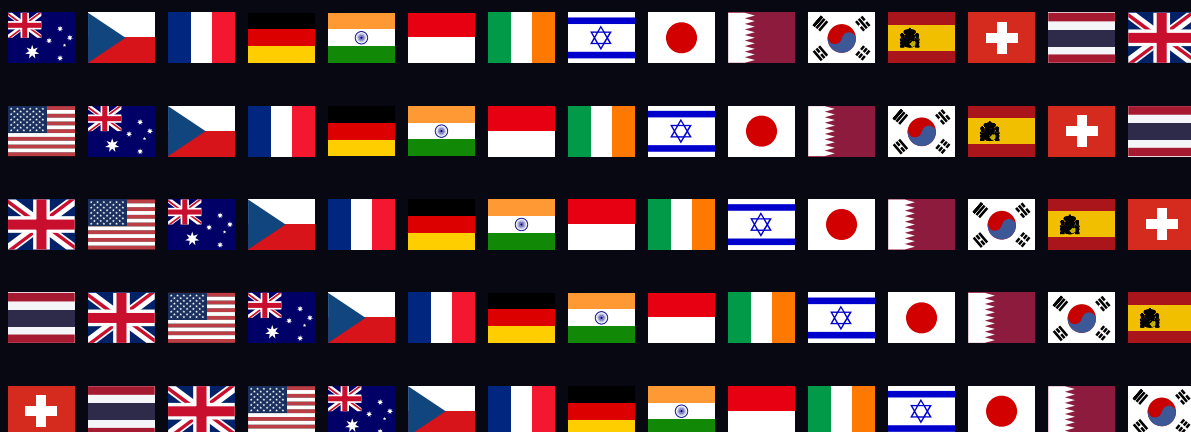


DIGITAL HEALTH

Australia



Digital Health

Consulting editors

Eveline Van Keymeulen, Oliver Mobasser, Samantha Peacock, Sara Patel, Brett Shandler

Latham & Watkins LLP

Quick reference guide enabling side-by-side comparison of local insights, including market overview; legal and regulatory framework; data protection and management; intellectual property rights, licensing and enforcement; advertising, marketing and e-commerce; payment and reimbursement; and recent trends.

Generated 27 January 2023

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. © Copyright 2006 - 2023 Law Business Research

Table of contents

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

Investment climate

Recent deals

Due diligence

Financing and government support

LEGAL AND REGULATORY FRAMEWORK

Legislation

Regulatory and enforcement bodies

Licensing and authorisation

Soft law and guidance

Liability regimes

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

Data protection law

Anonymised health data

Enforcement

Cybersecurity

Best practices and practical tips

INTELLECTUAL PROPERTY

Patentability and inventorship

Patent prosecution

Other IP rights

Licensing

Enforcement

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

e-Commerce

PAYMENT AND REIMBURSEMENT

Coverage

UPDATES AND TRENDS

Recent developments

Contributors

Australia



Susan Jones
sejones@gtlaw.com.au
Gilbert + Tobin



John Lee
jlee@gtlaw.com.au
Gilbert + Tobin



Andrew Hii
ahii@gtlaw.com.au
Gilbert + Tobin



Kevin Ko
kko@gtlaw.com.au
Gilbert + Tobin



MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

Key players include:

- the Australian government, which has provided A\$503 billion for healthcare in the 2022 government budget. The federal government funds health services through the Department of Health, the Therapeutic Goods Administration, the Medical Research Future Fund (MRFF) and the Australian Digital Health Agency (ADHA), which is responsible for the National Digital Health Strategy and Framework for Action and operates My Health Record, an online platform that aggregates an individual's key health information and provides interoperability between clinical information systems across the health sector;
- state and territory governments, which among other things operate Australia's public hospitals, including emergency departments and ambulance services;
- private healthcare businesses, including operators of private hospitals, day surgeries, primary and referred care clinics and imaging and pathology services;
- healthcare professionals;
- developers and suppliers of digital health systems;
- private health insurers;
- venture capital and private equity funds;
- academic institutions, especially the Commonwealth Scientific and Industrial Research Organisation and universities;
- a range of cross-sector innovation and commercialisation bodies, including ANDHealth, the Digital Health Cooperative Research Centre and MTPConnect; and
- industry associations, including the Medical Software Industry Association, the Medical Technology Association of Australia, AusBiotech, BioMelbourne Network and the Australasian Institute of Digital Health.

Participants in the healthcare industry (government and private) are increasing their adoption of digital health technologies to improve health outcomes, meet the needs of their stakeholders and respond to various health system issues (eg, increasing rates of chronic conditions, emphasis on prevention, management and in-home care, focus on value-based healthcare, declines in private health insurance, crisis in aged care, inequality in access to health services, hospital waiting times and budget pressures). Key areas of focus include telehealth and virtual health services (including for mental health and aged care), artificial intelligence (AI), interoperability, health informatics, payments and e-referral and booking.

Law stated - 08 December 2022

Investment climate

How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

Over the past decade, the private health sector has led developments in the digital health industry. However, federal, state and territory government-funded investments have significantly increased over the past few years. The covid-19 pandemic, the 2019–2020 bushfires, the Royal Commission into Aged Care Quality and Safety and the Productivity

Commission's report into Mental Health have all accelerated investment in digital health and greater coordination between governments and private sector participants. The Australian government estimates that it delivered 10 years of reform in 10 days with the 2020 introduction of whole-of-population access to telehealth under Medicare.

