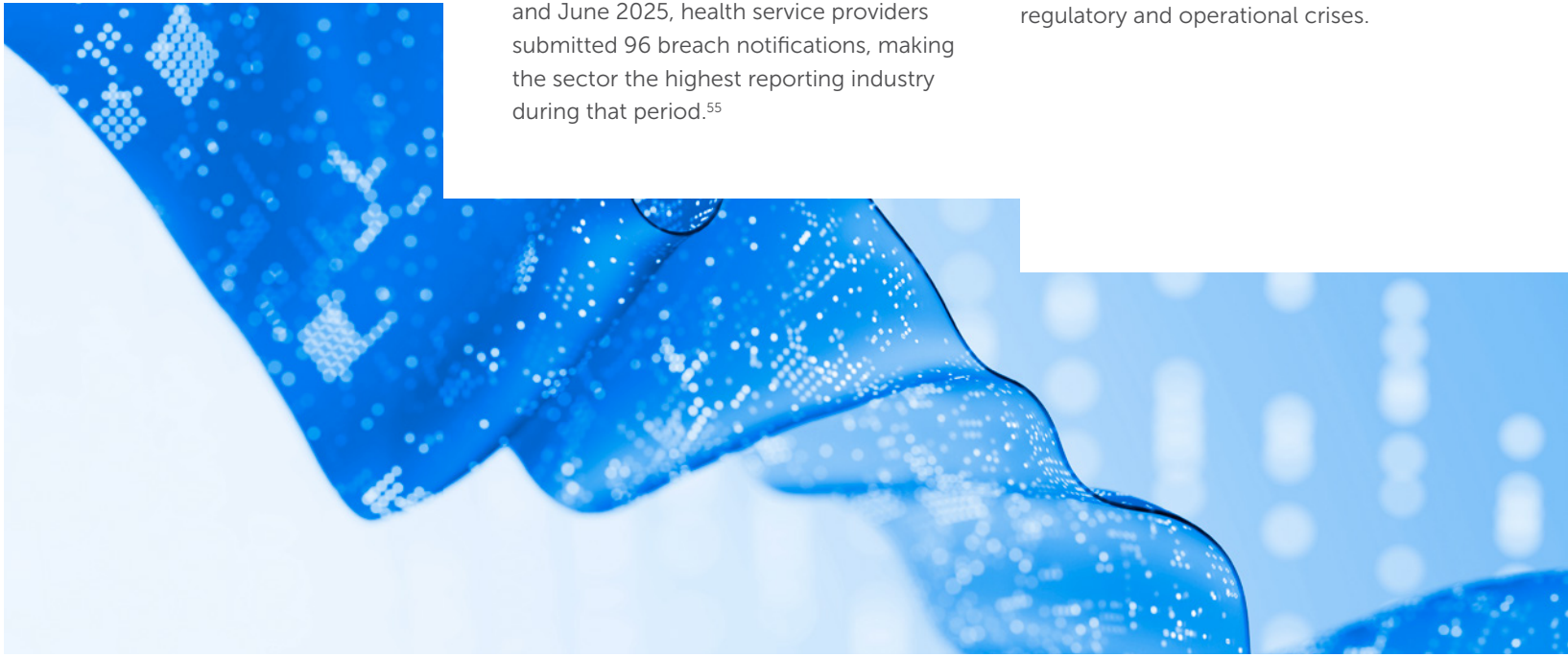
OAIC regulatory action in the health sector

The OAIC has recently signalled a more proactive and enforcement-led approach to privacy regulation. In January 2026, the OAIC commenced its first targeted compliance sweep of privacy policies, reviewing approximately 60 businesses across six sectors for compliance with the Privacy Act – particularly the requirements of APP 1 relating to privacy policies.

Chemists and pharmacists were identified as priority sectors due to the volume and sensitivity of personal information collected in the course of medication provision, including health conditions, prescription histories and patient identifiers.

Recent amendments to the Privacy Act have significantly expanded the regulatory consequences for privacy infringements. Entities with non-compliant privacy policies may now face compliance notices, infringement notices and civil penalties, including penalties of up to A$66,000 for certain contraventions. Importantly, the OAIC's enforcement powers enable it to take administrative action quickly, signalling a shift towards more active regulatory oversight.

As a practical matter, organisations should proactively audit privacy policies against APP 1.3 and 1.4. Clinical laboratories, digital health platforms, sponsors, contract research organisations and other life sciences organisations should treat privacy policy compliance as a core governance priority. Organisations should proactively audit privacy policies against APP 1.3 and 1.4, ensure collection notices accurately reflect current data handling practices, and maintain documentation demonstrating compliance efforts in the event of regulatory inquiry.



Emerging dispute trends in privacy and health information

The Notifiable Data Breaches (**NDB**) scheme, introduced through the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* and in operation since February 2018, requires organisations regulated by the Privacy Act to notify both the OAIC and affected individuals where an eligible data breach is likely to result in serious harm.

The OAIC publishes regular statistics on reported data breaches, that consistently identify the health sector as one of the most affected industries. Between January and June 2025, health service providers submitted 96 breach notifications, making the sector the highest reporting industry during that period.[55]

The health sector's persistent vulnerability reflects several structural factors, including:

- the large volumes of sensitive data held across healthcare systems;
- complex data-sharing arrangements between providers, laboratories, pharmacies, insurers and researchers;
- reliance on legacy IT infrastructure in parts of the sector; and
- the high value of medical and personal data to cybercriminals.

Recent cyber incidents illustrate how privacy failures can escalate into major regulatory and operational crises.

Major health sector breaches

Major cyber incidents in the Australian healthcare sector illustrate the scale of legal, regulatory and operational consequences that can arise when sensitive health data is compromised.

CASE STUDY

The Medibank breach – regulatory and prudential consequences of cyber failure

In October 2022, attackers accessed Medibank's systems and exfiltrated data relating to approximately 9.7 million customers. Rather than encrypting systems, the attackers threatened to publish the stolen data unless a ransom was paid. Medibank refused, resulting in the release of personal and health information on the dark web.

The OAIC subsequently commenced civil penalty proceedings in the Federal Court, alleging that Medibank failed to take reasonable steps to protect personal information under APP 11 of the Privacy Act.

The breach also triggered prudential consequences. The Australian Prudential Regulation Authority required Medibank to increase its capital adequacy by A$250 million until cybersecurity deficiencies were remediated.

LESSON

Cyber breaches involving health data can trigger multiple regulatory consequences

The Medibank breach demonstrates that privacy incidents involving health data can trigger multiple regulatory responses simultaneously, including privacy enforcement, prudential supervision and reputational damage. For life sciences organisations, cyber resilience is therefore not simply an IT issue but a core governance and regulatory risk.

CASE STUDY

Australian Clinical Labs – enforcement risk for breach management failures

In February 2022, a cyber incident involving Australian Clinical Labs resulted in the compromise of highly sensitive patient data held by Medlab Pathology, including pathology results, Medicare numbers and credit card information. Approximately 86GB of data was later published on the dark web.

Following investigation, the Federal Court declared that the organisation had contravened several provisions of the Privacy Act, including failing to take reasonable steps to protect personal information and failing to conduct a timely assessment of the breach under the Notifiable Data Breaches scheme.

In October 2025 the Federal Court imposed civil penalties of A$5.8 million for contravening multiple provisions of the Privacy Act, including sections 13G(a), 26WH(2) and 26WK(2).

LESSON

Breach response failures can lead to significant regulatory penalties

The decision highlights the OAIC's increasing willingness to pursue civil penalty litigation where organisations fail not only to secure personal information but also to comply with breach assessment and notification obligations.

CASE STUDY

MediSecure – operational consequences of data retention risk

In April 2024, MediSecure experienced a cyber incident involving historical prescription records and health information accumulated over many years. The incident highlighted risks associated with data retention practices, legacy system security and the storage of sensitive information beyond operational necessity.

The financial and operational consequences were severe. MediSecure was unable to absorb the costs associated with incident response and regulatory compliance and ultimately entered voluntary administration.

The OAIC closed its inquiries without investigation due to the company's insolvency.

LESSON

Long-term retention of health data can create existential operational risk

The incident illustrates that privacy failures can create existential business risks, particularly where organisations retain large volumes of historical health data without strong governance or cybersecurity protections.

