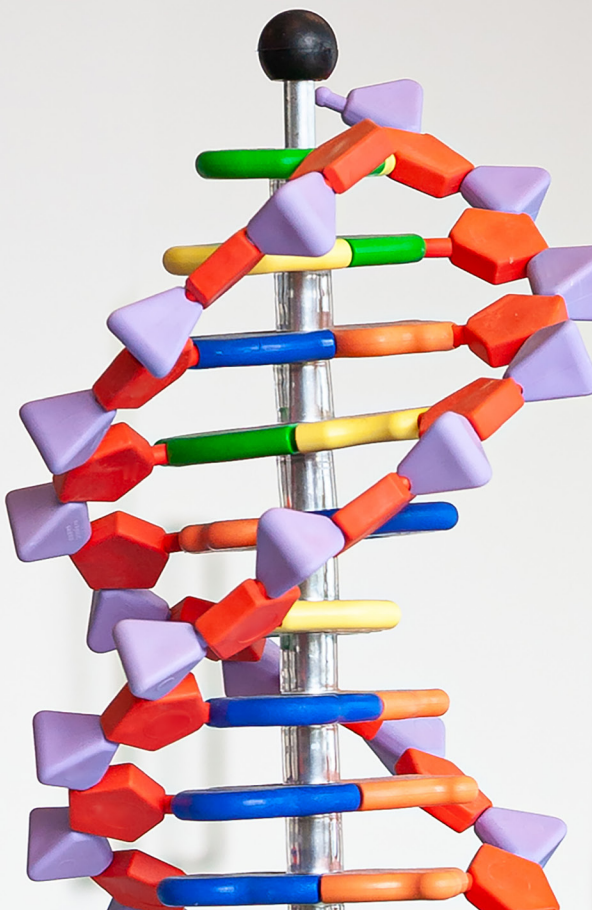
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Digital Healthcare 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers



Australia: Law & Practice

Greg Williams, Timothy Webb and Ken Saurajen
Clayton Utz

AUSTRALIA

Law and Practice

Contributed by:
Greg Williams, Timothy Webb and Ken Saurajen
Clayton Utz

Contents

1. Digital Healthcare Overview p.6
1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics p.6
1.2 Regulatory Definition p.6
1.3 New Technologies p.7
1.4 Emerging Legal Issues p.7
1.5 Impact of COVID-19 p.8

2. Healthcare Regulatory Environment p.9
2.1 Healthcare Regulatory Agencies p.9
2.2 Recent Regulatory Developments p.9
2.3 Regulatory Enforcement p.10

3. Non-healthcare Regulatory Agencies p.11
3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies p.11

4. Preventative Healthcare p.12
4.1 Preventative Versus Diagnostic Healthcare p.12
4.2 Increased Preventative Healthcare p.13
4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information p.14
4.4 Regulatory Developments p.14
4.5 Challenges Created by the Role of Non-healthcare Companies p.16

5. Wearables, Implantable and Digestibles Healthcare Technologies p.16
5.1 Internet of Medical Things and Connected Device Environment p.16
5.2 Legal Implications p.17
5.3 Cybersecurity and Data Protection p.18
5.4 Proposed Regulatory Developments p.18

6. Software as a Medical Device p.20
6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies p.20

7. Telehealth p.21
7.1 Role of Telehealth in Healthcare p.21
7.2 Regulatory Environment p.22
7.3 Payment and Reimbursement p.22

8. Internet of Medical Things p.22
8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things p.22

9. 5G Networks p.22
9.1 The Impact of 5G Networks on Digital Healthcare p.22

10. Data Use and Data Sharing p.23
10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information p.23

11. AI and Machine Learning p.25
11.1 The Utilisation of AI and Machine Learning in Digital Healthcare p.25
11.2 AI and Machine Learning Data Under Privacy Regulations p.26

12. Healthcare Companies p.26
12.1 Legal Issues Facing Healthcare Companies p.26

13. Upgrading IT Infrastructure p.27
13.1 IT Upgrades for Digital Healthcare p.27
13.2 Data Management and Regulatory Impact p.28