The covid-19 pandemic-driven focus on the need to shift patients out of physical sites, unless totally necessary, has created a more agile and responsive Australian healthcare system, and this shift requires ongoing investment into the development and implementation of new technologies. ANDHealth, one of Australia's leading health technology commercialisation organisations, stated in its 2022 report on the state of the Australian digital health sector – The Awakening Giant: The Rise of Australia's Evidence-Based Digital Health Sector – that while there has been a 20-fold increase in global investment in the digital health sector in the past decade, 2022 has seen global digital health funding slow down, in line with the state of the macroeconomic environment.

However, the key challenge in the Australian digital health industry remains funding and access to capital to drive the commercialisation of innovations. This has been particularly relevant in respect of foreign investment following temporary restrictions that were implemented in the Australian foreign investment regime in response to the covid-19 pandemic. Although many of these restrictions were lifted on 1 January 2021, foreign investment continues to be a key regulatory hurdle, particularly in relation to digital health investments with material technology or data assets.

Lack of reimbursement also remains another significant challenge for investment in digital health. Broader reimbursement of telehealth as a model of care and a clear regulatory landscape for Software as Medical Device products are a large step forward for the growth of Australia's domestic digital health industry. However, there are many other types of solutions in the sector that currently have no defined or well-understood reimbursement pathway. The industry has identified current nonspecific healthcare reimbursement policies as a substantial barrier to the commercialisation and implementation of digital health technologies, specifically in the areas of digital medicine and digital therapeutics.

Law stated - 08 December 2022

Recent deals

What are the most notable recent deals in the digital health sector in your jurisdiction?

In the private sector:

- in September 2022, Australian Securities Exchange (ASX)-listed company Advanced Human Imaging Ltd announced it had entered into an arrangement agreement to acquire all outstanding shares of Canadian company wellteq Digital Health Inc. The shareholders of wellteq Digital Health Inc and the Supreme Court of British Columbia approved the plan of arrangement in November 2022 and completion occurred in early December 2022;
- in September 2022, Pfizer acquired ASX-listed, University of Queensland startup ResApp Health Limited for A\$179 million. ResApp Health Limited has developed smartphone technology to diagnose and measure the severity of respiratory diseases based on analysis of a patient's cough;
- in August 2022, biotech investor Dr Glenn Haifer and Ampersand Capital Partners, a global healthcare private equity firm, acquired AcuraBio (formerly Luina Bio), a leading Australian biopharmaceutical contract development and manufacturing company, for an undisclosed amount;
- in August 2022, private equity firm Adamantem Capital acquired 100 per cent of the share capital in GenesisCare's cardiology businesses – Genesis Heart Care Pty Ltd and Genesis Sleep Care Pty Ltd – for between A\$200 million and A\$250 million;
- in July 2022, private equity firm Pemba Capital Partners acquired the group of companies operating as SACARE, a leading South Australian operator of supported accommodation and care services for people living with a

complex disability, for an undisclosed amount;

- in July 2022, equity firm BGH Capital completed its successful off-market cash takeover of in vitro fertilisation provider Virtus Health for A\$697 million;
- in April 2022, Cochlear announced its intention to acquire hearing solutions provider Oticon Medical for approximately A\$170 million. On 1 December 2022, the Australian Competition and Consumer Commission (ACCC) announced it has significant preliminary competition concerns in relation to the proposed acquisition. The ACCC's provisional date for the announcement of its decision is 16 March 2023;
- in January 2022, the bioanalytical laboratory business Agilex Biolabs was acquired by Australian healthcare company Healius for an enterprise value of A\$301.3 million;
- in December 2021, healthcare AI company Harrison.ai raised A\$129 million in one of the largest Series B funding rounds ever for an Australian startup (Harrison.ai previously raised A\$60 million in a A\$40 million Series B funding round and A\$20 million investment by I-MED Radiology in June 2021, and A\$29 million in a Series A funding round in December 2019). In June 2022, Harrison.ai also formed a joint venture with Sonic Healthcare, one of the world's largest medical diagnostics providers, to develop and commercialise new clinical AI solutions in pathology;
- in November 2021, Australian medical technology company Artrya Limited was listed on the ASX after it raised A\$40 million in an initial public offering. Artrya Limited has developed AI-based software solutions for non-invasive diagnosis of coronary artery disease, such as its software-as-a-medical-device, Artrya Salix;
- in November 2021, The Citadel Group acquired medical practice management technology company Genie Solutions for an undisclosed sum, thought to be in the range of A\$260 million; and
- in September 2021, Atmo Biosciences secured A\$9.6 million in an oversubscribed capital raise.

In the public sector:

- in March 2022, the Australian government announced an investment of A\$107.2 million to modernise the Australian healthcare system. This includes A\$72 million towards the transformation of health payments and services, A\$32.3 million towards the 2018–2022 Intergovernmental Agreement on National Digital Health and A\$2.9 million towards the Australian Institute of Health and Welfare to safeguard national health data; and
- in the second half of 2021, Western Sydney Local Area Health District selected a joint venture between Calvary and Medibank to provide hospital-in-the-home services to help it manage the surge of patients with coronavirus.

Law stated - 08 December 2022

Due diligence

What due diligence issues should investors address before acquiring a stake in digital health ventures?

Key issues in due diligence include:

- understanding how the company complies with Australian privacy and data regulations (which are particularly important for healthcare companies given the sensitivity of the information being handled), including protecting data assets and flows critical to the company's operation; and
- ensuring that a company has the necessary ownership or rights to use information technology that is key to the business, including necessary rights to license its products commercially.