Challenges for life sciences organisations

Life sciences organisations operating nationally may also need to navigate overlapping regulatory regimes beyond the Privacy Act. In addition to State and Territory health privacy legislation in New South Wales, Victoria and the Australian Capital Territory,[56] some organisations may also be affected by the *My Health Records Act 2012 (Cth)*, the *Healthcare Identifiers Act 2010 (Cth)*, the *National Health (Privacy) Rules 2025* and, in some cases, the *Security of Critical Infrastructure Act 2018 (Cth)*.

These overlapping frameworks are particularly relevant for organisations conducting multi-site clinical trials, digital health initiatives, real-world evidence programs or operating healthcare platforms at scale.

De-identification as an ongoing governance obligation

Under the Privacy Act, whether data is anonymous or de-identified is context dependent. Information that appears de-identified in one setting may become identifiable when combined with other datasets or accessed by parties with different capabilities.[57]

For life sciences organisations using de-identified datasets for research, product development, real-world evidence generation or AI training, the key question is whether re-identification risk remains low in practice. This requires ongoing assessment of technical safeguards, contractual protections and the capabilities of those who may access or link the data.

Life sciences organisations should therefore treat de-identification as an ongoing governance obligation rather than a one-time technical exercise.

CASE STUDY

I-MED Radiology Network – governance of de-identified health data

The I-MED Radiology Network (I-MED) matter illustrates the increasing regulatory scrutiny surrounding the use of de-identified health data in AI development.

In July 2025, the Office of the Australian Information Commissioner (**OAIC**) concluded preliminary inquiries into the handling of patient imaging data by I-MED, Australia's largest diagnostic imaging provider.

Between 2020 and 2022, I-MED shared fewer than 30 million patient studies, including X-rays, CT scans and associated diagnostic reports, with Annalise.ai – a former joint venture with Harrison.ai – for the purpose of developing and training an AI diagnostic model.

Patients were not notified of this use of their data and did not provide consent. Following media reports in September 2024, the OAIC commenced preliminary inquiries to assess whether the disclosure contravened the APPs, particularly APP 6, which regulates the use and disclosure of sensitive information for secondary purposes.

After reviewing the evidence, the Privacy Commissioner concluded that the data had been de-identified to a sufficient degree that it no longer constituted personal information under the Privacy Act.

The Commissioner noted that I-MED's de-identification practices reflected many of the practices endorsed by the National Institute of Standards and Technology, including:

- cryptographic hashing;
- time-shifting of dates;
- aggregation of outlier data; and
- redaction of embedded identifying text.

The OAIC also recognised the presence of contractual safeguards between I-MED and Annalise.ai, including provisions that:

- prohibited attempts to re-identify individuals;
- required secure storage of the dataset; and
- required notification if personal information was inadvertently disclosed.

While the Commissioner characterised the matter as a useful example of de-identification practices, she emphasised that the findings should not be interpreted as a broader endorsement of I-MED's overall compliance with the Privacy Act.

Insight: De-identified health data remains subject to regulatory scrutiny

The case highlights the importance of robust de-identification governance frameworks when life sciences organisations seek to use health data for research, analytics or AI development.

In particular, the OAIC's analysis emphasised several factors that contributed to the conclusion that the dataset was sufficiently de-identified:

- removal of direct identifiers such as names, addresses and patient ID numbers;
- application of recognised technical de-identification techniques;
- an assessment of the practical likelihood of re-identification occurring;
- contractual safeguards preventing re-identification; and
- ongoing governance and oversight of the data environment.

Together, these measures demonstrate that effective de-identification requires a layered governance approach, combining technical controls, contractual protections and ongoing risk assessment.

Importantly, despite the OAIC's findings, the case generated significant public discussion regarding the secondary use of health data. In response, I-MED subsequently introduced a consent-based approach, seeking patient consent before using de-identified imaging data for AI model training.

The episode highlights that maintaining public trust and transparency may require measures that extend beyond strict legal compliance.

> *"As health data becomes central to AI development, privacy governance can no longer be treated as a compliance exercise – it is a core component of responsible innovation in the life sciences sector."*
>
> Sonja Read

Overseas disclosures and data sovereignty

Cross-border data flows are a defining feature of the life sciences sector. Global clinical trials, international pharmacovigilance databases, multinational research collaborations and cloud-based digital health platforms frequently involve the transfer of personal information outside Australia.

However, these activities can trigger obligations under APP 8, often in circumstances where organisations may not initially recognise that offshore data processing constitutes a disclosure under the Privacy Act.

Under APP 8, where an organisation discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the recipient does not breach the APPs (other than APP 1) in relation to that information.

Importantly, section 16C of the Privacy Act provides that the Australian organisation may be liable for acts or practices of the overseas recipient that would constitute a breach of the APPs.

This accountability model creates particular challenges for life sciences organisations operating in global research and regulatory ecosystems.

Practical scenarios in the life sciences sector

Cross-border disclosures commonly arise in contexts such as:

- global clinical trials involving international research sites;
- pharmacovigilance reporting to global safety databases;
- multinational regulatory submissions requiring pooled datasets;
- cloud-based digital health platforms and medical devices with offshore processing; and
- collaborations with international research institutions or analytics providers.

In these circumstances, the Australian organisation remains responsible for ensuring that overseas recipients handle personal information consistently with Australian privacy law.

Satisfying the 'reasonable steps' requirement

In practice, organisations typically demonstrate compliance with APP 8 by implementing contractual and governance safeguards. These may include:

- binding contractual obligations requiring the overseas recipient to comply with the APPs;
- data transfer agreements within corporate groups;
- due diligence assessing the privacy practices and security standards of overseas recipients; and
- monitoring and audit rights to verify compliance with contractual obligations.

These measures are particularly important in the life sciences sector, where data may move through multiple intermediaries including contract research organisations, data analytics providers and cloud service providers.

Emerging reforms: the 'white list' mechanism

Recent reforms introduced through the Privacy and Other Legislation Amendment Act 2024 (Cth) create a mechanism allowing the Australian Government to prescribe countries or binding schemes that provide privacy protections substantially similar to the APPs.

Where personal information is disclosed to a recipient located in a prescribed jurisdiction, the Australian organisation may not be required to implement additional contractual protections.

However, the list of prescribed jurisdictions has not yet been finalised, meaning organisations must continue to rely on contractual safeguards and due diligence when transferring personal information overseas.

Life sciences organisations should therefore closely monitor the development of the proposed 'white list' framework, as it may materially affect the governance of international research collaborations and cross-border data flows.

Consent and collection complexities in health contexts

Health information is classified as sensitive information under the Privacy Act and is therefore subject to stricter requirements than other categories of personal information. Under APP 3, organisations must generally obtain consent before collecting such information.

Sensitive information may usually only be used for the primary purpose of collection unless an exception applies, such as where the individual has consented, the secondary use is reasonably expected and directly related to the primary purpose, or the activity falls within a permitted health situation under the Privacy Act.

Section 16B of the Privacy Act allows certain research uses of health information without consent where strict conditions are satisfied, including that the research is relevant to public health or public safety, the purpose cannot reasonably be achieved using de-identified data and obtaining consent is impracticable.[58]

For life sciences organisations conducting clinical research, pharmacovigilance or real-world evidence programs, the design of consent frameworks and collection notices is therefore critical to ensuring that secondary uses of health data remain lawful and aligned with patient expectations.

Technical and organisational measures

APP 11 requires organisations to take reasonable steps to protect personal information from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. It also requires organisations to destroy or de-identify personal information once it is no longer needed for a permitted purpose under the Privacy Act.

For life sciences organisations, these obligations can present particular challenges. Health information is inherently sensitive, datasets are often large, and many organisations operate complex digital environments involving clinical research platforms, connected medical devices and cloud-based infrastructure.

Unlike some jurisdictions, Australian privacy law does not prescribe specific cybersecurity standards. Instead, compliance with APP 11 is assessed against a risk-based 'reasonable steps' standard.

Recent reforms introduced by the *Privacy and Other Legislation Amendment Act 2024 (Cth)* clarify that reasonable steps include both technical measures and organisational measures designed to safeguard personal information.

In determining what constitutes reasonable steps, regulators generally consider factors such as:

- the sensitivity of the information, noting that health data attracts particularly high protection expectations;
- the volume of data held, which may increase the potential impact of a breach;
- the likelihood and severity of threats, including ransomware attacks, insider threats and targeted cyber intrusions; and
- the cost and practicality of security measures, although cost alone will rarely justify the absence of widely adopted safeguards.

In practice, life sciences organisations are typically expected to implement a combination of technical and governance controls to protect sensitive health information. These commonly include encryption of sensitive data, strong access controls and authentication mechanisms, active monitoring of systems for security incidents, and organisational measures such as staff training, vendor risk management and tested incident response procedures.

