DIGITAL HEALTH

Australia

LEXOLOGY
Getting The Deal Through

Digital Health

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 25 January 2022

Table of contents

UPDATES AND TRENDS

Recent developments

Contributors

Australia

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

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

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

John Lee
jlee@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 (funds 42 per cent of all health services, including 78 per cent of research), especially the Department of Health, the Therapeutic Goods Administration (TGA), the Medical Research Future Fund (MRFF) and the Australian Digital Health Agency (ADHA), which is responsible for the National Digital Health Strategy 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 (fund 27 per cent of all health services), 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 heath systems;
- private health insurers (fund 9 per cent of all health services);
- 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 and the Australasian Institute of Digital Health.

Participants in the healthcare industry (government and private) are increasing their adoption of digital health technologies in order 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), AI, interoperability, health informatics, payments and e-referral and booking.

Law stated - 25 November 2021

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 the 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 introduction of whole-of-population access to telehealth under Medicare.

However, the key challenge in the Australian digital health industry remains funding and access to capital to drive 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.

Law stated - 25 November 2021

Recent deals

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

In the private sector:

- 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.
- In August 2021, Telstra acquired the GP clinical and management software company Medical Director for A$350 million.
- In August 2021, Livingbridge acquired a large controlling stake in Everlight Radiology for A$500 million.
- In August 2021, epilepsy diagnosis and monitoring technology company Seer Medical raised A$34 million in a Series A funding round.
- In July 2021, Telstra acquired a majority stake in medical software company Power Health for A$95 million.
- In July 2021, healthcare AI company Harrison.ai raised A$60 million in a A$40 million Series B funding round and A$20 million investment by I-MED Radiology. (Harrison.ai previously raised A$29 million in a Series A funding round in December 2019.)
- In July 2021, telehealth company Eucalyptus raised A$30 million in a Series B funding round. (Eucalyptus previously raised A$8 million in a Series A funding round in May 2020.)
- In May 2021, CBA acquired health technology provider Whitecoat for an undisclosed sum.
- In May 2021, fintech Tyro Payments acquired digital health payment platform Medipass for A$22.5 million.
- In December 2020, Pacific Equity Partners acquired a majority stake in The Citadel Group for A$503 million.
- In December 2020, telemedicine company Dr Care Anywhere raised A$102 million in an IPO on the ASX

In the public sector:

- 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 covid-19.
- In June 2021, NSW allocated A$141 million for a statewide single digital patient record that will bring together the different instances of its EMR, PAS and LIS systems on a single platform, preferably software-as-a-service-based.
- In December 2020, eHealth NSW set up the Virtual Accelerator to coordinate the range of innovations prompted by covid-19, including telehealth and remote monitoring.
- In November 2020, the South Australia government allocated A$197 million to complete the rollout of EMR and PAS systems in its metropolitan local health networks.
- In November 2020, following the release by the Department of Health of a National Contact Tracing Review, NSW, Victoria and the Australian Capital Territory (ACT) agreed to pilot a national digital data exchange mechanism that would allow the states and territories to share contact-tracing data for the covid-19 pandemic and future outbreaks.
- In October 2020, Wellbeing SA selected a joint venture between Calvary and Medibank to provide its new in-home

hospital care programme, My Home Hospital.

- In early 2020, the Australian government introduced whole-of-population access to Medicare-subsidised telehealth as well as electronic prescriptions and home delivery of medicines for vulnerable Australians.
- In February 2020, Sydney Local Health District launched the first virtual hospital in New South Wales (NSW), the RPA Virtual Hospital, which treated over 3,500 patients in its first seven months.
- In July 2020 ACT Health awarded a tender to Epic for its A$151 million digital health record project.
- In October 2019, WA Health entered into a A$47.2 million agreement for a replacement medical imaging system.
- In August 2019, WA Health issued a request for information on the feasibility and potential options for implementing a statewide EMR system as part of its 10-year digital health strategy.
- In April 2019, NSW Health entered into a A$95 million agreement for a statewide medical imaging system.
- In 2017, NSW Health commenced the rollout of a statewide eMeds and eFluids systems with a budget of about A $406 million.

Law stated - 25 November 2021

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 data flows critical to the company's operation; and
- ensuring that a company has 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 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.
- 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 - 25 November 2021

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 (for example, 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 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 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 Partnership 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 - 25 November 2021

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) (CCA), which is the standard competition law framework in Australia. The CCA also includes the Australian Consumer Law (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) (TGA Act), which regulates all therapeutic goods, that is medical devices, medicines (including complementary, over-the-counter and prescription) and the Therapeutic Goods Regulations 1990, and the Therapeutic Goods (Medical Devices) Regulations 2002 (Cth) (together, the TGA Regulations). The TGA Act was updated earlier this year 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 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. 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 also regulates the treatment of health information contained in individuals' health records (My Health Record) and healthcare identifiers operated by Medicare.

Law stated - 25 November 2021

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.

Law stated - 25 November 2021

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 - 25 November 2021

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 is responsible for the development and operation of a national digital health strategy, as well as development and implementation of specifications and standards in relation to digital health. The Australian Digital Health Agency publishes guides and other resources that may be relevant to providers of digital health products and services.

