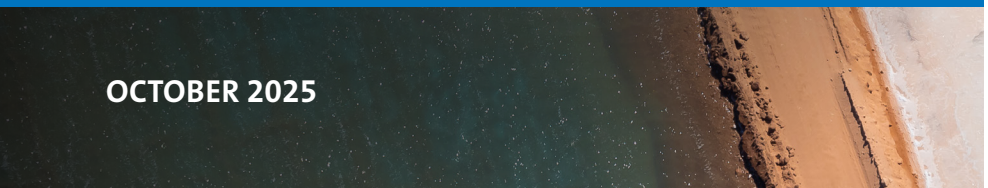
Allens

In alliance with Linklaters

Cyber resilience and incident response

A guide for healthcare sector organisations and boards



OCTOBER 2025

Healthcare is one of the most targeted sectors for cyber incidents, and their impact is typically more severe.

In Australia, the Genea, MediSecure, Medibank and Australian Clinical Labs cyber incidents have brought much-needed attention to the social impact that can result from the compromise of health information. Despite this, very little sector-specific guidance has been published about how healthcare providers should prepare for and respond to a major cyber incident that significantly impacts their operations.

It's a potentially life-threatening gap. The recent spike in ransomware attacks on healthcare providers and their suppliers globally has revealed the fragility of our digitally connected and highly fragmented healthcare ecosystem. It also demonstrates the disruptions to patient care that can occur if healthcare delivery organisations aren't operationally resilient.

In addition to facing the human consequences, healthcare providers that find themselves unable to withstand or recover quickly from a major cyber incident are likely to become fertile ground for rising class action activity and regulatory enforcement action.

Included in this guide

This guide seeks to assist organisations on their journey from existing legacy systems to more modernised service delivery. It contains tools to help healthcare providers and their boards:

1. navigate the complex regulatory landscape and understand their legal exposure
2. become operationally resilient
3. manage their supply chain
4. identify key governance red flags

all while investing in health services and technologies that can address inefficiencies and waste in the system, and unlock new models of healthcare.

Six reasons why cyber incidents proliferate in the healthcare sector

The healthcare sector has experienced the highest number of data breaches reported to the Office of the Australian Information Commissioner (the ***OAIC***) of all sectors in every one of its notifiable data breach (***NDB***) reports since the NDB scheme began in 2018.

The challenge of digital transformation in the healthcare sector is that technological advancements that enable better, more efficient and accessible patient care also increase the sector's vulnerability to attack. This is due to enhanced connectivity and breadth of access to systems, and the centralisation of sensitive data.

1 Criticality and continuity of care

The critical nature of healthcare services and low tolerance for operational disruption makes the healthcare sector a prime target for ransomware attacks, as organisations are more likely to pay ransom demands quickly to restore operations and meet continuity of care obligations.

> *[In the US], the healthcare and public health sector has been the most targeted critical infrastructure sector [by ransomware] since at least as far back as 2015.*[1]

2 High value of health (and other commercially sensitive) data

The specific characteristics of health information make it particularly valuable to cyber criminals. Health records contain comprehensive information about individuals that can be used for:

- identity fraud
- extortion
- fake insurance or payment claims
- accessing prescriptions or medical equipment
- other malicious activities.

This information is often difficult (if not impossible) to replace, meaning it retains value for longer. Biotechnology, pharmaceutical, research and life sciences organisations, and medical device manufacturers also hold *commercially valuable data,* such as medical research and development, intellectual property and trade secret information, which may motivate other threat actors such as insiders, corporate competitors and nation-state actors, to target systems or data.

> *Stolen health data sells for 10–20 times more than credit card information on the dark web (with some reports suggesting it sells for exponentially more), enabling cyber criminals to extract as much as US$[1000] per record.*[2]

Six reasons why cyber incidents proliferate in the healthcare sector

3 Large quantity of high-value health data

The adoption and upload of electronic health records by medical practices and hospitals, sometimes mandated by regulation and on a national level (eg upload by default in the My Health Record system), has boosted the quantity of health data available to cyber criminals.