Taken together, these measures form the foundation of a privacy and cybersecurity program capable of meeting the 'reasonable steps' standard under APP 11.

Practical guidance: Privacy governance best practice framework

Life sciences organisations should adopt structured governance measures to ensure that the collection, use and protection of sensitive health information complies with the Privacy Act and the APPs.

The framework on the following pages summarises key governance measures that organisations should consider when managing privacy and cybersecurity risks.

Recent reforms, rising enforcement activity and increasing cyber risk all point in the same direction: privacy governance is becoming a core operational issue for organisations handling sensitive health data. For life sciences organisations, privacy risk can no longer be managed solely through compliance processes. It requires coordinated oversight across legal, regulatory, technology and commercial teams, together with robust governance over how health data is collected, used and protected.

As regulators increase enforcement activity and cyber threats continue to escalate, privacy governance is becoming a central operational issue for organisations handling sensitive health data. For life sciences organisations in particular, effective privacy governance requires coordinated oversight across legal, regulatory, technology and commercial teams, together with clear accountability for how health data is collected, used and protected.

Key requirement	Focus areas	Recommended actions
Governance and accountability Establish clear governance structures with leadership oversight and defined responsibilities for data privacy and cybersecurity.	■ Establishment of a dedicated privacy function with senior management reporting ■ Development of a Privacy Management Plan documenting APP implementation ■ Creation of privacy and security policies covering data collection, use, disclosure, storage and individual rights ■ Board-level privacy and cybersecurity reporting ■ Integration of privacy and cyber risk into enterprise risk management ■ Executive accountability with appropriate resourcing.	■ **Policies:** Develop privacy and information security policies reflecting Privacy Act requirements, including 2025/2026 reforms ■ **Privacy management plan:** Implement a plan outlining APP compliance, breach handling and third-party risk management ■ **Leadership oversight:** Assign executive accountability (e.g. Privacy Officer) with board reporting ■ **Risk management:** Integrate cyber and privacy risk into enterprise risk management.
Data mapping and classification Organisations must know what personal data they hold, where it flows, and how it's handled.	■ Comprehensive inventory of all personal information holdings, including health records, employee data, and customer information ■ Classification of data by sensitivity level (health and other sensitive information, biometric data, genetic information) ■ Mapping of data flows across systems, third parties and international transfers ■ Documentation of lawful bases for collection and processing under the Privacy Act ■ Identification of legacy systems or shadow IT containing unmanaged personal information ■ Data retention periods aligned with legal requirements ■ Regular audits to maintain current data mapping.	■ **Inventory:** Document all personal information held, including sources, storage locations and recipients ■ **Data flow mapping:** Map data flows including cross-border transfers to ensure APP 8 compliance ■ **Classification:** Classify data by sensitivity, with health information requiring strictest controls ■ **Minimisation:** Establish retention schedules and secure deletion processes.
Privacy compliance and data lifecycle management Ensure APP compliance and State/Territory health legislation requirements throughout the data lifecycle.	■ Implementation of consent management systems for optional data uses (marketing, research, AI training) ■ Express consent mechanisms for collecting sensitive health information ■ Processes for communicating material privacy practice changes ■ Controls ensuring data use and disclosure aligns with consent or lawful basis ■ Safeguards for overseas transfers including adequacy assessments ■ PIA processes for new projects, systems or AI applications. ■ Data quality processes to maintain accuracy.	■ **Consent and collection practices:** Review collection and consent mechanisms; maintain records and enable withdrawal ■ **Use, disclosure and cross-border transfer:** Implement controls aligning with consent or lawful basis (APP 6); use safeguards for overseas transfers (APP 8) ■ **PIAs:** Conduct PIAs for new projects involving personal information, especially health data or AI ■ **Data quality:** Maintain accuracy and integrity processes (APP 10); regularly audit and cleanse data ■ **Retention and erasure:** Implement retention policies; securely destroy or de-identify data when no longer needed (APP 11).

Key requirement	Focus areas	Recommended actions
Information security controls and cyber defences Align cybersecurity controls with recognised frameworks and Australian healthcare standards.	▪ Implementation of the Australian Signals Directorate Essential Eight[59] mitigation strategies as baseline protection ▪ Adoption of healthcare-specific frameworks (ISO 27001, NIST Cybersecurity Framework) ▪ Regular vulnerability assessments and penetration testing ▪ Incident detection and response capabilities with 24/7 monitoring for critical assets ▪ Access controls and privileged access management for health data systems ▪ Encryption at rest and in transit ▪ Business continuity and disaster recovery planning ▪ Security controls for medical devices and IoT technologies ▪ Secure software development lifecycle.	▪ **Access control:** Enforce least privilege access with multi-factor authentication ▪ **Encryption:** Use encryption for data in transit and at rest ▪ **Device security:** Ensure cybersecurity in product design; regularly patch systems including medical devices ▪ **Monitoring:** Implement continuous network monitoring with intrusion detection ▪ **Secure development:** Integrate cybersecurity into development; perform regular penetration testing ▪ **Resilience:** Maintain secure offline backups; test disaster recovery plans regularly.
Third party and supply chain management Manage privacy and security risks from third party relationships, including hospitals, cloud providers, and vendors.	▪ Due diligence for onboarding vendors handling personal information ▪ Contractual protections including data protection obligations and audit rights ▪ Regular vendor security assessments ▪ Management of overseas service providers and cross-border transfers ▪ Incident notification requirements in vendor contracts ▪ Vendor off-boarding procedures ensuring secure data return or destruction ▪ Register of third parties with data access, including sub processors ▪ Ongoing monitoring of vendor compliance.	▪ **Due diligence:** Assess vendor security posture and certifications ▪ **Agreements:** Include contractual protections specifying security requirements, breach notification and indemnities ▪ **Standards:** Communicate minimum cybersecurity standards for vendors ▪ **Breach coordination:** Establish plans for responding to vendor breaches.
Incident response and data breach management Prepare a detailed breach response plan for swift, effective incident management	▪ Development and testing of a comprehensive data breach response plan ▪ Procedures for breach containment, investigation and remediation ▪ Assessment criteria for notifiable data breach (**NDB**) scheme thresholds ▪ Templates for OAIC notification within required timeframes ▪ Protocols for notifying affected individuals.	▪ **Incident response team:** Create cross-functional team with defined roles and external contacts ▪ **Breach playbook:** Document procedures for detection, containment, assessment, notification and recovery ▪ **Notification templates:** Draft pre-approved templates for OAIC and affected individual communications ▪ **Escalation protocols:** Establish thresholds for identifying and escalating suspected incidents ▪ **Contractual audit:** Review contracts to identify breach notification obligations ▪ **Containment procedures:** Document procedures to isolate systems and preserve evidence ▪ **Impact assessment:** Develop criteria to assess 'eligible data breach' thresholds ▪ **Testing:** Conduct annual tabletop exercises; document lessons learned ▪ **Post-incident review:** Create methodology for root cause analysis and corrective actions.

Key requirement	Focus areas	Recommended actions
Privacy-by-design and AI / data innovation Embed privacy and security into new products and technologies from the design phase.	▪ Integration of privacy and cybersecurity checkpoints in product development ▪ PIAs during design phase for new technologies ▪ Data minimisation; use of anonymised or synthetic data where feasible ▪ Transparent disclosure of AI use in healthcare products ▪ TGA compliance for software/AI classified as medical devices ▪ Continuous evaluation of AI models for privacy impacts and bias ▪ Monitoring of AI-specific regulations and governance frameworks.	▪ **Design checks:** Integrate privacy and cybersecurity into development; conduct PIAs ▪ **Minimisation:** Use anonymised or synthetic data where feasible ▪ **Regulatory compliance:** Ensure TGA compliance for software/AI medical devices ▪ **Evaluation:** Continuously evaluate AI models for privacy impacts and bias.
Training and awareness Build a culture of privacy and security through regular training.	▪ Privacy training for all staff on Privacy Act requirements and data handling ▪ Cybersecurity awareness training on phishing, ransomware and social engineering ▪ Specialised workshops for teams handling sensitive data ▪ Clear internal guidance on privacy and security questions ▪ Regular evaluation of training effectiveness with annual updates ▪ Role-specific training for developers, clinicians and third-party management.	▪ **Privacy training:** Train all staff on Privacy Act requirements and data handling ▪ **Cybersecurity training:** Conduct regular cyber awareness training ▪ **Specialised workshops:** Provide targeted training for teams handling sensitive data ▪ **Guidance:** Post clear internal guidance on privacy and cybersecurity ▪ **Refresh:** Evaluate training effectiveness and update annually.
Monitoring, auditing and continuous improvement Establish ongoing processes to monitor compliance and continuously improve.	▪ Periodic internal and external audits of privacy and security controls ▪ Active vulnerability management with prompt patching and annual penetration testing ▪ Tracking of all incidents including near-misses; analysis for patterns ▪ Monitoring of regulatory developments from OAIC and other regulators ▪ Policy updates for Privacy Act reforms and evolving guidance ▪ Continuous improvement with action plans following audits or incidents ▪ Up-to-date documentation to demonstrate compliance.	▪ **Audits:** Conduct periodic internal and external audits for APP compliance ▪ **Vulnerability management:** Maintain active patching and annual penetration testing ▪ **Incident monitoring:** Track all incidents and near-misses; analyse for patterns ▪ **Regulatory watch:** Monitor OAIC developments; update policies for Privacy Act reforms ▪ **Continuous improvement:** Implement action plans following audits or incidents ▪ **Documentation:** Maintain current records to demonstrate compliance.