14. Intellectual Property p.28
14.1 Scope of Protection p.28
14.2 Advantages and Disadvantages of Protections p.29
14.3 Licensing Structures p.29
14.4 Research in Academic Institutions p.30
14.5 Contracts and Collaborative Developments p.30

15. Liability p.30
15.1 Patient Care p.30
15.2 Commercial p.31

Clayton Utz is recognised as a leading life sciences law firm. With 17 partners and over 25 qualified lawyers across its Sydney, Melbourne, Brisbane and Perth offices practising in this area, the firm continues to build a reputation for innovative and incisive advice. The team has a unique combination of scientific, regulatory and legal expertise in prescription pharmaceuticals, OTC and complementary medicines and medical devices, and is consistently the legal firm of choice for many Australian and global pharmaceutical and medical device companies. The firm advises on all aspects of the product life cycle, including the strategy, protection and enforcement of IP, clinical trials, marketing approval, product labelling, reimbursement, approval and registration processes, promotion and distribution, product risk, product liability and product recall. Clayton Utz counts both established global pharmaceutical companies and agile start-ups among its clients. It has advised Medicines Australia (the prescription pharmaceutical industry body) about significant policy initiatives in the pharmaceutical space.

Authors

Greg Williams has over 20 years' experience providing regulatory and litigation advice to Australian and overseas pharmaceutical and medical device companies. In the regulatory sphere, he provides advice across the whole product life cycle, including product registration, reimbursement, advertising disputes, and product safety and recalls. He has particular expertise in providing strategic advice in relation to pricing and reimbursement issues and has assisted a number of clients of Clayton Utz to navigate difficult and contentious Australian reimbursement applications. In litigation, Greg defends product liability claims and class actions. He has been involved in the defence of several prominent pharmaceutical and medical device product liability claims.

Timothy Webb is a partner in the intellectual property and technology practice group at Clayton Utz. His expertise covers all aspects of intellectual property law (eg, copyright, trade marks, patents, designs, confidential information, domain names) in both contentious and non-contentious matters. He has extensive public sector experience. He has also acted for clients in landmark Australian test cases for both copyright and designs. Tim is also the joint head of the firm's trade mark and brand protection group, which is responsible for matters relating to the registration of trade marks, including clearance.

Ken Saurajen is a partner in Clayton Utz's intellectual property and technology practice group, with a formidable reputation for the design and structuring of some of Australia's and the Asia Pacific region's most difficult and unorthodox telecommunications, media and technology transactions. He specialises in strategic, front-end information technology contracting and is renowned for his work on large-scale, complex IT procurements, outsourcing and transformation projects, software licensing, electronic payment systems, bespoke data contracting and commercialisation projects. Ken has a long track record as a regular contributor to industry dialogue concerning issues at the intersection of technology, business and policy.

Clayton Utz

Level 15
1 Bligh Street
Sydney
NSW 2000
Australia

Tel: +612 9353 4000
Fax: +612 8220 6700
Email: gwilliams@claytonutz.com
Web: www.claytonutz.com

CLAYTON UTZ

1. Digital Healthcare Overview

1.1 Digital Healthcare, Digital Medicine and Digital Therapeutics

There are many solutions to long-standing problems in the healthcare industry that can be addressed with innovative technologies, including those of healthcare providers, patients and regulators.

From a healthcare provider's perspective, advances in digital healthcare may assist in responding to changes in its operating environment (eg, the restrictions created by the COVID-19 pandemic), as well as improved efficiencies and practice management. This includes the adoption of online booking systems for medical practices, telehealth capabilities, and data record-keeping systems.

From a technical perspective, there has been an increase in the prevalence of "do-it-yourself" devices that work with mobile phone apps to allow people to easily monitor their own signs, such as blood oxygenation or electrocardiography. These give practitioners easier access to more comprehensive patient data. At the far end of the spectrum, practitioners may also have increasingly advanced digital medicine options available to deploy, prescribe or administer, such as medical devices that are controlled by software, for example, insulin pumps controlled by mobile phone applications. These technologies are enabled by advances in mobile computing power and internet infrastructure.