Healthcare organisations also tend to hold on to health data for extended periods—sometimes *indefinitely* (which can be complicated by concepts of retaining data to ensure continuity of care).

> *On average, healthcare organisations secure 50% more sensitive data than the global average, making ransomware attacks more impactful.*[3]

4 Complex and interconnected systems and supply chain

As investment in modernisation increases, healthcare organisations are increasingly relying on more complex, interconnected systems, supply chains and vertically integrated care models across the industry.

These layers of connectivity can make it difficult for organisations to comprehensively secure their environment at scale.[4] Additionally the vulnerabilities that arise from inconsistent application of security practices across disparate systems, and reliance on multiple suppliers, creates additional entry points for attackers.

5 Insider threats

The volume of healthcare staff required to access sensitive information and connected systems increases the potential for privilege misuse.

When coupled with ineffective account management and user access controls to limit access to sensitive information and systems, and miscellaneous staff errors (often resulting from phishing and other social engineering attacks), it is unsurprising that insider threats—both intentional and inadvertent—are a leading cause of breaches in the healthcare sector.[5]

> *Almost 20% of a healthcare organisation's sensitive data holdings are affected by a successful ransomware attack, compared to just 6% at other organisations.*[6]

6 Outdated technology and rapid digital transformation

Many healthcare institutions rely on outdated technology and legacy systems, which do not have the same protections as modern technology/ systems, making this infrastructure more susceptible to attack.

The push towards digital transformation (through digital platforms, telehealth and increasing reliance on remote monitoring) has also led many healthcare providers to adopt new technologies quickly without fully addressing associated cybersecurity risks from an organisational perspective.

The regulatory landscape

Healthcare organisations need to navigate a growing patchwork of cybersecurity, data and AI regulatory regimes. They are also facing scrutiny from an expanding cohort of regulators.

Privacy and data handling

- Privacy Act, including APP 11.1 and 11.2[i] with further reforms to come
- Australian Consumer Law, including undisclosed data practices[ii]
- CPS 234 Information Security
- ASIC Act[iii]
- Spam Act
- Do Not Call Register Act and Telemarketing Standard
- Consumer Data Right[iv]
- Therapeutic Goods Act, regulatory marketing authorisations and advertising regulations[v]
- Over 800 federal and state laws imposing overlapping record retention and destruction obligations from Corporations Act to tax, employment, anti-money laundering and superannuation-specific legislation

Cyber incident response

- Privacy Act, including the NDB Scheme[vi]
- My Health Records Act[vii]
- Security of Critical Infrastructure Act[viii]
- Corporations Act, including reporting obligations, continuous disclosure obligations and directors' duties[ix]
- Terrorism financing, financial crime and sanctions laws[x]
- Competition and Consumer Act[xi]
- CPS 234 Information Security[xii]
- Cyber Security Act, including the mandatory ransomware payment reporting obligations[xiii]
- CPS 230 Operational Risk Management[xiv]
- Other healthcare sector-specific legislation/licences

Governance and risk management

- Privacy Act, including APP 1.2
- Corporations Act
- CPS 234 Information Security
- CPG 235 Managing Data Risk
- SPS 220 Risk Management
- Other Prudential Standards and Guidance
- Financial Accountability Regime Act 2023
- FIRB requirements[xvi]
- CPS 230 Operational Risk Management

Cybersecurity, data protection and operational resilience

- Privacy Act, including APPs 1.2,[xv] 11.1 and 11.2
- ASIC Act
- CPS 234 Information Security
- Security of Critical Infrastructure Act
- CPS 230 Operational Risk Management

KEY

- Privacy and marketing
- Security
- Corporations
- Financial services and regulatory
- Financial crime
- Health sector
- Consumer

Overview of key regulators and interest groups

Australian Government and regulatory bodies—general

- OAIC
- Australian Securities & Investment Commission (***ASIC***)
- Foreign Investment Review Board

Australian Government and regulatory bodies—healthcare sector specific

- Australian Digital Health Agency
- Therapeutic Goods Administration
- Australian Health Practitioner Regulation Agency
- Australian Commission on Safety and Quality in Health Care
- Aged Care Quality and Safety Commission
- Private Health Insurance Ombudsman
- Australian Organ and Tissue Authority
- Australian Radiation Protection and Nuclear Safety Agency
- Australian Research Council
- Cancer Australia
- National Blood Authority
- National Health and Medical Research Council
- National Health Funding Body
- National Mental Health Commission

State and territory governments

National Human Research Ethics Committee

Patient and consumer advocacy groups

Governance red flags

As healthcare providers strive to enhance their cyber resilience, it is essential to be aware of these governance red flags that could indicate potential vulnerabilities or areas in need of improvement.