2.2

Artificial intelligence and intellectual property in life sciences R&D

How AI is reshaping inventorship, ownership and infringement risks

Lead author:
Zeina Milicevic, Partner

"AI is accelerating discovery in life sciences, but the legal frameworks governing inventorship and authorship are structured to protect human innovation and creativity."

Zeina Milicevic

Chapter summary

AI is rapidly transforming research and development in the life sciences sector. AI applications range from machine learning and neural networks for drug discovery to product development.

AI presents a significant market opportunity by reducing the time and cost of R&D. AI can assist in collecting, analysing, interpreting and presenting key data throughout the R&D process. These improvements in efficiency and capability expand the possibilities for innovation and growth across the life sciences sector.

*However, the growing use of AI in research raises complex intellectual property questions. Patent and copyright frameworks are structured to protect inventions and creative works produced by humans. As AI systems play a greater role in generating research outputs, uncertainty arises regarding inventorship, authorship and ownership of valuable research and development (**R&D**) assets.*

This chapter examines how existing intellectual property law applies to AI-assisted innovation in life sciences research. It considers recent international developments, the implications for patent and copyright protection and practical steps organisations can take to protect their intellectual property and mitigate infringement risks when using AI systems.

Introduction

AI is increasingly embedded throughout the life sciences R&D pipeline. Machine learning models are used to identify potential drug targets, while predictive analytics can assist in optimising clinical trial design. AI systems are also used to analyse complex genomic and biomedical datasets, enabling researchers to extract insights from large volumes of scientific data. In addition, automated tools are increasingly deployed to support molecule design and optimisation, helping accelerate the early stages of drug discovery.

These technologies offer significant commercial opportunities by accelerating discovery and improving research efficiency. For example, the global market for AI-enabled drug discovery is projected to grow substantially over the next decade as pharmaceutical and biotechnology organisations invest in data-driven innovation.

However, the increasing reliance on AI tools raises important questions about how intellectual property law applies where AI is involved in creation.

Impact on intellectual property protection

Courts around the world have begun to consider whether inventions generated with the assistance of AI can be protected under existing patent frameworks.

Inventorship refers to the individual who is recognised as having created a patentable invention. **Authorship** refers to the individual who is recognised as having created an original work, relevant to copyright protection. **Ownership** refers to who holds the legal right to exploit or commercialise the resulting IP – which may differ from the inventor or author.

CASE STUDY

DABUS litigation – can an AI system be a patent inventor?

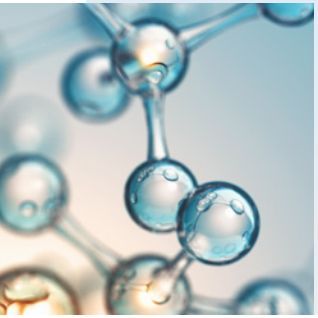
Computer scientist Stephen Thaler[60] filed patent applications in several jurisdictions naming an AI system known as DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) as the sole inventor.

The applications were intended to test whether existing patent frameworks could recognise AI-generated inventions.

In Australia, the Federal Court initially held that an AI system could be listed as an inventor. However, the decision was overturned on appeal in *Commissioner of Patents v Thaler*,[61] where the Full Federal Court held that the *Patents Act 1990 (Cth)* requires an inventor to be a natural person. The Full Court reached this decision primarily through statutory construction and also considered the history of patent law and its role in rewarding human ingenuity.

Dr Thaler subsequently sought special leave to appeal to the High Court, which was refused.

Courts in the US, the UK and the EU have reached similar conclusions.



LESSON

AI-generated inventions still require human inventorship

As it stands, Australian law requires that a patent inventor be a natural person. This means that an AI system or AI tool cannot be named as an inventor on a patent application. Any change in this position would require legislative reform.

In litigation, when faced with a question of who is the true inventor of a patent, a key consideration is whether a person has materially contributed to the invention having regard to the quality, rather than the quantity, of the contribution. This framework may guide the approach to how courts consider the question of AI contributions to innovations.

For life sciences organisations using AI-assisted discovery tools, organisations may wish to ensure that research workflows document human contributions that may support inventorship claims in future patent applications.

> *"As AI becomes embedded in life sciences R&D, protecting innovation will increasingly depend not only on patents, but on how organisations structure data governance, trade secrets and human oversight."*
>
> Zeina Milicevic

Copyright law and authorship

Copyright is another important intellectual property right that can arise in research and development activities.

Copyright protects literary and artistic works, including materials commonly generated in scientific research such as:

- research notes;
- datasets and databases;
- data visualisations and charts; and
- analytical tools and reports.

Consequently, copyright can be key to protecting data that supports research, but that may not appear in the patent application itself.

Under the *Copyright Act 1968 (Cth)*, copyright subsists only in works created by a human author. Works generated entirely by AI systems without human involvement are therefore unlikely to attract copyright protection.

This creates potential risks for organisations that rely heavily on AI systems to generate research outputs. Copyright law differs from patent law in that copyright protection arises automatically upon creation of a work. There is no requirement to register copyright (or name an author upon creation). This means that questions of whether a work has a human author may not arise until an enforcement dispute.

The level of human contribution required for copyright protection in AI-assisted works remains uncertain. Using tools in creation is not new and does not preclude copyright protection. However, the human creator must contribute sufficient 'independent intellectual effort'. With AI-generated works, it is unclear what level of human contribution will satisfy this authorship requirement.

Overseas jurisdictions are also grappling with this question. For example, the United States Copyright Office refused copyright registration for an AI-generated artwork created using extensive prompting, concluding that the work lacked sufficient human authorship.[62] By contrast, a Chinese court has found that prompt selection and parameter choices may constitute sufficient human input to support copyright protection.[63]

These divergent outcomes highlight the evolving and uncertain nature of copyright protection for AI-generated materials.

Strategic considerations for securing IP protection

In the current legal environment, life sciences organisations should take proactive steps to ensure that AI-assisted innovation remains capable of attracting intellectual property protection.

Practical measures may include:

- identifying which stages of research workflows require meaningful human involvement to support inventorship or authorship;
- maintaining contemporaneous records documenting human contributions to inventions and research outputs;
- implementing internal policies governing the use of AI tools in R&D processes; and
- auditing research workflows to assess whether outputs treated as proprietary assets involve sufficient human input to support intellectual property protection.

Alternative strategies for protecting AI-generated innovation

Where patent or copyright protection may be uncertain, organisations should consider adopting a multi-layered intellectual property strategy.

Trade secrets and confidential information can play an important role in protecting valuable research assets, including proprietary datasets, algorithms and technical know-how.

Unlike patents, trade secrets do not require public disclosure and can remain protected indefinitely, provided the information remains confidential and continues to provide a competitive advantage.

Survey results indicate that **70%** of organisations have established formal governance frameworks to address IP and data ownership risks in AI.

To maintain trade secret protection, organisations should:

- identify and clearly classify confidential research assets;
- restrict access to sensitive information on a need-to-know basis;
- implement robust confidentiality agreements with employees and collaborators; and
- adopt contractual controls when sharing proprietary information with research partners.

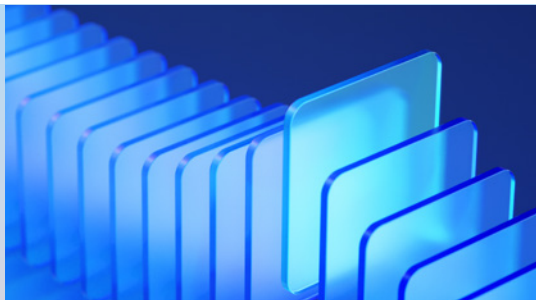
IP infringement risks associated with AI systems

The use of AI tools in research can also create intellectual property infringement risks.