Specifically, we recommend addressing the following due diligence issues:

- **privacy:** ascertain whether a company's privacy policies provided to customers upon collection of personal information are compliant with the Privacy Act 1988 (Cth) (the Privacy Act) and the Australian Privacy Principles (APPs). Specifically, consider compliance with requirements regarding obtaining consent for the collection of sensitive information (which includes health information). We note that the Australian government is currently reviewing the Privacy Act, and that these reforms are expected to increase the privacy protections afforded to individuals;
- **data:** report on the types of data (including personal information and sensitive information) collected and held by the company and how this data and personal information is obtained and used by the company, to ensure compliance with the APPs. Report on any transfers of personal information or data-sharing relationships, including any arrangements for the outsourcing of data-processing activities and any disclosure of data and personal information overseas, to ensure compliance with APP 8;
- **cyber security:** report on any information security or cyber incidents, regulatory investigations and complaints regarding the company's privacy handling or marketing activities that have taken place in the past five years, as well as undertaking an assessment of a company's cyber security measures and whether the company has policies and procedures in place to respond to any cyber security incident or breach. Assess whether the company is subject to the recently amended Security of Critical Infrastructure Act 2018 (Cth) (the SOCI Act) (which captures certain entities in the health care and medical sector) and if so, review the company's preparedness with respect to compliance with the SOCI Act (eg, identification of relevant assets, development of risk management and incident notification plans (eg, the Critical Infrastructure Risk Management Program)), review and amendment of material contracts to address compliance obligations (eg, to address the government's rights to require access to information, or to give directions or exercise step-in rights); and
- **ownership of key IT systems:** review any material IT agreements (including software licensing agreements) entered into by the company. Report on the key information technology (including any products, hardware and software) or third-party services used by the company to assess whether it has ownership of or right to use such information technology.

Law stated - 08 December 2022

Financing and government support

What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

There are no financing structures that are unique to digital health ventures in Australia; financing structures are determined largely based on more typical considerations regarding the financial profile of the relevant target (eg, what stage the relevant target is at in its life cycle).

Australian government initiatives include:

- the decision to support the delivery of telehealth under the Medicare Benefits Schedule and electronic prescriptions and home delivery of medications because of the covid-19 pandemic;
- the continued investment in the Health Delivery Modernisation Program, to deliver Australia's Long Term National Health Plan. In the 2022–23 budget, the Australian government committed to investing A\$72 million to modernise Australia's health system, including delivering innovative new digital health services and commencing the transformation of health payments and services towards a more streamlined, digital model. More health services will be made available digitally, including Medicare enrolment and re-enrolment, and the Pharmaceutical

Benefits Scheme written authority approval;

- the MRFF is an ongoing research fund valued at A\$20 billion in July 2020. Its priorities for 2020 to 2022 include digital health tools. It invests in all research stages including the final commercial product;
- the ADHA is tasked with improving health outcomes through the delivery of digital healthcare systems. It operates the My Health Records system and promotes its use by developers of digital health products and services. The ADHA is also tasked with overseeing electronic prescriptions and telehealth;
- the Digital Health Cooperative Research Centre operates through collaborative R&D programmes between government, industry and academia to foster new companies and products, a new digital health workforce and forge new national and international partnerships;
- the R&D tax incentive provides a tax offset for eligible R&D activities. It has two core components: a refundable tax offset for certain eligible entities whose aggregated turnover is less than A\$20 million and a non-refundable tax offset for all other eligible entities; and
- the 'Early stage venture capital limited partnerships' programme helps fund managers attract pooled capital so they can raise new venture capital funds of between A\$10 million and A\$200 million to invest in innovative Australian early stage businesses, offers tax benefits to fund managers and investors and connects investors with early-stage businesses.

Law stated - 08 December 2022

LEGAL AND REGULATORY FRAMEWORK

Legislation

What principal legislation governs the digital health sector in your jurisdiction?

The legislation that governs competition in the digital health sector is the Competition and Consumer Act 2010 (Cth) (the CCA), which is the standard competition law framework in Australia. The CCA also includes the Australian Consumer Law (the ACL), which covers consumer protection issues. There are no special rules for the digital health sector.

Additional key legislation includes the Therapeutic Goods Act 1989 (Cth) (the TGA Act), which regulates all therapeutic goods, that is medical devices, medicines (including complementary, over-the-counter and prescription), the Therapeutic Goods Regulations 1990 (Cth) , and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations). The TGA Act was updated in 2021 to address the increase in medical-related software-based products being developed. The TGA Act includes new classification rules for software-based medical devices, including for those that provide a diagnosis for health conditions, monitor the state of health conditions, specify a treatment or provide therapy. The reforms also amend the 'Essential Principles' – the requirements relating to the safety and performance of medical devices – in relation to cyber security, the management of data and information, and requirements relating to the development, product and maintenance of medical devices. These changes have brought Australia's approach into alignment with those of our key trading partners.

Digital health technologies that collect personal information will also need to comply with Australia's privacy laws as set out in the Privacy Act 1988 (Cth) (the Privacy Act). As health information is highly sensitive personal information, the Privacy Act includes more robust protections around its collection and handling by all organisations that provide a health service and hold health information. The Office of the Australian Information Commissioner (OAIC) also regulates the treatment of health information contained in individuals' health records (My Health Record) and healthcare identifiers operated by Medicare. The operation of the My Health Record scheme is governed by the My Health Records Act 2012 (Cth) .