- Cyber incident response documentation has not been reviewed and updated in over 12 months.
- An independent cybersecurity audit or assessment has not been conducted in over two years.
- Each of the cyber incident response team, executive leadership team and board have not participated in a cyber simulation in over 12 months.
- Role-appropriate cyber awareness, data governance and privacy training is not provided at least annually.
- Patient data is retained indefinitely.

Tip! *While there are often legitimate reasons for retaining data in certain forms (eg for clinical research, or to undertake comparative studies analysing conditions over time), it will rarely be the case that all records should be retained in all circumstances for all time.*

- There is unrestricted or widespread access to high-risk systems, accounts or patient data.
- There are no internal guardrails or frameworks to assess whether a particular technology use will be regulated (eg as a medical device).
- Strong Multi-factor Authentication (***MFA***) controls (or, where not feasible, strong compensating controls) are not implemented on high-risk accounts that provide access to sensitive information or critical systems.
- System accounts and/or credentials are shared openly or without additional controls.
- It is hard or impossible to quickly and accurately identify which individuals have accessed certain data or systems (and when).
- Role-based access controls and credential/password management requirements are not documented, enforced and periodically reviewed/audited.
- The organisation does not implement effective processes to ensure security alerts are proactively flagged to, and reviewed by, the IT security team.
- The organisation relies on legacy systems that are no longer supported by manufacturers, or does not have a security patch management framework.

What regulators expect *from boards*

> *It is ultimately the board's responsibility to ensure that management is fully across the cyber threat they face and, where necessary, takes appropriate action to ensure its entity remains cyber resilient.*[7]

Each of ASIC, the Australian Prudential Regulation Authority (***APRA***) and the OAIC has confirmed that boards are ultimately responsible for data and information security governance. Directors may also be personally liable for regulatory breaches (direct and ancillary):

- ☐ Active board-level oversight of cyber risk management—the board should regularly engage with, and receive reports from, management to facilitate a deep understanding of the cyber risks facing their organisation.

  Tip! *Directors should consider whether they understand cyber risks well enough to oversee and challenge the actions taken by management to mitigate these cyber risks.*

- ☐ The organisation's cyber risk appetite is defined and supported by an appropriate cyber governance and risk framework to identify, prepare for, manage and remediate cyber risks—including legal, regulatory compliance, technology, data, reputational and financial risks.

- ☐ The organisation can withstand and recover from a major cyber incident, with minimal impact on patients and other stakeholders.

  Tip! *Consider whether your organisation has current and comprehensive cyber incident response, business continuity and disaster recovery plans, which are regularly tested and updated.*

- ☐ Timely and adequate disclosures of cyber incidents, in line with regulatory obligations.

- ☐ Board-level oversight and support of key decision-making and responses—both during a significant cyber incident, and when dealing with the 'long tail' of post-incident risk.

  Tip! *Board-level reporting requirements should be balanced with the understanding that management will be under significant pressure and need to remain focussed on incident response. While the board should be informed of key actions, emerging/current risks and progress on critical issues, verbal briefings or email updates may be appropriate in lieu of extensive board papers.*[8]

- ☐ Board-level approval of out-of-cycle / extraordinary budget items and engagement with decisions on engagement with threat actors.

- ☐ The board and management undertake cybersecurity education and participate in testing, including scenario testing or incident simulations.

For more, see our *Insight*:
AICD's guide for directors on governing through a cyber crisis

What regulators expect *from organisations*

Healthcare organisations should ensure they can withstand and recover from a major cyber incident with minimal impact on patients and other stakeholders. Healthcare organisations should have current and comprehensive cyber incident response, business continuity, and disaster recovery plans, which are regularly tested and updated.