These risks may arise both during the development of AI systems and when organisations use AI-generated outputs.

AI models are typically trained using vast datasets that may include copyright-protected materials. Whether the use of such materials for training purposes constitutes copyright infringement remains an unresolved legal question in Australia.

On the output side, AI-generated materials may reproduce or closely resemble copyrighted works or patented inventions contained in the training data. Organisations that subsequently use or distribute these outputs may expose themselves to infringement risk.



To mitigate these risks, organisations should consider:

- conducting due diligence on AI tools and their training data sources;
- reviewing contractual arrangements with AI providers;
- implementing internal guidance governing the use of AI tools and prompts; and
- establishing governance frameworks for AI-assisted innovation and content generation.

Practical guidance: Protecting IP in AI-enabled R&D

Life sciences organisations integrating AI into research programs should consider adopting structured governance frameworks to manage intellectual property risks.

Key measures may include:

- documenting human contributions to inventions generated with AI tools;
- establishing internal policies governing the use of AI systems in R&D;
- implementing contractual protections with AI vendors and research partners;
- maintaining robust trade secret protection for proprietary datasets and algorithms; and
- regularly reviewing AI-assisted research workflows to ensure intellectual property protection remains available.

As AI becomes increasingly embedded in scientific discovery, organisations that proactively address intellectual property risks will be better positioned to protect their innovations and maintain competitive advantage.

2.3
AI governance and regulatory risk

Privacy, liability and regulatory risks arising from AI deployment

Lead authors: Sonja Read, Partner, Zeina Milicevic, Partner and Chelsea Gordon, AI Lead – Legal

Chapter summary

AI is increasingly embedded across the life sciences sector, supporting drug discovery, clinical research, diagnostics and patient care. While these technologies offer significant opportunities to accelerate innovation and improve healthcare outcomes, they also introduce new legal, regulatory and operational risks.

Unlike intellectual property questions surrounding AI-assisted inventions, which are considered in the previous chapter, this chapter focuses on the governance and regulatory implications of deploying AI systems in practice. In Australia, AI is currently regulated through a complex patchwork of existing legal frameworks rather than a dedicated AI statute. Privacy law, consumer protection law, therapeutic goods regulation, workplace safety obligations and sector-specific regulation may all apply depending on how AI systems are used.

> *AI governance is rapidly shifting from a voluntary best practice to an emerging regulatory expectation across the life sciences sector."*
>
> Chelsea Gordon

Introduction

AI is increasingly deployed across the life sciences sector, supporting clinical research, diagnostics, patient care and operational decision-making. While these technologies offer significant opportunities to improve healthcare outcomes and accelerate innovation, their adoption also introduces new legal, regulatory and operational risks.

Unlike the previous chapter, which focuses on intellectual property issues arising from AI-assisted innovation, this chapter examines the governance and regulatory implications of deploying AI systems in practice.

In Australia, AI is currently regulated through a complex patchwork of existing legal frameworks rather than a dedicated AI statute. Privacy law, consumer protection law, therapeutic goods regulation, workplace safety obligations and sector-specific regulation may all apply depending on how AI systems are used.

The evolving regulatory landscape in Australia

AI regulation varies significantly across jurisdictions.

In Europe, the **EU AI Act** introduces a comprehensive risk-based regulatory framework governing the development and deployment of AI systems. In the US, regulatory responses have emerged at both federal and state levels, including California's **Transparency in Frontier AI Act**, which focuses on accountability for advanced AI systems.

Australia has adopted a different approach. Rather than introducing standalone AI legislation, the Australian Government has signalled a preference for a **principles-based regulatory model** that relies primarily on existing legal frameworks.

The National AI Plan[65], released in December 2025, confirms the Government's intention to maintain a relatively light-touch regulatory approach designed to encourage investment and innovation.

Under this approach, AI systems are regulated indirectly through existing laws, including:

- privacy legislation;
- consumer protection law;
- copyright law;
- workplace health and safety law;
- sector-specific regulatory frameworks; and
- online safety regulation.

The Government has indicated that targeted regulatory reforms may occur where necessary to address specific AI-related risks.

For example, in October 2025 the Commonwealth Treasury released findings from a review examining whether the Australian Consumer Law (**ACL**) is fit for purpose in addressing risks arising from AI systems.[66]

At the same time, regulators are increasingly examining how existing regulatory frameworks apply to AI technologies within the health and life sciences sectors. The Department of Health and the Therapeutic Goods Administration (**TGA**) have both undertaken consultations regarding regulatory updates for AI-enabled medical technologies.

As a result, organisations operating in the life sciences sector must navigate a dynamic regulatory environment in which legal obligations may evolve rapidly.

95% of the leaders surveyed reported their organisation is using AI. The most common uses are:

1. Regulatory submissions/ compliance monitoring.
2. Clinical trial design or patient testing.
3. Commercial operations (marketing, sales).
4. Drug discovery and development.
5. Medical devices or diagnostic tools.

Insight: AI governance is becoming a core compliance issue

Although Australia does not yet have a standalone AI statute, regulatory scrutiny of AI systems is increasing. Organisations deploying AI technologies must therefore ensure that existing legal frameworks – particularly those relating to privacy, consumer protection and product safety – are appropriately integrated into their governance structures.

For life sciences organisations, AI governance is no longer solely a technical or operational issue. It is increasingly a core compliance and risk management function requiring coordinated oversight across legal, regulatory, clinical and technology teams.

> *"In practice, AI governance is not about the technology itself – it's about how organisations manage data, oversight and accountability around the systems they deploy."*
>
> Sonja Read

Key legal risks associated with AI deployment

The deployment of AI technologies in the life sciences sector can create several categories of legal risk beyond intellectual property issues.

Survey results show that product safety and data privacy AI governance frameworks are relatively well-established.

However, many organisations have not yet established formal AI governance frameworks addressing workforce capability and human oversight **(60%)**, third-party / vendor AI risk **(59%)**, or bias, ethics and regulatory risk **(57%)**.

Privacy risks

The use of personal information in AI systems presents significant privacy risks. Organisations that handle personal information are subject to the *Privacy Act 1988 (Cth)* (**Privacy Act**), which imposes obligations on Australian Privacy Principle (**APP**) entities regarding the collection, use, disclosure and security of personal information.

Civil penalties for serious or repeated interferences with privacy under the Privacy Act can reach the greater of A$50 million, three times the value of the benefit obtained, or 30% of adjusted turnover during the breach period.

Recent amendments to the Privacy Act introduced through the *Privacy and Other Legislation Amendment Act 2024 (Cth)* have further expanded regulatory exposure by introducing a statutory tort for serious invasions of privacy. Individuals may now bring civil proceedings where their privacy has been intentionally or recklessly invaded in circumstances where they had a reasonable expectation of privacy.

Because life sciences organisations frequently handle highly sensitive health information, the use of such data to train AI systems represents a particularly high-risk activity.

Surveillance law risks

Certain AI systems may involve the recording or analysis of audio or visual data. These activities may be regulated by state-based surveillance legislation.

For example, the *Surveillance Devices Act 2007 (NSW)* restricts the use of listening devices to record private conversations without consent. Similar laws apply in other Australian jurisdictions.

AI technologies such as clinical documentation tools ('AI scribes'), facial recognition systems or video-based diagnostic tools may therefore raise surveillance law compliance issues.

Consumer protection risks

AI-generated outputs may create risks under the ACL where organisations fail to disclose that services involve AI systems or fail to adequately communicate the limitations of those systems.

In certain circumstances, inaccurate or misleading AI-generated information could give rise to claims of misleading or deceptive conduct. In serious cases, civil penalties may reach the greater of A$50 million, three times the value of the benefit obtained, or 30% of adjusted turnover during the breach period.

Therapeutic goods regulation

Where AI is incorporated into medical devices, it may fall within the regulatory category of Software as a Medical Device (**SaMD**).

Manufacturers and sponsors must ensure that such devices are appropriately assessed by the Therapeutic Goods Administration before they can be supplied in Australia. This includes demonstrating the safety, performance and ongoing monitoring of AI-enabled systems.

Failure to comply with these obligations may constitute a breach of the *Therapeutic Goods Act 1989 (Cth)* (the **TG Act**) and attract significant civil or criminal penalties.