Law stated - 08 December 2022

Regulatory and enforcement bodies

Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

The Australian Competition and Consumer Commission (ACCC) enforces the CCA in Australia. The ACCC has a Digital Platforms Branch responsible for the ACCC's ongoing scrutiny of digital platform markets. Although the ACCC's investigations and inquiries into digital platforms are not specifically focused on the digital health sector, the outcomes of the ACCC's enforcement and regulatory actions do have implications for digital health businesses.

The TGA regulates medical devices, including software as a medical device, such as software that uses information about symptoms to make a diagnosis, and mobile apps coupled with devices for calculating medication dosages.

The OAIC enforces compliance with the Privacy Act and other privacy laws, in particular, to ensure the proper handling of personal information, including regulating the treatment of health information contained in individuals' health records (My Health Record) and healthcare identifiers operated by Medicare.

In June 2022, the Australian government formed the Digital Platform Regulators Forum, which comprises:

- the ACCC;
- the OAIC;
- the Office of the eSafety Commissioner; and
- the Australian Communications and Media Authority (ACMA).

The ACMA is also likely to become a more prominent regulator in digital health, after its March 2022 report on the adequacy of digital platforms' disinformation and news quality measures. ACMA's report found that the propagation of falsehoods and conspiracies undermines public health efforts and impacts business. Following the report, the Australian government announced its intention to provide the ACMA with new powers to combat harmful disinformation and misinformation.

Law stated - 08 December 2022

Licensing and authorisation

What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

Generally, therapeutic goods, including digital medical devices, need to be registered on the Australian Register of Therapeutic Goods (ARTG) prior to being sold in Australia. For example, software that meets the definition of a 'medical device' under the TGA Act needs to be registered on the ARTG before it can be supplied. Accordingly, the impact of regulation under the TGA Act should be considered by inventors in the early stages of product development.

Law stated - 08 December 2022

Soft law and guidance

Is there any notable 'soft' law or guidance governing digital health?

In Australia, there are no guidelines on the application of competition law specific to digital health markets. The ACCC's approach to competition law generally is reflected in various guidelines including its merger guidelines and authorisation guidelines (merger and non-merger), misuse of market power guidelines and concerted practices

guidelines.

The ACCC (together with state and territory consumer protection agencies) has also developed several practical guidelines on consumer protection issues such as unfair business practices, consumer guarantees, consumer product safety and sales practices.

The Australian Digital Health Agency (ADHA) is responsible for the development and operation of a national digital health strategy, as well as the development and implementation of specifications and standards in relation to digital health. Additionally, the ADHA has developed a Cyber Security Strategy for 2022-2025, which aims to uplift capability within the ADHA in response to the changing cyber environment. The ADHA publishes guides and other resources that may be relevant to providers of digital health products and services.

The TGA provides guidance in relation to the regulation of software-based medical devices to assist manufacturers and sponsors to understand the TGA Act's regulation of such devices (see 'Regulation of software based medical devices'). It also provides guidance for patients and consumers, among others, to inform them about the potential cyber security risks that may arise with connected medical devices (see 'Medical device cyber security information for users - Guidance for patients and consumers').

Law stated - 08 December 2022

Liability regimes

What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

In consumer protection, the ACL applies to digital health goods and services, including as follows:

- it prohibits misleading or deceptive conduct and false or misleading representations made in the course of advertising goods or services. The maximum penalty for making a false or misleading statement was substantially increased in October 2022 and is now the greater of:
 - A\$50 million;
 - three times the value of the benefit obtained from the breach; or
 - if that cannot be calculated, 30 per cent of adjusted turnover over the period that the breach occurred, with a minimum of 12 months;
- it grants automatic quality guarantees to consumers of goods or services. It also requires suppliers (and in some cases manufacturers) to remedy a failure to comply with the guarantees and to compensate consumers for reasonably foreseeable loss caused by the failure;
- it also enables plaintiffs to recover losses from manufacturers that supply products with safety defects;
- it sets out an 'unfair contract terms' regime that governs terms contained in standard-form consumer or small business contracts. In October 2022, Parliament passed the Treasury Laws Amendment (More Competition, Better Prices) Bill 2022 (Cth), which will make unfair contract terms unlawful and subject to civil penalties from November 2023 (currently, they are only rendered void); and
- consumers may bring actions for misleading or deceptive conduct, consumer guarantee failures or product safety breaches as a class.

In the context of the TGA Act, to be able to import and supply a medical device in Australia, the medical device is required to meet the Essential Principles for safety and performance. Failure to meet the Essential Principles can result in civil or criminal penalties under the TGA Act. The Essential Principles require the minimisation of risks associated

with the design, long-term safety and use of the device, which implicitly includes the minimisation of cybersecurity risks.

Law stated - 08 December 2022

DATA PROTECTION AND MANAGEMENT

Definition of 'health data'

What constitutes 'health data'? Is there a definition of 'anonymised' health data?

Health data includes:

- information or an opinion about an individual's health or any health services provided, or to be provided, to the individual;
- any personal information collected to provide or in providing a 'health service' to an individual (including organ donation); and
- genetic information about an individual that is in a form that could be predictive about the health of an individual (or relative of the individual).

The concept of 'providing health services' is very broad and can capture a range of services that may not be front of mind when thinking about health – for example, information collected by a gym on an individual in connection with a gym class, or Medicare billing information held by an insurance provider or debt collector.