Law stated - 25 November 2021

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 is the greater of:
- A$10 million;
- three times the value of the benefit obtained from the breach; or
- if that cannot be calculated, 10 per cent of annual turnover for the previous 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 who 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. The Australian government has recently sought public consultation on draft legislation that will make unfair contract terms unlawful and subject to civil penalties (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 minimisation of cybersecurity risks.

Law stated - 25 November 2021

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 - 25 November 2021

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 is regulated by 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)'s 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, ICT 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 - 25 November 2021

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 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. Use of healthcare identifiers are 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 - 25 November 2021

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.

If the breach of an APP were to be regarded as a 'serious interference with the privacy of an individual', then civil penalties of up to A$2.1 million per breach may apply. Additionally, in March 2019, it was announced that the

government intends to introduce higher penalties for breaches of the Privacy Act (however, these have not yet been implemented). This announcement has been mirrored in proposed reforms to the Privacy Act by the Australian Government. The proposed penalty changes to the Privacy Act include:

- an increase in the maximum penalty for serious and repeated interferences with the privacy of an individual under Privacy Act, increasing the current penalty from A$2.1 million (for corporate entities) to the greater of A$10 million, three times the value of any benefit obtained through the misuse of the information, and 10 per cent of the company's annual domestic turnover; and
- greater enforcement and remedial powers for the OAIC.

Law stated - 25 November 2021

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 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 who engage with government health agencies will typically be required to meet certain minimum IT security standards (for example, see the Digital Transformation Agency's Secure Cloud Strategy).

The Australian government has passed the Security Legislation Amendment (Critical Infrastructure) Bill 2021 (the Bill). The Bill is set to 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 Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act). The Bill was passed on 22 November 2021 and is expected to become law shortly thereafter. Key reforms made by the Bill include to:

- expand the definition of critical infrastructure sectors and assets that are covered by the SOCI Act to include the health care and medical sector (amongst others);
- require mandatory notification of cyber security incidents; and
- 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; and
- authorise the Australian Signals Directors to intervene in response to cyber-attacks where critical.

Law stated - 25 November 2021

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.

1. 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 specific 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 is 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.

1. 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.

1. Security – do you have adequate security to protect against unauthorised access and misuse?

Consider security safeguards that are reasonable in the circumstances.

Law stated - 25 November 2021

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 Federal Court of Australia found that an artificial intelligence (AI) system could be named as an inventor on a patent application (Thaler v Commissioner of Patents [2021] FCA 879). The Commissioner of Patents has appealed the decision asserting that the Patents Act 1990 (Cth) is incompatible with permitting an AI system to be an inventor.

Law stated - 25 November 2021

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 - 25 November 2021

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 - 25 November 2021

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

Law stated - 25 November 2021

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 - 25 November 2021

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 Administration (TGA) Act, which regulates all therapeutic goods, 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 and the Therapeutic Goods Advertising Code (No 2) 2018 (Cth), which ensures that the marketing and advertising of therapeutic goods to consumers is conducted in a manner that promotes the quality use of goods, is socially responsible and does not mislead or deceive consumers.

The advertising and marketing of health services, including digital health services, is governed by the Health Practitioner Regulation National Law Act 2009 (Cth) (National Law). To assist providers of health services in Australia understand how the 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), 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 - 25 November 2021

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 tickbox 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 EFTPOS device.

Law stated - 25 November 2021

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 – a digital health service which was embraced when Australia attempted to reduce community transmission of covid-19 – has been made temporarily available under the MBS from 13 March 2020, and its coverage is set to continue until 31 March 2021.

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.

Law stated - 25 November 2021

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 recently commenced a number of proceedings, focused on misleading and deceptive conduct around the use of consumer data in various sectors. In relation to digital health, on 7 August 2019, the ACCC commenced proceedings against HealthEngine (an online health directory) for misleading consumers around the use of their data and the publication of patient reviews and ratings.

On 20 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.

In mergers, the ACCC is currently reviewing Google's proposed acquisition of Fitbit as an enforcement investigation as the transaction completed on 14 January 2021 prior to the ACCC completing its merger review investigation.

The ACCC recently concluded its review of Microsoft's proposed acquisition of Nuance on 7 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.

In more general terms, the ACCC's approach following the Digital Platforms Inquiry 2017–2019, and with its new Digital Platforms Branch, is to focus on the proactive monitoring and enforcement of potentially anticompetitive conduct associated with the digital economy. The ACCC is currently conducting a Digital Platforms Services Inquiry 2020-2025

and has published interim reports in relation to online private messaging services, distribution of mobile apps, and the provision of web browsers and general search services to Australian consumers. Recommendations arising from this inquiry in relation to privacy issues and handling of consumer data may be relevant to the digital health sector. It is likely there will be more activity in this area in the future.

The Australian government passed the Security Legislation Amendment (Critical Infrastructure) Bill 2021 on 22 November 2021. The Bill is set to 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 Security of Critical Infrastructure Act 2018 (Cth). Significantly, the amendment will impose security obligations on 11 new sectors, including 'health care and medical'.

The recent amendments to the the Therapeutic Goods Administration (TGA) Regulations to exempt certain kinds of clinical decision support software from the Australian Register of Therapeutic Goods (ARTG) has reduced the regulatory burden for businesses providing this service, and is a significant development affecting the sector.

Law stated - 25 November 2021

Jurisdictions

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