Workplace and operational risks

The implementation of AI systems may create additional workforce risks in the life sciences sector. Where the use of an AI system poses work health and safety risks, a person conducting a business or undertaking (**PCBU**) has a duty to eliminate or minimise risks so far as reasonably practicable.[67]

For example, recent reforms in New South Wales impose additional obligations where digital work systems – including AI, algorithms or automated platforms – are used to allocate or manage work.

These provisions are intended to prevent technologies from imposing unsafe workloads or enabling unreasonable workplace surveillance.

To comply with these obligations, organisations should review their work health and safety policies and ensure they are aligned with internal AI governance frameworks and acceptable use policies.

Ethical and research risks

AI technologies used in clinical research may raise ethical considerations relating to participant consent, fairness and transparency.

Human research in Australia is subject to oversight by Human Research Ethics Committees (**HREC**s). The introduction of AI systems into clinical trials may therefore require additional approvals and disclosures.

AI-driven participant recruitment tools may also create risks of unintended bias or discrimination if training datasets are not appropriately representative.

Product liability risks

AI-enabled products and services may give rise to emerging product liability risks. In the US, litigation involving AI-powered technologies is beginning to test whether traditional product liability frameworks apply to AI systems. For example, *Garcia v Character Technologies, Inc* has raised questions about whether AI systems may be treated as a 'product' for the purposes of liability analysis.[68]

Similarly, in T*aylor v Intuitive Surgical* [69], a court found that a clinician may not be solely responsible for harm arising from the use of a robotic surgical system. The manufacturer was found to have breached its duty to warn the hospital purchaser about risks associated with the system.

While the position under Australian law remains uncertain, these developments highlight the potential for liability to extend beyond clinicians to technology developers and manufacturers where AI-enabled systems contribute to clinical decision-making.

CASE STUDY

AI training data and de-identification

In July 2025, the Office of the Australian Information Commissioner (**OAIC**) examined whether I-MED Radiology Network breached the Privacy Act when medical imaging data was shared with the healthcare AI organisation Harrison.ai for the purpose of training diagnostic algorithms.

The investigation considered whether the disclosure breached APP 6, which governs the use and disclosure of personal information. The OAIC ultimately concluded that the data had been sufficiently de-identified and therefore did not constitute personal information under the Privacy Act.

LESSON

De-identification is critical for AI training datasets

The investigation highlights the importance of robust data governance when using health information to train AI systems. Organisations should ensure that AI training datasets are appropriately de-identified and supported by clear governance frameworks, contractual safeguards and documented data handling processes.

CASE STUDY

AI-generated medical advice and consumer protection risk

In January 2026, reports emerged that Google's 'AI Overview' search functionality had provided incorrect medical information in response to queries relating to pancreatic cancer and liver disease.

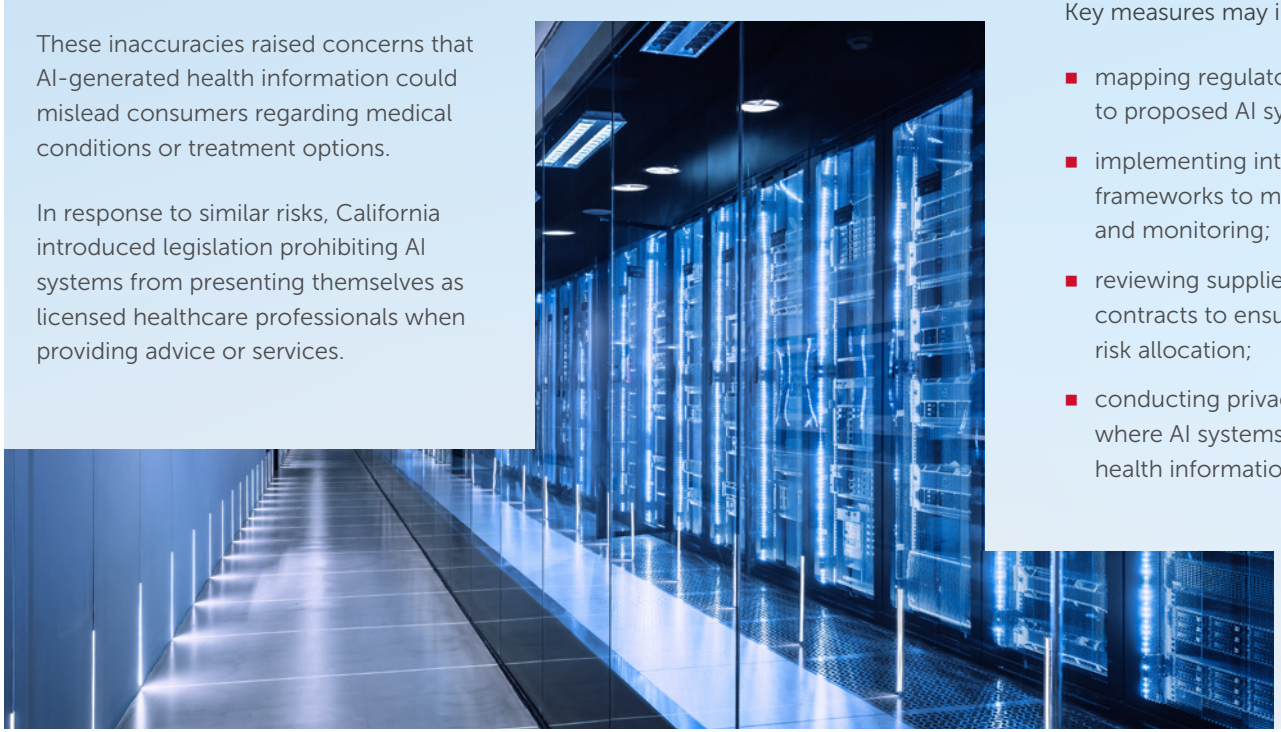
These inaccuracies raised concerns that AI-generated health information could mislead consumers regarding medical conditions or treatment options.

In response to similar risks, California introduced legislation prohibiting AI systems from presenting themselves as licensed healthcare professionals when providing advice or services.

LESSON

Transparency is essential when AI systems interact with patients

Organisations deploying AI-enabled health technologies should ensure that users clearly understand when they are interacting with an AI system and the limitations of AI-generated outputs.



Practical guidance: AI governance for life sciences organisations

To manage the legal risks associated with AI deployment, life sciences organisations should consider implementing structured AI governance frameworks.

Key measures may include:

- mapping regulatory obligations relevant to proposed AI systems and use cases;
- implementing internal AI governance frameworks to manage risk identification and monitoring;
- reviewing supplier and technology contracts to ensure appropriate risk allocation;
- conducting privacy impact assessments where AI systems process personal or health information;
- developing internal policies governing the use of AI systems in research and clinical contexts;
- ensuring that employees receive guidance on appropriate use of AI technologies; and
- reviewing insurance coverage to determine whether AI-related risks are adequately addressed.

As AI becomes increasingly embedded in scientific discovery and healthcare delivery, organisations that proactively address governance and regulatory risks will be better positioned to protect patients, maintain regulatory compliance and realise the benefits of AI-driven innovation.

2.4

Insurance gaps and dispute exposure

Why many organisations discover coverage gaps too late

Lead author:
Kemsley Brennan, Partner

"Many life sciences organisations discover gaps in their insurance cover only after a claim arises. Proactive review of insurance programs is critical to managing litigation and regulatory risk."

Kemsley Brennan

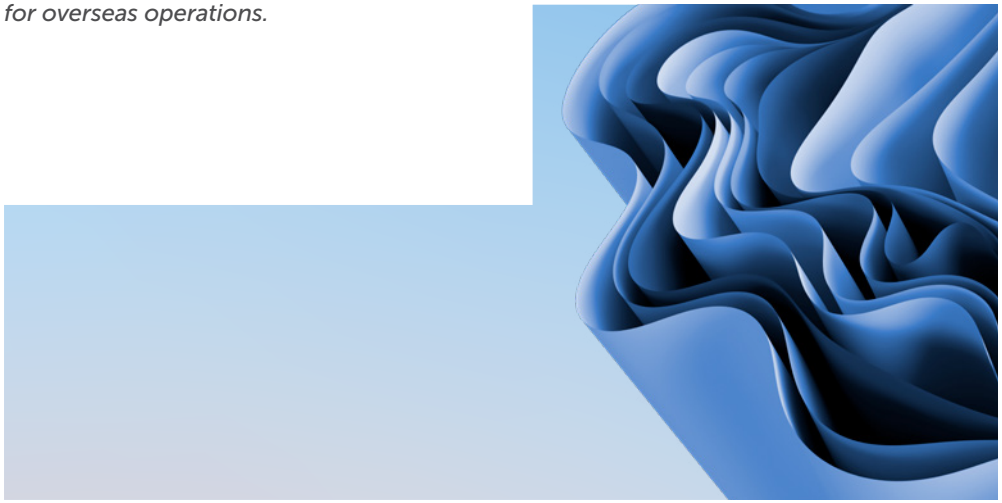
Chapter summary

Insurance plays a critical role in managing the litigation, regulatory and operational risks faced by life sciences organisations. Pharmaceutical, biotechnology, medical device and digital health organisations operate in a highly regulated environment where product liability claims, clinical trial disputes, shareholder actions and cyber incidents can lead to substantial financial exposure.