Anonymised health data is not defined, although the Australian Privacy Principles (APP) Guidelines state that 'anonymity' means that an individual dealing with an entity cannot be identified. Critically, health data that may be anonymous in the hands of one entity may not be anonymous in the hands of another. The ability of an entity to link a data set with other information is relevant to whether data is truly anonymised.

Law stated - 08 December 2022

Data protection law

What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Given the sensitivity of health information, its collection, use and management are regulated by the Privacy Act 1988 (Cth) (the Privacy Act).

Health data is treated more strictly than personal information under the Privacy Act. Health data is a subset of 'sensitive information' and consent is required for its collection.

Generally, an organisation can collect health data from a person if:

- the person provides their consent (express or implied); and
- the information is reasonably necessary for the organisation's activities.

Implied consent arises when consent can be inferred from the circumstances and conduct of the person providing the health information. This is a higher test than that imposed on other personal information. The Australian government is currently undertaking a review of the Privacy Act. As part of this review, the government is considering updating the

definition of 'consent' to be voluntary, informed, current, specific, and an unambiguous indication through clear action.

APP 11 requires entities to take reasonable steps to protect personal information (including sensitive information, such as health information) it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. According to the Office of the Australian Information Commissioner (OAIC) APP Guidelines, 'reasonable steps' will depend on the circumstances in each particular case and may include governance, culture and training, internal practices, procedures and systems, information and communications technology security, access security, and destruction and de-identification.

In addition, the handling of health information is also subject to certain state-based legislation, which differs from the Privacy Act in some aspects, but the differences are relatively minor.

Law stated - 08 December 2022

Anonymised health data

Is anonymised health data subject to specific regulations or guidelines?

APP 2 provides that individuals must have the option of dealing anonymously or by pseudonym with entities subject to the Privacy Act. However, entities are not required to provide these options if the entity is required or authorised by law to deal with identified individuals or if it is impracticable for the entity to deal with individuals who have not identified themselves. There may also be practical consequences for patients who do not wish to identify themselves, as their ongoing healthcare may be difficult for organisations to manage and they are unlikely to be able to claim a Medicare or health fund rebate.

De-identification may be one way to protect the privacy of individuals. De-identification involves removing personal identifiers (such as name, address, date of birth, etc) and removing or altering other information that could identify an individual (such as unique characteristics). However, with the increasing capability of technology and the sophistication of cyber-attacks, it is becoming more and more difficult to de-identify data effectively. The Australian government is currently reviewing the Privacy Act, and considering increasing the relevant threshold from 'de-identified' to 'anonymous' (for information to no longer be considered 'personal information').

Types of de-identified health data include Medicare numbers and healthcare identifiers. Medicare numbers are primarily used by individuals to claim benefits under the Medicare Benefits Scheme. APP 9 restricts the use or disclosure of a patient's government-related identifier to specific circumstances (eg, it is reasonably necessary to verify the patient's identity for an organisation's activities).

Healthcare identifiers are unique 16-digit numbers that identify individual healthcare providers, healthcare provider organisations (such as digital health organisations) and individuals receiving healthcare. Healthcare identifiers help to reduce the potential for mix-ups with health data and are the foundation for government initiatives such as the My Health Record system, in which individuals' health information can be viewed securely online. They are not health records, but are limited to identifying information such as name, date of birth and sex to uniquely identify patients. The use of healthcare identifiers is regulated by the Healthcare Identifiers Act 2010 (Cth) and Healthcare Identifiers Regulations 2020 (Cth), which provide that healthcare identifiers may only be collected, accessed, used and disclosed for limited purposes (such as providing healthcare, for example, by using it to access the My Health Record of a healthcare recipient). In circumstances where a healthcare identifier is used or disclosed for purposes not permitted by the legislation, criminal and civil penalties may apply.

Law stated - 08 December 2022

Enforcement

How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The Privacy Act gives the Privacy Commissioner a range of privacy regulatory powers, including powers that allow the OAIC to work with entities to facilitate best privacy practices, as well as investigative and enforcement powers to use in response to privacy breaches.

For example, if a healthcare company fails to obtain consent to collect the health information of an individual, the company will be in breach of APP 3 regarding the collection of sensitive information.

A breach of an APP is an 'interference with the privacy of an individual' under section 13(1) of the Privacy Act and, although it is not a civil penalty provision, it can lead to regulatory action and penalties. The provisions of the Privacy Act are enforceable under Parts 6 and 7 of the Regulatory Powers (Standard Provisions) Act 2014 (Cth), which provide for enforceable undertakings and injunctions to be issued to enforce provisions.

In March 2019, it was announced that the Australian government intended to investigate the effectiveness of Australia's current data protection regime and potentially reform the Privacy Act, including by introducing higher penalties for breaches of the Privacy Act. In November 2022, the first legislation tabled in the Australian Parliament in connection with this review – the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Privacy Bill) – passed both Houses of Parliament. The Privacy Bill covers four key objectives with respect to the Privacy Act:

- to significantly increase the maximum penalty for serious or repeated interferences with the privacy of an individual under the Privacy Act, increasing the former penalty from A\$2.22 million (for corporate entities) to the greater of A\$50 million, three times the value of any benefit directly or indirectly obtained from the contravention, or, if the value of the benefit cannot be ascertained, 30 per cent of the company's adjusted turnover during the breach turnover period (minimum 12 months) for the contravention;
- to give the OAIC enhanced powers to request information and conduct compliance assessments of the notifiable data breach regime under the Privacy Act;
- to give the OAIC new enforcement powers, including allowing the OAIC to require entities to conduct external reviews of their internal procedures and to publish notices about specific privacy breaches to affected individuals; and
- to introduce new information-sharing powers for the OAIC and the Australian Communications and Media Authority, the regulator that oversees telecommunications providers.