Regulators expect that your organisation...

- ☐ Has an overarching, documented, cyber governance and risk framework or program to assess cybersecurity risk, and improve cybersecurity posture and preparedness for a cyber incident.
- ☐ Regularly monitors and reports on compliance with this framework, and there is both board and management-level oversight and accountability over the whole program.
- ☐ Maintains a detailed, up-to-date inventory of technology assets and critical operations, and understands the movement of patient data (and other valuable information) throughout these systems, who has access, and how they are protected.

  Tip! *A failure to understand where sensitive or valuable data resides can result in a lack of cybersecurity awareness and, accordingly, a lack of investment in cybersecurity infrastructure.*

- ☐ Ensures appropriate technical and operational controls are implemented, documented and regularly tested to assess the overall efficacy of those controls and documentation.

  Tip! *It can be difficult for entities to track whether security measures have been appropriately implemented, are being adhered to in practice, and the efficacy of these controls, if this documentation is lacking.*

- ☐ Is not overly reliant on the cybersecurity controls of key service providers.
- ☐ Is able to withstand and recover from disruption and ensure continuity of key services with minimal impacts to patients / consumers.
- ☐ Has systems in place to quickly identify and internally escalate issues, and to notify relevant regulators and other key stakeholders where required.
- ☐ Maintains a comprehensive record-retention and destruction program.
- ☐ Manages third-party risk throughout the lifecycle of arrangements, including by conducting due diligence / classifying third-party risks, setting baseline technical and operational requirements, applying compensating controls and monitoring compliance on an ongoing basis.
- ☐ Reinforces the importance of cybersecurity as a collective responsibility.
- ☐ Ensures its people are aware of its controls, policies and processes, supported by regular roles-based training.
- ☐ Invests in adequate resourcing (staff and tools) and appropriate IT infrastructure to manage and mitigate technology and cyber risks.
- ☐ Leverages data assets and artificial intelligence in a compliant and ethical manner.

Getting operationally resilient

Operational resilience is the ability to maintain critical operations during, respond effectively to, and recover quickly from, disruptive events.

Healthcare organisations are experienced at designing and implementing sophisticated systems and processes for risk identification, health quality and safety management. However, organisations must continue to ensure they are operationally resilient.

1. Maintain an up-to-date, fit-for-purpose operational risk assessment

This should involve an assessment of:

- the operational risks (threats and vulnerabilities) your organisation faces
- the operational, financial, legal and reputational impacts, should those cyber risks eventuate
- the effectiveness of current operational and technical controls.

Enterprise-wide risk assessments should be undertaken routinely (including following changes to the threat landscape, information assets and the regulatory environment) to ensure they remain accurate and up-to-date. Targeted risk assessments should be undertaken for strategic decisions or business activities (eg for entry into a new jurisdiction, acquisition of a company or a new business arrangement).

Tip! *APRA's new Prudential Standard CPS 230 (Operational Risk Management) provides a useful blueprint of some of the governance and supplier uplifts that healthcare organisations can take to optimise operational resilience.*

2. Set (and monitor compliance with) tolerance levels for disruption to critical operations

For each critical operation, consider the maximum period of disruption, maximum extent of acceptable data loss, and minimum service levels for alternative arrangements. Regularly reassess the adequacy of tolerance levels.

3. Identify and eliminate single points of failure in your supply chain

Consider arrangements with multiple alternative suppliers to diversify your risk. Develop contingency plans where there is a lack of suitable alternatives to critical healthcare suppliers.

Tip! *Ask:*

- *Do we have an up-to-date map of our data, critical operations, technology assets and inventory of suppliers?*
- *Do we have a supplier risk management policy?*
- *Do we authenticate, log, monitor and audit access to systems and data by supply chain vendors?*
- *Do we have appropriate frameworks to identify and manage AI procurement risks?*
- *What controls are in place to minimise patient/stakeholder impacts when the information security of one (or more) of our suppliers is compromised?*

4. Assess how your operational risk management framework is operating in practice

Operating effectiveness is as important as design effectiveness. Your framework should include processes to monitor, test and report on compliance with that framework, including by independently validating that staff are adhering to documented processes, and relevant controls being implemented and operating as intended.