Despite this risk landscape, many life sciences organisations discover only after a claim arises that their insurance programs contain significant gaps in coverage. Policies may exclude key activities such as clinical trials, professional services or product recalls, or may contain territorial limitations that restrict cover for overseas operations.

As the preceding chapters illustrate, life sciences organisations operate within an increasingly complex legal and regulatory risk landscape. Insurance therefore plays a critical role in transferring and managing the financial consequences of these risks when disputes or regulatory actions arise.

This chapter outlines the key insurance coverages that life sciences organisations should consider and highlights common coverage gaps. It also provides practical guidance for reviewing insurance programs, managing policy exclusions and ensuring that coverage limits remain appropriate as businesses expand into new markets or technologies.



Introduction

Life sciences organisations operate in a complex risk environment shaped by regulatory oversight, scientific uncertainty and global markets. Litigation risks may arise from product safety concerns, clinical trial outcomes, regulatory investigations or shareholder claims. At the same time, emerging risks such as cyber-attacks and data breaches create additional exposures.

Insurance is therefore an essential component of risk management for organisations operating across the pharmaceutical, biotechnology and medical technology sectors. However, insurance programs must be carefully structured to ensure that they respond appropriately to the specific risks faced by life sciences businesses.

Standard corporate insurance policies are rarely sufficient on their own. Life sciences organisations typically require a combination of specialised policies designed to address risks arising throughout the product development lifecycle, from early-stage research through to product commercialisation.

Insight: Insurance gaps often emerge only after a claim

A common challenge for life sciences organisations is that insurance coverage gaps are only discovered once litigation or regulatory action has commenced. Exclusions relating to clinical trials, professional services or contractual liabilities may significantly reduce the protection provided by otherwise comprehensive policies.

Regular review of insurance programs – particularly when organisations expand internationally, launch new products or begin clinical trials – is therefore essential to ensure coverage remains aligned with the organisation's evolving risk profile.

Key insurance coverages in the life sciences sector

A comprehensive insurance program for life sciences organisations typically includes several specialised coverages designed to address different categories of risk.

General liability insurance

General liability insurance forms the foundation of most corporate insurance programs. It typically provides cover for third-party claims arising from bodily injury or property damage caused by the organisation's activities.

However, these policies often contain exclusions relevant to life sciences organisations, including exclusions relating to clinical trials, professional services or contractual liabilities. Organisations should therefore review policy wording carefully to ensure key exposures are not excluded.

Product liability insurance

Product liability insurance provides protection against claims arising from the design, manufacture or distribution of pharmaceutical products, biotechnology products or medical devices.

These policies typically respond to third-party claims alleging that a product caused injury or harm to consumers.

For organisations distributing products internationally, it is important that product liability policies provide worldwide territorial coverage, particularly where products are supplied into high-litigation jurisdictions such as the US.

Clinical trials liability insurance

Clinical trials liability insurance provides coverage for risks associated with clinical research involving human participants. Policies generally cover compensation claims arising from death, bodily injury or illness suffered by participants during the course of a clinical trial.

These policies are typically written on a claims-made basis, meaning coverage is triggered when a claim is first made and notified during the policy period.

Clinical trials policies should ideally include broad coverage for:

- participant injury compensation;
- defence costs;
- settlement payments; and
- medical expenses arising from trial participation.

Many policies also extend coverage to additional insured parties such as contract research organisations, investigators, clinical trial sites and ethics committees.

Directors' and officers' liability insurance

Directors' and officers' (D&O) liability insurance protects company directors and senior executives against claims arising from alleged wrongful acts committed in their management capacity.

D&O policies typically include three forms of cover:

- **Side A cover** – protection for individual directors and officers;
- **Side B cover** – reimbursement for the company when it indemnifies directors; and
- **Side C cover** – entity coverage for claims brought directly against the company.

Life sciences organisations face heightened D&O risk due to volatile clinical trial outcomes, capital-raising pressures and regulatory scrutiny.

CASE STUDY

Mayne Pharma Group Limited – D&O insurance limits under pressure

In 2024, the ASX-listed pharmaceutical company Mayne Pharma Group Limited agreed to settle a shareholder class action for approximately A$38 million, without admitting liability.[70]

Insurance covered only A$4.7 million of the settlement, leaving the organisation to fund the remainder.

LESSON

D&O policy limits may be insufficient for major shareholder litigation

The case illustrates the importance of stress-testing D&O policy limits against potential shareholder class actions, regulatory investigations and market disclosure claims.

Professional indemnity insurance

Professional indemnity insurance provides cover for claims alleging financial loss arising from negligent advice or professional services.

In the life sciences sector, this may include services such as:

- clinical trial management;
- research services;
- laboratory testing; and
- consulting or advisory services.

Product liability policies frequently exclude professional services claims, meaning that a separate professional indemnity policy is often necessary.

Intellectual property insurance

Life sciences organisations frequently face risks relating to alleged infringement of intellectual property rights, including patents, trademarks, designs or copyright.

Intellectual property insurance can provide coverage for defence costs and damages arising from third-party claims alleging infringement of intellectual property rights.

Although some limited coverage may be available under general liability policies, many organisations obtain standalone intellectual property insurance to ensure more comprehensive protection.

Product recall insurance

Product recall insurance provides coverage for costs associated with recalling defective products from the market. These costs may include:

- regulatory notification;
- product retrieval and disposal;
- transportation and logistics;
- crisis management and communications; and
- business interruption losses.

Product recall insurance is particularly important in the pharmaceutical and medical device sectors where regulatory authorities may require urgent market withdrawal of products.

The **Therapeutic Goods Administration's updated recall procedures**, introduced in March 2025, have increased regulatory expectations regarding product recall readiness in Australia.

Cyber liability insurance

Life sciences organisations increasingly hold large volumes of sensitive data, including patient records, clinical trial data and proprietary research information.

Cyber liability insurance provides protection against losses arising from cyber incidents such as data breaches, ransomware attacks or system disruptions.

Traditional property or liability policies often exclude cyber-related incidents, meaning that a dedicated cyber insurance policy is typically required.

CASE STUDY

Merck – cyber insurance disputes following the NotPetya attack

In 2017 a cyber-attack involving the NotPetya malware caused approximately US$1.4 billion in losses for pharmaceutical company Merck & Co.[71]

Merck's insurers initially declined coverage under an 'acts of war' exclusion contained in its insurance policies. The dispute resulted in significant litigation before the matter was eventually resolved through settlement.

LESSON

Cyber policy exclusions can materially affect coverage

The dispute highlights the importance of carefully reviewing cyber insurance policy wording, particularly exclusions relating to cyber warfare or state-sponsored attacks.

Managing policy exclusions and coverage gaps

Insurance policies frequently contain exclusions, limitations or special conditions that may significantly affect coverage.

For example, insurers may exclude liability assumed under contract beyond ordinary legal obligations. This can create gaps where organisations provide broad indemnities or performance guarantees to commercial partners.

Organisations should therefore review insurance policies carefully to identify exclusions relating to:

- specific products or components;
- known safety concerns;
- contractual indemnities;
- professional services; and
- clinical trials activities.

Where possible, organisations may seek to negotiate narrower exclusions or obtain additional endorsements from insurers.

Ensuring coverage for global operations

Life sciences organisations often operate internationally through clinical trials, overseas manufacturing arrangements or product distribution networks.

Insurance policies should therefore be reviewed to ensure that territorial coverage extends to all relevant jurisdictions.

Some policies restrict coverage to Australia and New Zealand or exclude claims arising in the US due to higher litigation risks. Where organisations operate globally, it may be necessary to arrange international insurance programs or obtain local policies in relevant jurisdictions.