Additionally, the Privacy Act's extraterritorial application has been broadened by the passing of the Privacy Bill. The Privacy Act requires entities that are established outside of Australia to meet the obligations of the Privacy Act if they 'carry on business' in Australia; however, the Privacy Bill has removed the former requirement in the Privacy Act for such entities to collect or hold personal information in Australia for the Privacy Act to apply.

Law stated - 08 December 2022

Cybersecurity

What cybersecurity laws and best practices are relevant for digital health offerings?

APP 11 imposes a legal obligation on entities to take steps as are reasonable in the circumstances to protect the

personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. Apart from this general obligation, there are no mandated IT security standards for the handling of health data in Australia. Some specific standards have been developed, including the ' Information security management in health using ISO/IEC 27002 ' and the National eHealth Security and Access Framework v4.0 . However, compliance with these standards is voluntary.

The OAIC has published its ' Guide to health privacy ' and the Australian Digital Health Agency has published an ' Information Security Guide for small healthcare businesses '. IT service providers that engage with government health agencies will typically be required to meet certain minimum IT security standards (eg, see the Digital Transformation Agency's Secure Cloud Strategy).

The Australian government has passed the Security Legislation Amendment (Critical Infrastructure) Act 2021 (the SLACI Act) and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (the SLACIP Act). These Acts implement the first initiative of Australia's Cyber Security Strategy 2020 , which is to protect Australia's critical infrastructure providers from cyber threats by amending the SOCI Act. Key reforms made by the SLACI Act and SLACIP Act include to:

- expand the definition of critical infrastructure sectors and assets that are covered by the SOCI Act to include the healthcare and medical sector (among others);
- require mandatory notification of cyber security incidents;
- implement government assistance and intervention measure that give the Australian government the power to direct entities to gather information and take certain actions in respect of cyber security matters;
- authorise the Australian Signals Directors to intervene in response to cyber-attacks where critical;
- create a new 'positive security obligation' requiring responsible entities to create and maintain a critical infrastructure risk-management programme, including consideration of cyber and information security hazards; and
- introduce a new framework of 'enhanced cyber security obligations' that must be complied with by operators of systems of national significance (namely, Australia's most important critical infrastructure assets).

Law stated - 08 December 2022

Best practices and practical tips

What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Organisations should consider the following three key questions:

- consent: do you have adequate consent to collect, use and disclose health data for this purpose? Where health data is collected in addition to personal information, additional consent may be required. The Privacy Act distinguishes between the use and disclosure of personal information for 'primary purposes' versus 'secondary purposes'. The 'primary purpose' is the specific purpose for which the health information was collected. The context in which the health information was collected is relevant to this concept. A 'secondary purpose' is any use or disclosure for reasons other than the primary purpose. Secondary purposes are prohibited, unless the secondary purpose falls within a specifically permitted exception. In the health information context, the most common permitted exceptions are:
 - the individual would reasonably expect the organisation to use the information for the secondary purpose, and the secondary purpose is directly related to the primary purpose;

- if the use and disclosure are required to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
- if the use and disclosure is in connection with the provision of a health service or research or if the individual is incapable of giving consent (in each case, subject to specific rules); and
- if required by law or for law enforcement purposes;
- data systems: do you have appropriate data management systems in place? There are differing legal requirements for the handling of health data and personal information; however, these types of information are most often collected together. It is important to understand which data fits into each category, and to establish distinct data management processes for these different types of data; and
- security: do you have adequate security to protect against unauthorised access and misuse? Consider security safeguards that are reasonable in the circumstances.

Law stated - 08 December 2022

INTELLECTUAL PROPERTY

Patentability and inventorship

What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Patentees of digital health-related inventions, which often require computer implementation in one form or another, need to navigate the patentability requirement in Australia. While abstract ideas and computer-implemented inventions are not regarded as patentable subject matter in Australia, patents directed to other aspects of digital health-related inventions such as hardware, telemetry and diagnostic tools may be patent-eligible.

Recently, the Full Federal Court of Australia found that an artificial intelligence system could not be named as an inventor on a patent application (*Commissioner of Patents v Thaler* [2022] FCAFC 62). The High Court of Australia (Australia's apex court) declined to hear an appeal of this decision (*Thaler v Commissioner of Patents* [2022] HCATrans 199).

Law stated - 08 December 2022

Patent prosecution

What is the patent application and registration procedure for digital health technologies in your jurisdiction?

The Australian patent system provides the same application process across all technologies, including digital health. There are no specific provisions for digital health technologies. IP Australia (incorporating the Australian Patent Office) is responsible for pre-grant examinations, pre-grant oppositions, re-examinations and amendments to patents and patent applications. As in other jurisdictions, the process of filing to grant can take more than 18 months.

Law stated - 08 December 2022

Other IP rights

Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Registrable IP rights are available in the form of design rights that safeguard the visual appearance of new and

distinctive products, such as wearable devices that incorporate digital health offerings. Design rights are secured through an application process administered by IP Australia and last for five years initially (renewable for another five years).