From a regulatory perspective, much will turn on the extent to which such products are therapeutic goods regulated under the Therapeutic Goods Act 1989 (Cth) (the "TG Act"). Medical devices are regulated under Chapter 4 of the TG Act, which is administered by the Therapeutic Goods Administration (TGA). The regulation of medical devices is discussed further in **6. Software as a Medical Device**.

1.2 Regulatory Definition

The terms "digital health" and "digital medicine" are not defined in any Australian regulatory framework. There are, however, active organisations in this space that provide definitions for each of these terms.

Digital Health

The term "digital health" is defined by the Australian Government Institute of Health and Welfare as: "An umbrella term referring to a range of technologies that can be used to treat patients and collect and share a person's health information, including mobile health and applications, electronic health records, telehealth and telemedicine, wearable devices, robotics and artificial intelligence."

An example of digital health in Australia is the My Health Record initiative, which is a federal government-operated database that stores an individual's health information in one place. This is regulated by the Australian Digital Health Agency (ADHA).

Digital Medicine

It is more difficult to find a government agency which defines "digital medicine". However, ANDHealth, an organisation established to support the commercialisation of digital medicine in Australia, defines digital medicine as: "Evidence based software and/or hardware products that measure and/or intervene in human health. They all require clinical evidence and are likely to require regulatory approval."

Digital medicine which meets the definition of a medical device will be subject to regulation

by the TGA. On the other hand, many products, including healthcare-enabling technologies, are now excluded from the regulatory regime.

1.3 New Technologies

The key technologies enabling new capabilities in digital healthcare and digital medicine include telemedicine, blockchain electronic health records (or comparable systems such as My Health Record, which uses a public key infrastructure) and artificial intelligence-enabled medical devices.

Digital Healthcare

Since the beginning of the COVID-19 pandemic in early 2020, digital healthcare and its enabling technologies have increased in popularity as the healthcare industry came to rely on technologies to enable consultations with medical practitioners to take place remotely.

This shift, based on necessity, has provided opportunities to improve accessibility and appeal to healthcare for patients who might have had obstacles in attending a consultation previously, including those who live remotely, those who have work or carer commitments, and those with compromised immunity who prefer not to attend a clinic.

At the same time, the federal government's My Health Record has created the potential for medical records to be accessed across medical practices, meaning patients who have not opted out of the programme can be treated by any doctor without needing to have their files transferred manually. If implemented effectively, this has the potential to improve the standard of healthcare provided, as the medical practitioner has all previous tests, results and medical history available to them on the database. However, the use of electronic health records in Australia is in its infancy. Use of the My Health Record system is not yet widespread enough to deliver on its potential benefits. Take-up has been limited by concerns about data security.

Digital Medicine

The most critical development in digital medicine is the increasing prevalence of software which, whether operating alone or in conjunction with certain hardware, operates as a medical device – eg, technologies that can diagnose or at least identify the possible presence of health conditions based upon the application of an algorithm to personal health data which is provided directly by the patient.

Such technologies are instances of "software as a medical device" and will be regulated by the TGA as a standalone medical devices.

1.4 Emerging Legal Issues

Important emerging legal issues in digital health include cybersecurity/data privacy and the boundaries of medical device regulation. The increased use of digital healthcare and rapid innovations in digital medicine have meant that the law has lagged behind in implementing legislation to address the newly created risks associated with these technologies.

Cybersecurity

Cybersecurity concerns are a key emerging legal issue arising from digital health. The increased availability of digital healthcare means that personal health information will increasingly be stored electronically in connected systems, making such information vulnerable to theft. Concerns about cybersecurity have been heightened by a number of high profile data breaches in 2022, including a data breach of Medibank (Australia's largest private health insurer).

Cybersecurity breaches of medical devices that use network functions could result in not only a loss of personal health data privacy, but also changes in device functionality, placing lives at risk.

Healthcare providers using Australia's My Health Record electronic medical records are required by the My Health Records Rule 2016 (Cth) to have a written policy addressing their security arrangements in respect of access to the system, known as a "My Health Record system security policy".