Foreign regulatory regimes may also impose insurance requirements. For example, the EU Medical Devices Regulation (**EU MDR**) requires manufacturers to maintain 'sufficient financial coverage' for potential liability claims.

Claims notification and policy conditions

Many insurance policies operate on a claims-made basis, meaning that coverage depends on notifying the insurer of claims or potential claims during the policy period.

Organisations should notify insurers as soon as practicable of any circumstances that could give rise to a claim. These may include serious customer complaints, regulatory investigations or adverse clinical trial events.

Prompt notification is critical because failure to notify circumstances within the policy period may result in coverage being denied.

In some situations, legal advice may be helpful when preparing notifications to ensure that potential claims are captured appropriately under the policy.

Setting appropriate policy limits

Determining appropriate insurance limits requires careful consideration of the organisation's risk profile.

Organisations should regularly review coverage limits with their insurance brokers and advisers, particularly where the organisation:

- launches new products;
- expands into new markets;
- outsources manufacturing;
- begins new clinical trials; and
- handles increasing volumes of patient data.

Insurance limits should also account for the possibility that multiple related claims may be aggregated under a single policy limit.

Where defence costs are included within policy limits, prolonged litigation can quickly erode available coverage.

Practical guidance: Insurance coverage checklist

The following checklist summarises key governance measures that life sciences organisations should consider when reviewing their insurance programs and identifying potential coverage gaps.

For life sciences organisations operating in a highly regulated and litigation-sensitive environment, insurance should be treated as a strategic risk management tool rather than an administrative procurement exercise. Regular review of insurance coverage, policy limits and exclusions is essential to ensure that coverage evolves alongside the organisation's operational, regulatory and geographic risk profile.

Key action items	Implementation	Practical notes/examples
Confirm that all key life science risks are insured	Organisations should ensure they carry the full suite of policies relevant to their operations, including (as applicable): ■ public and product liability ■ clinical trials liability ■ D&O liability ■ professional indemnity (particularly for R&D, testing or advisory activities) ■ cyber liability ■ product recall and contamination insurance ■ intellectual property infringement insurance.	Life sciences organisations face a broader risk landscape than most industries. Standard public and product liability insurance is rarely sufficient alone. Verify you hold the full spectrum of policies a life sciences business needs. Address common gaps with the specialist coverages below.
Consider specialist coverage: Clinical trials liability	Organisations should consider whether the organisation holds clinical trials liability insurance for all current and planned trials, across all phases and jurisdictions. Review territorial limits, indemnity limits and participant injury wording for compliance with ethics committee and regulatory requirements.	Regulators and ethics committees often require clinical trials liability cover. Policies may only respond to Australian trials unless they expressly include overseas sites. Gaps commonly arise when organisations expand trials internationally without updating insurance.
Consider specialist coverage: D&O liability	Organisations should review any D&O policy coverages including additional coverages, limits, sub-limits and exclusions, and policy conditions against the organisation's capital structure, disclosure obligations and regulatory exposure. It is important to stress test the policy limits against potential shareholder class actions and regulatory investigation and prosecution scenarios.	In 2024, Mayne Pharma Group Limited (ASX: MYX) settled a shareholder class action for AU$38 million (without admitting liability). Insurance covered only AU$4.7 million – the organisation funded the balance. This highlights the consequences of insufficient D&O policy limits and the importance of appropriate limit adequacy for shareholder class action exposure.
Consider specialist coverage: Professional indemnity	Organisations should confirm whether the business provides R&D, testing, design, advisory or consultancy services (including to third parties). If so, organisations should consider whether these activities fall under a professional indemnity policy or product liability policy.	Product liability insurers commonly exclude professional services claims unless the organisation holds separate cover – a frequent gap for biotech and medtech organisations engaged in contract research or advisory work.
Consider specialist coverage: Cyber liability	Organisations should consider whether they require dedicated cyber insurance. It may be insufficient to rely on property, 'all-risks' or general liability policies. Consider whether the policy responds to data breaches (including patient and trial data), ransomware and extortion, business interruption, incident response and forensics, legal and regulatory response costs, notification and credit monitoring, and third-party liability claims. Review any exclusions (e.g. war or state-sponsored attack), sub-limits, waiting periods and notification requirements. Align internal incident response procedures with policy conditions. It is also important not to attach cyber liability as an endorsement to a general policy; cyber insurance should typically be structured as a standalone policy.	Life sciences organisations hold highly sensitive data including patient records and clinical trial results. Traditional liability policies usually do not respond to cyber incidents. In 2017, Merck suffered ~US$1.4 billion in losses from the NotPetya cyber-attack. Insurers denied cover under an 'acts of war' exclusion – underscoring the need to scrutinise cyber policy language.

Key action items	Implementation	Practical notes/examples
Consider specialist coverage: Product recall and contamination	It is important to review whether product liability policies exclude recall and contamination costs. Where necessary, obtain dedicated recall and contamination insurance covering first party recall expenses and associated business interruption losses.	Product liability insurance often excludes recall and correction costs. The TGA's updated Procedure for Recalls, Product Alerts and Product Corrections took effect on 5 March 2025 – recall readiness and insurance are more important than ever.
Review intellectual property infringement insurance	It is important to ensure that the life science organisation has intellectual property insurance that will provide cover for breach of intellectual property rights	There may be some cover for intellectual property breaches under the General Liability policy but such cover is usually very limited. Obtaining a standalone Intellectual Property policy is a prudent approach.
Scrutinise exclusions and contractual assumptions of risk	Organisations should conduct a detailed review of policy exclusions, limitations and conditions – focusing on known defects, specific components, ingredients and jurisdictions. Cross check insurance cover against indemnities and guarantees in commercial contracts.	Insurers generally do not cover liabilities you assume under contract beyond ordinary legal duties. If broad indemnities or performance guarantees are not specifically endorsed by the insurer, they will not be covered.
Ensure coverage matches global operations	It is important to consider territorial limits and jurisdictional exclusions across all policies. Confirm coverage extends to overseas trials, customers and subsidiaries. Assess compliance with foreign regulatory insurance requirements and arrange local or global programs where needed.	Some insurers limit cover to Australia and New Zealand or exclude the US due to litigation risk. Foreign regulations may impose additional requirements – e.g. the EU MDR[72] requires 'sufficient financial coverage' for liability.
Manage claims and notifications proactively	Organisations should implement internal escalation procedures for complaints, investigations, adverse events and potential circumstances which may give rise to claims. Notify insurers as soon as practicable of any circumstance that may give rise to a claim. Ensure compliance with all policy conditions.	Insurers write many policies on a claims-made basis. Timely notification of circumstances that may give rise to a claim is critical to preserving coverage.
Set adequate policy limits	Organisations should seek advice from their insurance broker to set policy limits. Consider excess or umbrella layers to protect against catastrophic losses. Review limits regularly as the business evolves.	Some policies aggregate multiple related claims into a single 'occurrence,' meaning one policy limit applies to what could otherwise be numerous claims. This may reduce deductibles but can be dangerous if limits are inadequate for mass claims. Where defence costs erode limits, prolonged litigation can quickly exhaust coverage and therefore an annual assessment of limits of insurance of each policy which forms the insurance program is essential.

Key contacts

Simone Mitchell
Life Sciences Sector Lead
M +61 407 234 079
Simone.Mitchell@minterellison.com

James Hutton
Health Industry Lead
M +61 416 197 158
James.Hutton@minterellison.com

David Taylor
Partner
M +61 423 182 320
E David.Taylor@minterellison.com

Jonathan Kelp
Partner
M +61 408 669 914
E Jonathan.Kelp@minterellison.com

Sonja Read
Partner
M +61 411 276 772
E Sonja.Read@minterellison.com

Zeina Milicevic
Partner
M +61 401 181 568
E Zeina.Milicevic@MinterEllison.com

Chelsea Gordon
AI Lead – Legal
M +61 413 804 145
E Chelsea.Gordon@minterellison.com

Kemsley Brennan
Partner
M +61 402 974 557
E Kemsley.Brennan@minterellison.com

About MinterEllison

MinterEllison is Australia's leading independent law firm enhanced by specialist consulting.

Our dedicated, full-service, multidisciplinary life sciences team advise across the life sciences product and business lifecycle – from concept to commercialisation, and beyond.

This report was prepared with contributions from Jaimie Wolbers, Rebecca Pereira, Jacky Wong, Jasper Choi, Laura Skazlic, Maria Rychkova, Fiona Chui, Mikah Pajaczkowska-Russell, Meghan Philp, Adam Karras and Sophie Whalley.