Additionally, unregistrable forms of IP including copyright, know-how, trade secrets and confidential information may arise in the context of digital health technologies and offerings. Contractual measures (such as non-disclosure agreements) may help to protect the know-how, trade secrets and confidential information, such as secret algorithms in a digital health app, often in conjunction with physical and technological security measures. Copyright arises automatically in some subject matter likely to be integral to digital health offerings, such as in computer code in a digital health app.

Law stated - 08 December 2022

Licensing

What practical considerations are relevant when licensing IP rights in digital health technologies?

Arrangements involving the licensing or assignment of patents are subject to Australian competition laws. In September 2019, the Competition and Consumer Act 2010 (Cth) (the CCA) was amended to repeal a section that previously exempted certain IP assignments and licensing arrangements from the full operation of the CCA. Since the repeal of this IP exemption, the Australian Competition and Consumer Commission appears to be taking an increasing interest in restrictions in IP arrangements.

Compliance with the Therapeutic Goods Act 1989 (Cth) of any relevant IP assets claimed is also likely to be an important practical consideration.

Law stated - 08 December 2022

Enforcement

What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

In Australia, there are no bespoke procedures that govern the enforcement of IP rights relating to digital health technologies.

Law stated - 08 December 2022

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

Rules relating to advertising and marketing of digital health products appear in the Therapeutic Goods Act 1989 (Cth), which regulates all therapeutic goods, the Therapeutic Goods Regulations 1990 (Cth), and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations), which include provisions about advertising therapeutic goods and information about both ingredients and patient information, as well as the Australian Register of Therapeutic Goods.

The Therapeutic Goods (Therapeutic Goods Advertising Code) Instrument 2021 (Cth) (the Advertising Code) ensures

that the marketing and advertising of therapeutic goods to consumers is conducted in a manner that promotes the safe and effective use of goods, is socially responsible and does not mislead or deceive consumers. In contrast to the previous iteration of the Advertising Code, the new Advertising Code is far more instructive as to permitted products and prohibited practices. The TGA has also published guidance on social media advertising, the ' TGA social media advertising guide '.

The advertising and marketing of health services, including digital health services, is governed by the Health Practitioner Regulation National Law Act Scheme , with nationally consistent laws passed by each state and territory parliament. To assist providers of health services in Australia understand how national law is to be applied to advertising, the Australian Health Practitioner Regulation Agency has set out guidelines for advertising regulated health services.

In addition, the rules that apply to registered trademarks (contained in the Trade Marks Act 1995 (Cth)), and in relation to passing off and misleading and deceptive conduct (torts and the Australian Consumer Law) are relevant in marketing and advertising digital health products and services.

Law stated - 08 December 2022

e-Commerce

What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

The rules governing e-commerce are the same as the rules governing general commerce and there are no specific rules governing e-commerce for digital health offerings. Similarly, entering into contracts electronically only requires compliance with general contract law and there are no technology-specific rules. As with all customer contracts, businesses must take all reasonable steps to present the contract terms to the customer and ensure that the customer has indicated their consent to those terms. For example, customers accepting terms by selecting a tick box online is equivalent to the customer signing the contract.

Payment rules to note include the Payment Card Industry Data Security Standards (PCI DSS), which are intended to help businesses protect their own and customers' data from breaches and theft. Compliance with the PCI DSS is not mandatory but is strongly recommended given there are legal consequences for data breaches.

Medicare Easyclaim is a Medicare initiative that allows patients to claim and receive Medicare rebates through their healthcare providers. Businesses offering digital health services covered by Medicare may wish to integrate the Medicare Easyclaim system into their practice management software products or alternatively, Medicare Easyclaim can be a stand-alone process via an Electronic Funds Transfer at Point of Sale (EFTPOS) device. EFTPOS providers continue to integrate Medicare Easyclaim into their infrastructure to allow for instantaneous rebates and lodgement of claims.

Some private health insurers provide similar claiming services to Medicare Easyclaim, so that patients do not have to separately claim to their private health insurer to cover a particular cost.

Law stated - 08 December 2022

PAYMENT AND REIMBURSEMENT

Coverage

Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

Reimbursement is important for creating incentives for the implementation and adoption of digital health products and

services in Australia. It is a complex area, and when it comes to digital health products and services under current schemes, it is likely that some products will be covered while others will not.

The Australian government broadly aims to assist Australians in accessing health services and technologies by subsidising the cost of health-related goods and services, including through the Pharmaceutical Benefits Scheme (subsidies for certain medicines) and the Medicare Benefits Schedule (MBS) (subsidies for certain health services). Telehealth services – being health services provided via videoconference or telephone, instead of via face-to-face consultations – were made temporarily available under the MBS in 2020 in response to the covid-19 pandemic. They have now been made permanently available.

The Australian government has also increased accessibility to Dexcom G6 Continuous Glucose Monitoring technology. From 1 July 2022, all Australians with type 1 diabetes now have access to Dexcom, which links to a person's smartphone via Bluetooth, providing alerts when blood glucose levels are abnormal. Previously, only individuals with either type 1 or 2 diabetes who met the Medicare Coverage Criteria could access the subsidy.

Private health insurers are required to pay benefits for products listed on the Prosthesis List published by the Australian Government Department of Health (if the product is provided to a patient with the right cover). The current Prostheses List includes various digital health products, such as cardiac implantable electronic devices and cardiac remote monitoring systems. For example, products such as the VISIA AF MRI XT SureScan ICDs, a digital single chamber implantable cardioverter defibrillator, and Cochlear Baha 5 SuperPower Sound Processor, a wireless-enabled smartphone-compatible fully programmable digital sound processor for implantable bone conduction hearing systems, are included on the list.