The TGA requires that, where relevant, medical devices should be appropriately cybersecure in order to comply with safety and performance standards under the Therapeutic Goods (Medical Device) Regulations 2002 (the "Medical Device Regulations").

More generally, where personal information is accessed or disclosed without authority and there is a risk that the breach will cause serious harm, the Privacy Act 1988 (Cth) (the "Privacy Act") requires organisations to inform affected individuals and the Office of the Australian Information Commissioner (OAIC) that serious harm may occur.

Medical Device Regulation

The regulation of software-based medical devices by the TGA is another emerging issue, given that digital forms of healthcare have necessarily entailed the proliferation of such devices. It is important to strike the right balance between appropriate regulation of the technology and not limiting the development of new technologies that may not fit neatly into existing categories.

As of 25 February 2021, changes were made to the Medical Device Regulations, clarifying existing requirements, introducing new requirements for software-based medical devices, and expressly exempting or excluding certain types of software from the requirement for registration.

1.5 Impact of COVID-19

COVID-19 has accelerated the uptake of digital healthcare technologies which facilitate the remote delivery of health services.

The benefits of telehealth, as discussed in **1.3 New Technologies**, were crucial during the pandemic. Australia's Medicare system subsidises doctors' provision of most medical services to Australian citizens and permanent residents. Subsidised services are listed on the Medicare Benefits Schedule (MBS). During 2020, the federal government both increased the number of subsidised telehealth services and removed many of the pre-conditions for the provision of existing listed telehealth services.

Those changes were temporary and were originally scheduled to operate until 31 March 2021. They were ultimately extended until 30 June 2022. From 1 July 2022, revised telehealth arrangements continued for some, but not all, subsidised telehealth services. Further adjustments were made to the subsidisation of telehealth services on 1 October 2022 and 1 April 2023.

Similarly, Australia's Pharmaceutical Benefits Scheme (PBS) subsidises the dispensing of prescription medicines. Some high-cost medicines require medical testing before a prescription is authorised. Many of these requirements were temporarily suspended from 1 May 2020. However, the COVID-19 arrangements have now ceased.

The federal government also introduced changes to permit the dispensing of most PBS medicines on the basis of a digital image of a prescription. These measures ceased at the end of March 2023. However, COVID-19 has driven a move to the use of electronic prescribing using secure digital token. Such prescribing is now permitted in most Australian jurisdictions.

2. Healthcare Regulatory Environment

2.1 Healthcare Regulatory Agencies

The key regulatory agencies in Australia that oversee technologies, devices and treatment include the following.

Therapeutic Goods Administration (TGA)

The TGA is the medicine and therapeutic regulatory agency of the Australian government, governed by the TG Act. It is responsible for regulating the supply, import, export, manufacturing and advertising of therapeutic goods and it carries out a range of assessment and monitoring activities to ensure that therapeutic goods available in Australia are of an acceptable standard.

Generally, any product for which therapeutic claims are made must, unless there is an applicable exemption, be approved by the TGA for entry on the Australian Register of Therapeutic Goods (ARTG) before it can be legally supplied in Australia.

Australian Digital Health Agency (ADHA)

The ADHA is a statutory authority in charge of implementing Australia's National Digital Health Strategy, which seeks to improve the quality and delivery of healthcare and the Australian health system by digital means.

This organisation manages the Australian My Health Record electronic health record programme. The agency also promotes other forms of digital healthcare, including telehealth and electronic prescription systems, and has an advisory role to the Government Minister for Health regarding the implementation and delivery of national digital health initiatives.an

Australian Health Practitioner Regulation Agency (AHPRA)

AHPRA is the regulatory agency of the Australian government for health practitioners. It is governed by the Health Practitioner Regulation National Laws that operate across the states and territories. The scope of its work includes managing registrations for qualified health practitioners, managing complaints and conducting audits to ensure compliance with national board requirements. AHPRA publishes guidelines for health practitioners in relation to telehealth.