5. Maintain an up-to-date register of critical operations and suppliers

This register should outline critical operations and suppliers, which—if disrupted—would have an adverse impact on patients and other stakeholders.

Tip! *For each critical operation, establish an associated disruption tolerance level (defining levels for the maximum period of time your organisation could tolerate a disruption, and minimum service levels that would need to be maintained while operating alternative arrangements during a disruption).*

Getting operationally resilient

6. Ensure adequate resources and capabilities

Ensure there is appropriate access to the people, resources and technology needed to maintain disrupted critical operations within approved tolerance levels, recover quickly and remediate the root cause of any issues.

7. Document, test and update business continuity controls and processes

Test these against a range of severe but plausible scenarios, including disruptions to services provided by material service providers and scenarios where contingency arrangements are required. Protect your backups.

8. Prepare for ransomware

Treat ransomware as an inevitability, and ensure you understand the impact of system failures and data loss (whether your own or that of your suppliers) on patients and your business.

Tip! *Find out how long it will take to restore systems from backup, the legality of paying a ransom demand, delegations and approval requirements, the scope of your insurance coverage, how you will engage with regulators and other government agencies, and how you will manage communications with key stakeholders.*

9. Consider AI safety and security

When using AI in connection with optimising workflow, clinical decision support or patient care, or using data in connection with the development of AI tools, consider evolving AI-specific regulation, industry standards and community expectations.

Tip! *AI governance measures should include or involve:*

- *processes to assess new AI use cases through an ethical and reputational lens*
- *particular care in relation to use cases involving sensitive information*
- *tracking both general and sector-specific AI regulatory developments*
- *preparedness to respond to—and withstand—serious AI incidents, system weaknesses and malfunctions.*

Key baseline technical controls

In recent enforcement action, the OAIC highlighted certain technical deficiencies as potential indicia of organisational failures to take reasonable steps to protect personal information from unauthorised access and disclosure.

This signals the types of baseline technical controls the OAIC (and other regulators) expect.

Password complexity controls and monitoring

Prevent the use of insecure or common passwords and/or re-use of passwords across multiple accounts. Monitor and review processes to ensure passwords used to access important data repositories and/or servers are encrypted and not stored in plain text.

Authentication and user access controls—including MFA and other controls to authenticate users, devices and other assets at a level commensurate with risk.

Account management controls to identify and revoke access for dormant accounts and users.

Privileged access management

Restrict privileges to information assets in accordance with the principle of least privilege, and ensure user access controls and permissions are regularly audited.

Security logging in accordance with recognised standards.

Detect and respond to information security incidents—including ensuring that the organisation:

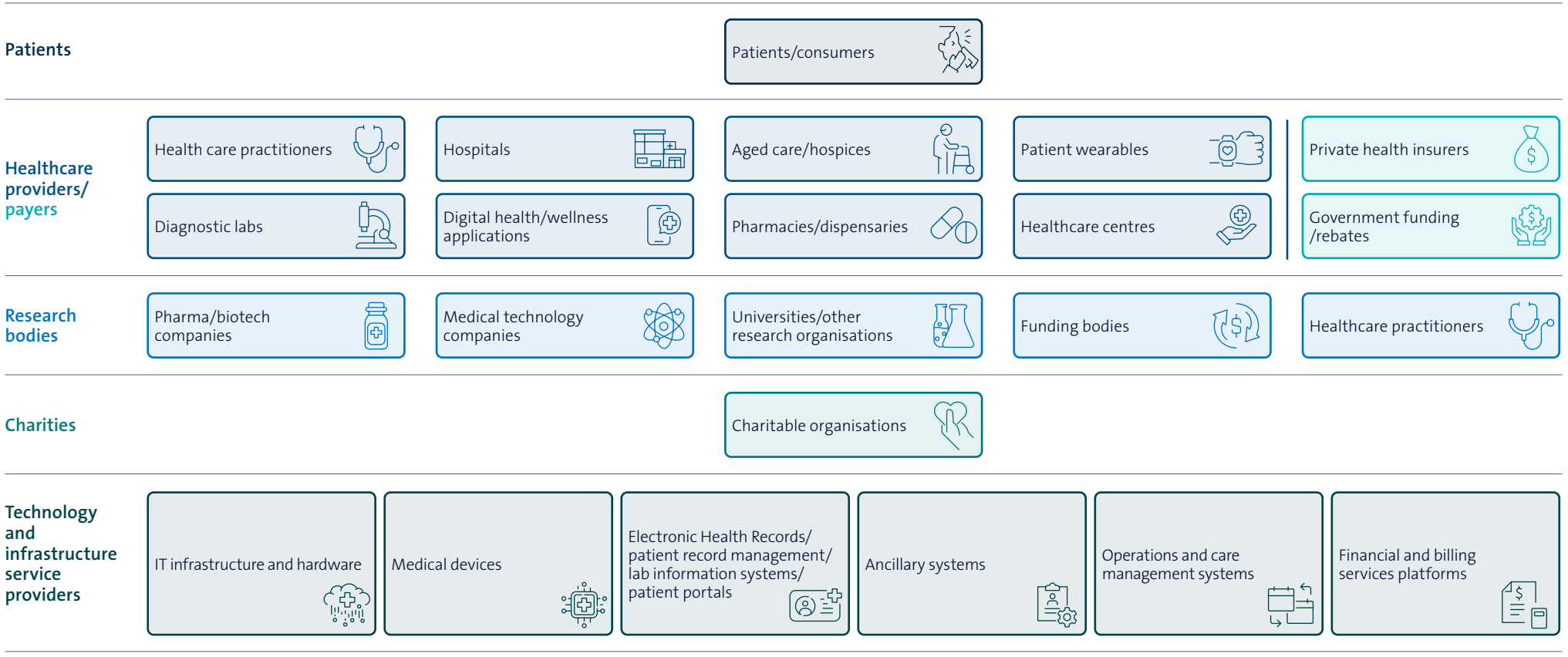
1. undertakes first-level review and triage of all security alerts generated by end-point detection and response software
2. has clear, documented guidance for escalating security alerts
3. configures volumetric alerts for exfiltration of large or abnormal volumes of data from servers used to connect to critical information assets.

For more, see our *Insight*: Comparative review of security measures

Spotlight: managing your supply chain

Supply chain attacks exploit vulnerabilities in vendors with weaker security controls to infiltrate other organisations. Unfortunately, these attacks are particularly prevalent in the healthcare sector due to its complex and interconnected network of stakeholders, systems and supply chains. This connectivity can leave organisations vulnerable if security practices are not comprehensively managed across the entire ecosystem.

Healthcare ecosystem



Key contacts

Valeska Bloch
Partner and Head of Cyber
T +61 2 9230 4030
Valeska.Bloch@allens.com.au

Phil O'Sullivan
Partner and Health Sector Leader
T +61 2 9230 4393
Phil.O'Sullivan@allens.com.au

David Rountree
Partner
T +61 7 3334 3368
David.Rountree@allens.com.au

Isabelle Guyot
Partner
T +61 2 9230 4752
Isabelle.Guyot@allens.com.au

Nick Li
Senior Associate
T +61 3 9613 8009
Nick.Li@allens.com.au

Maddison Ryan
Senior Associate
T +61 3 9613 8340
Maddison.Ryan@allens.com.au

Our latest thinking on cyber

Defending from within: a guide to insider threat management

A step-by-step guide to assessing compromised data after a cyber incident

Why organisations must embed mental health and wellbeing support into cyber incident response planning

Establishing and preserving legal professional privilege in a cyber incident

End notes

1. United States of America, Department of Health and Human Services, HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, Federal register/Vol. 90, No.3 (HIPAA Proposal Paper), page 912–913.
2. Fierce Healthcare, Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web; HIPAA Proposal Paper, page 912–913.
3. TechTarget, Healthcare organizations secure 50% more sensitive data than global average.
4. For more on these risks, see Pulse: Unexpected risks of the IoT revolution: Cyber security in medical devices.
5. For more on insider threats, see Defending from within: a guide to insider threat management.
6. Rubrik Zero Labs, The State of Data security: Measuring your data's risk.
7. AICD, Governing Through a Cyber Crisis—Cyber Incident Response and Recovery for Australian Directors.
8. APRA, Improving cyber resilience: the role boards have to play.