Separately, the Practice Incentives Program eHealth Incentive is a computer program administered by Services Australia that incentivises general practices to keep up to date with, and to adopt, digital health technology by providing periodic payments to eligible practices.

Law stated - 08 December 2022

UPDATES AND TRENDS

Recent developments

What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

The digital economy, including consumer data issues in digital health, is an area of priority for the Australian Competition and Consumer Commission (ACCC).

The ACCC continues to commence proceedings focused on misleading and deceptive conduct around the use of consumer data in various sectors. For example:

- in 2019, the ACCC commenced proceedings against HealthEngine (an online health directory) for misleading consumers about the use of their data and the publication of patient reviews and ratings;
- in August 2020, by consent of the parties, the Federal Court ordered that HealthEngine pay A\$2.9 million in penalties for engaging in misleading and deceptive conduct; and
- on 24 October 2022, the ACCC commenced proceedings against Fitbit LLC for misleading consumers about their rights under the consumer guarantee regime in the Australian Consumer Law.

In relation to merger reviews:

- since January 2022, the ACCC is continuing to investigate Google's acquisition of Fitbit, a year after the

transaction was completed in January 2021. The ACCC's ongoing investigation contrasts with the approach of various regulators overseas, including the European Union, that have conditionally cleared the transaction; and

- the ACCC concluded its review of Microsoft's proposed acquisition of Nuance in October 2021. The ACCC considered the impact of the proposed acquisition in healthcare transcription software and customer engagement solutions, and found that it was unlikely to have the effect or likely effect of substantially lessening competition.

More generally, on 11 November 2022, the ACCC released its fifth interim report in its Digital Platforms Services Inquiry 2020-2025, on regulatory reform (DPSI-5). DPSI-5 included a suite of recommendations for regulating digital platforms. The key recommendations are likely to impact Australia's digital health industry, namely:

- consumer measures to prevent and remove scams, harmful apps and fake reviews, with dispute resolution and complaint escalation processes;
- economy-wide consumer measures prohibiting unfair trading practices, and expanded prohibitions against unfair contract terms; and
- mandatory codes of conduct for designated digital platforms, on a service-specific basis including for search, app stores, adtech and mobile operating systems. The codes would address competition law issues including self-preferencing, interoperability, transparency, exclusivity, data barriers to competition, unfair dealings, impediments to consumer switching and price parity clauses.

The government has said it is considering the ACCC's recommendations in DPSI-5 and will consult publicly to seek the views of stakeholders.

Previous interim reports of the Digital Platforms Services Inquiry 2020-2025 have focused on online private messaging services, mobile app stores, web browsers and general search services, online retail marketplaces, and social media services.

The Australian government passed the Security Legislation Amendment (Critical Infrastructure) Act 2021 and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022, which implement the first initiative of Australia's Cyber Security Strategy 2020, being to protect Australia's critical infrastructure providers from cyber threats by amending the SOCI Act. Significantly, the amendments impose security obligations on 11 new sectors, including the 'health care and medical' sector.

The recent amendments to the Therapeutic Goods Regulations 1990 (Cth), and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations) to exempt certain kinds of clinical decision support software from the Australian Register of Therapeutic Goods have reduced the regulatory burden for businesses providing this service, and is a significant development affecting the sector.

Since 2019, the Attorney-General has been conducting a review of the Privacy Act 1988 (Cth) (the Review), with several rounds of public consultations. Submissions to the most recent consultation closed in January 2022, and it is unclear what reforms will arise out of the Review.


There has been an increased focus on cybersecurity in Australia following two of the largest known cybersecurity breaches in Australia's history: the September 2022 data breach affecting Australia's second-largest telecommunications provider, Optus, which compromised the information of about 9.8 million former and current customers; and the October 2022 data breach affecting Medibank, Australia's largest private health insurance provider. In December 2022, Medibank confirmed that the personal data of up to 10 million customers had been released on the dark web by the criminals responsible for the data breach. As a result of these data breaches and as part of the Review, it is likely that tougher legislative requirements will be imposed in respect of data retention and how much data entities

are permitted to collect, and also more stringent requirements on digital health providers given the sensitive data assets they hold.

The National Health (Pharmaceutical Benefits) Regulations 2017 (Cth) have been amended to allow electronic prescriptions under the Pharmaceutical Benefits Scheme. As a result, electronic prescribing has become widely available, with less need for paper prescriptions. Telehealth has also become more prevalent, as, from 1 July 2022, the arrangements for the Medicare Benefits Schedule to support patient access to telehealth services were made permanent. These particular developments demonstrate the increased reliance on digital technology in the health sector.

Law stated - 08 December 2022

Jurisdictions

	Australia	Gilbert + Tobin
	Czech Republic	dubanska & co
	France	Intuity
	Germany	Ehlers Ehlers & Partner
	India	Chadha & Chadha Intellectual Property Law Firm
	Indonesia	ABNR
	Ireland	Mason Hayes & Curran LLP
	Israel	Naschitz Brandes Amir
	Japan	Anderson Mōri & Tomotsune
	Qatar	Al Marri & El Hage Law Office
	South Korea	Bae, Kim & Lee LLC
	Spain	Baker McKenzie
	Switzerland	Lenz & Staehelin
	Thailand	Baker McKenzie
	United Kingdom	Latham & Watkins LLP
	USA	Seyfarth Shaw LLP