2.2 Recent Regulatory Developments

Regulation of Software-Based Medical Devices

There has been a steady increase in the number of digital medical products available on the market – eg, symptom checkers and diagnostic apps, diabetes management software, and melanoma and skin analysis software. These devices may not fit easily into established pathways for review of the safety and efficacy of health technology. Furthermore, some have been created by developers with limited experience in relation to the requirements for establishing the safety and efficacy of medical devices.

On 25 February 2021, changes were made to the TG Act and the Medical Device Regulations to introduce new classification rules and better define the boundary between software which is regulated as a medical device and software

which is not. The new regulatory regime is discussed further in **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**.

At the same time, the TGA has introduced changes to the regulation of custom-made medical devices. Custom-made medical devices are and will continue to be exempt from the requirement for registration on the ARTG. However, the changes not only introduce new reporting requirements for manufacturers of custom-made medical devices, but also introduce new categories of medical devices: patient-matched medical devices and medical devices manufactured using a medical device production system (MDPS).

Patient-matched medical devices and MDPSs will need to be included on the ARTG. This is a significant regulatory development to accommodate devices, the production of which is enabled by digital technology (eg, devices which are 3D-printed from a pre-specified design envelope with adaptations to meet the needs of individual patients).

Regulation of Digital Healthcare

In recent years, especially in light of the COVID-19 pandemic, health practitioners have increasingly turned to digital forms of healthcare delivery to overcome barriers to individual access. This not only includes telehealth forms of healthcare delivery that use technology as an alternative to face-to-face consultations, but also digital information systems such as My Health Record, a federal government programme initiated in 2015, which provides an online summary of key health information, electronic prescribing systems, and systems for the home delivery of medication.

The ADHA promotes the use of these technologies and provides regulatory oversight, supporting healthcare integration and delivering improvements to the quality and efficiency of healthcare. For example, the ADHA not only promoted an increase in the use of the My Health Record system, but also expanded the system to include more Australian Immunisations Register information, assisting with the COVID-19 vaccine roll-out. In also engaging in significant education and promotion campaigns, the ADHA allows for greater individual awareness of new forms of healthcare, providing support to these individuals at a time when more traditional forms of healthcare service delivery have been unavailable or inaccessible.

2.3 Regulatory Enforcement

The TGA

The TGA has not identified any specific areas for regulatory enforcement that relate to digital healthcare or digital medicine. More generally, the TGA has a risk-based compliance framework, meaning that its response to low-risk breaches of its regulatory framework will be to educate the infringing party (particularly if that party is not a repeat offender). Its regulatory options escalate to warning letters suspending or cancelling products on the ARTG, right through to enforceable undertakings, the exercise of compulsory powers and ultimately court action.

The changes to the regulatory regimes for software as a medical device and the patient-matched medical devices outlined in **2.2 Recent Regulatory Developments** will result in changed requirements for ARTG listing of existing products. There is a transitional period for sponsors of those products to update their ARTG registrations which runs through to November 2024. It is reasonable to expect that the TGA will be

focused over coming years on ensuring that sponsors update their registrations before the expiry of the transition period.

The ADHA

The ADHA focuses on providing transparent digital health standards, as well as ensuring sustainable governance of these standards. It provides annual reports on the performance of digital health systems, in order to ensure accountability within the sector.

Given the amount of private information that exists within digital healthcare databases, privacy is a key concern of the ADHA. The agency works closely with the Office of the Australian Information Commissioner (OAIC) to maintain privacy and safety across the healthcare system. A Memorandum of Understanding between the ADHA and the OAIC exists to manage the way in which the OAIC provides advice, assistance and independent regulatory services using the personal data in the My Health Record system.

AHPRA

AHPRA provides recourse where serious concerns regarding safe and professional healthcare practices by a practitioner exist. Where a concern is received by AHPRA, it performs a risk assessment of the practitioner in the context of the concern raised.

After assessing concerns, AHPRA may take regulatory action by issuing cautions, imposing conditions on practitioners with a focus on improvement, refer the matter or aspects of the matter for further investigation by, for example, a tribunal or the police, or refer the health practitioner for a health or performance assessment.