Australian legislation overview

i **Australian Privacy Principle (APP) 11.1**—obligation to destroy and de-identify personal information; **APP 11.2**—obligation to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.

ii **Australian Consumer Law *(ACL)*** contained in Sch 2 of the *Competition and Consumer Act 2010* (Cth)—the Australian Competition and Consumer Commission has a broad remit to investigate 'undisclosed data practices'—bringing a sharp focus on transparency of data practices.

iii ***Australian Securities and Investment Commission Act 2001* (Cth) ss12DA and 12DB**.

iv **Consumer Data Right**, established through Part IVD of the *Competition and Consumer Act 2010* (Cth)—the regime was slated to be rolled out to insurance—although it is unclear when this will occur following the consultation on proposed changes to the regime last year.

v Advertising in the healthcare sector is subject to several layers of regulation and industry self-regulation.

For example: (1) the ACL prohibits false, misleading or deceptive representations about goods and services including in advertising; (2) therapeutic goods legislation regulates direct-to-consumer advertising; (3) State-based Health Practitioner National Law imposes restrictions on advertising of health services; (4) advertising to healthcare professionals with respect to medicines and medical devices are subject to industry self regulation by Medicines Australia (MA) and the Medical Technology Association of Australia (MTAA); and (5) Codes administered by the Australian Association of National Advertisers (AANA) also apply to advertising directed to consumers for therapeutic goods and healthcare services.

vi ***Privacy Act 1988* (Cth)**, **Part IV Notifiable Data Breach Scheme**—mandatory notification to OAIC/individuals when a data breach is likely to cause serious harm.

vii ***My Health Records 2012* (Cth)**—notification to the Australian Digital Health Agency of potential or actual My Health Record data breaches.

viii ***Security of Critical Infrastructure Act 2018* (Cth)**—SOCI bound entities must notify the ACSC within 12 hours of a cyber incident with a significant impact, or within 72 hours of a cyber incident with a relevant impact.

ix ***Corporations Act 2001* (Cth) ss180**, **181** duties of directors; **ss292**, **299** reporting obligations; **s674A** continuous disclosure obligations.

x Organisations must not make payments to a threat actor or deal with assets if the threat actor is a designated person or entity (eg *Criminal Code Act 1995* **(Cth)**, State based crimes acts, *Proceeds of Crimes Act 2002* (Cth), *Autonomous Sanctions Act 2011* (Cth), *Charter of the United Nations Act 1945* (Cth)).

xi ***Competition and Consumer Act 2010* (Cth) s18**—prohibition on misleading and deceptive conduct.
Tip! Consider disclosures/statements made in the wake of a cyber incident.

xii ***CPS 234* paragraphs 35 and 36**—notification to APRA: (i) as soon as possible (or within 72 hours) after becoming aware of an information security incident that materially affected, or had the potential to materially affect the entity or the interests of its customers, or which has been notified to another regulator; or (ii) within 10 days of becoming aware of a material security control weakness that it cannot remediate in a timely manner.

xiii ***Cyber Security Act 2024* (Cth)**—reporting business entities must report ransomware and cyber extortion payments within 72 hours of making the payment or becoming aware that a payment has been made. Obligations will commence on 29 May 2025. Consultation for the content of any mandatory report closed in February 2025.

xiv ***CPS 230 (Operational Risk Management)* paragraph 33**—notification to APRA as soon as possible (or within 72 hours) after becoming aware of an operational risk incident that is likely to have a material financial impact, or a material impact on the organisation's ability to maintain critical operations.

xv **APP 1.2**—obligation to put in place policies, procedures and practices to ensure compliance with APPs.

xvi In the healthcare sector it is important to consider rules relating to foreign investment.