3. Non-healthcare Regulatory Agencies

3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

The Australian Competition and Consumer Commission (ACCC)

The ACCC is Australia's competition and consumer protection regulator. It has an important role to play in policing online conduct directed at consumers, including conduct by providers of online health services. Its role includes:

- ensuring that software-based health products are not in breach of competition and consumer laws;
- protecting consumers from misleading and deceptive conduct in relation to online health services; and
- undertaking enforcement action in relation to the misuse of consumer data.

The ACCC has a specialist Digital Platforms Branch and in 2019 published the final report of its Digital Platforms Inquiry. The ACCC is currently conducting a further inquiry in relation to digital platform services (eg, search engines, messaging services and online marketplaces).

In 2018, the ACCC commenced regulatory proceedings against HealthEngine, the operator of Australia's largest online heath marketplace for alleged misleading conduct in relation to its failure to disclose to users of the platform that it was sharing user information with insurance brokers, and its failure to publish negative reviews. In August 2020, the Federal Court ordered that HealthEngine pay AUD2.9 million in penalties in respect of this conduct.

The Office of the Australian Information Commissioner (OAIC)

The OAIC, discussed in **2.3 Regulatory Enforcement**, is the national regulator for privacy and freedom of information. With respect to healthcare, the OAIC has a range of responsibilities regarding data management:

- It handles complaints associated with the collection, use and disclosure of personal health information. This includes a process whereby a person may make a complaint on behalf of a class of persons affected by a breach of the Privacy Act. The OAIC has the power to order the payment of compensation to affected individuals.
- It conducts privacy assessments to ensure that personal information, such as health information, is handled in accordance with legislative requirements. and
- It reports on and conducts investigations in relation to data breaches where personal information, such as health information, is accessed or disclosed without authorisation, or lost.

The Privacy Act recognises information about an individual's health as "sensitive information", meaning that it is subject to additional protections above and beyond those which apply to personal information generally.

The OAIC also has a statutory role under the Privacy Act in approving guidelines for the use of personal information in medical research, which are discussed in **10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information**.

While there are no specific examples of OAIC enforcement action involving the health industry, it has had a role to play in education in relation to the privacy issues arising from the government's My Health Record programme as well as its COVIDsafe App (in respect of both of which the OAIC has been given additional enforcement powers).

While neither agency has enforcement policies at present which specifically target healthcare, both have a particular focus on digital services. As the HealthEngine enforcement action shows, health service providers can be affected by that focus.

4. Preventative Healthcare

4.1 Preventative Versus Diagnostic Healthcare

The treatment of preventative and diagnostic care under the Australian health system depends not so much on its classification as preventative or diagnostic, but rather on the nature of the intervention involved.

If an intervention involves the use of a medicine or an in vitro diagnostic device, that intervention will first need to be entered on the ARTG. This involves assessment of the technology in question by the TGA in accordance with the TG Act to ensure that it is of acceptable safety, quality and efficacy. There are different requirements for medicines and medical devices, but the same agency applies those standards.

The reimbursement of such interventions again depends on the nature of the technology involved. Medicines are reimbursed through the PBS. However, more often both preventative and diagnostic interventions involve a medical procedure, which may be reimbursed through Medicare, a government scheme which subsidises the cost of medical procedures.

In order for a preventative or diagnostic procedure to be listed on the Medicare Benefits Schedule, it must be reviewed by the Medical Services Advisory Committee (MSAC). MSAC is an independent scientific committee, established by the Minister for Health to evaluate medical services, health technologies and health programmes proposed for public funding, in order to advise the Minister for Health on whether a medical service, health technology or programme should be publicly funded, and the circumstances in which it should be funded.

Further, many preventative healthcare campaigns involve not only the funding of specific interventions, but also raising public awareness about the availability and importance of such interventions. There is no specific system for the funding public health campaigns. They are funded and run by the government through either the Commonwealth or State Ministers for Health (or both). Current examples of these campaigns include the bowel screening campaign for prevention and early detection of bowel cancer, the breast cancer screening campaign, skin cancer screening campaign and the newly proposed national neonatal screening programme.

The statutory regimes that apply to diagnostic and preventative healthcare include the Competition and Consumer Act 2010 which will apply to any conduct which is in "trade or commerce".

4.2 Increased Preventative Healthcare

There are multiple factors that have contributed to the rise in preventative healthcare. From an Australian perspective this includes population health studies – eg, the 2017–18 National Health Survey – that inform policy, planning and government funding.

These studies have found that the cost and healthcare burdens on Australia's healthcare system could be alleviated by prevention and early detection programmes. Australia's ageing population has informed the preventative healthcare national bowel cancer screening programme, which is free for people aged 50 and over.

Lifestyle factors and social trends also influence preventative healthcare campaigns. An example of this is the beach culture in Australia and the preventative healthcare campaigns around wearing sunscreen and also diagnostic skin cancer checks.

The emergence of COVID-19 highlighted how important it is to have an agile health system focused on prevention and in December 2021 the Australian government introduced a national preventative health strategy for the period 2021–30. The most recent National Budget included AUD6.3 million over three years from 2023-24 to continue the Australian Burden of Disease Study and initiatives to monitor and improve the evidence base of health and wellbeing outcomes, in line with the aforementioned national preventative health strategy 2021–30.

Universally, the advancement in medical technology has improved early disease detection techniques, and the funding of preventative healthcare campaigns has changed the way people view their healthcare providers and encouraged them to become more proactive.

The reason for the change is that it is recognised by governments and insurers that preventative medicine is more cost effective than disease treatment. Whilst there is a wide range of diagnostic testing that is accessible to the public through government funding and private health-

care insurance, there is still a long way to go in further utilising all of the technological advancements in medicine to encourage prevention. There are still highly effective screening tests that are relatively inaccessible to the general public due to their high cost and the absence of a specific reimbursement pathway, for example gene sequencing, which could further assist in the detection and prevention of diseases.

4.3 Regulated Personal Health Data and Unregulated Fitness and Wellness Information

To the extent that wellness and fitness data comprises personal information, it is likely to be regulated by the Privacy Act 1988 (Cth) (the "Privacy Act").

The Privacy Act takes a relatively expansive view as to what constitutes health information. Health information includes information or an opinion about the health (including an illness, disability, or injury) of an individual, an individual's expressed wishes about the future provision of health services to the individual, and a health service provided or to be provided to an individual. Health information also includes other personal information collected to provide, or in providing, a health service to an individual.

A similarly broad approach is taken to what comprises a health service, and includes activities intended or claimed by the individual or person performing it to assess, maintain or improve the individual's health, as well as those that record the individual's health for the purposes of assessing, maintaining, improving, or managing the individual's health. Health information is a type of sensitive information under the Privacy Act, and consequently more stringent obligations and requirements apply.

The Privacy Act applies to most private healthcare providers, while state and territory legislation applies to public healthcare providers. In some instances, the state and territory legislation (eg, the Health Records and Information Privacy Act 2002 (NSW)) also extends to private healthcare providers.

The Therapeutic Goods Act 1989 (Cth) and the Therapeutic Goods (Medical Devices) Regulations 2002 set out the "Essential Principles" which provide safety requirements for manufacturers regarding the design and production of medical devices. The Essential Principles have been recently amended, including in relation to the management of data and information.

The fitness sector in Australia otherwise remains largely self-regulated, including by the voluntary application by members of Fitness Australia's National Fitness Industry Code of Practice (November 2018) (the "Code"). The Code reiterates each member's privacy law obligations and specifies that each member must not use or disclose to another person confidential information about a consumer obtained under the consumer agreement or by providing fitness services to the consumer unless the information is otherwise lawfully used or disclosed.

4.4 Regulatory Developments

Australian Digital Health Agency (ADHA)

The ADHA is a statutory authority in charge of implementing Australia's National Digital Health Strategy, which seeks to improve the quality and delivery of healthcare and the Australian health system by digital means.

The agency promotes innovative forms of digital healthcare to further proactive and accessible ways to engage with healthcare providers, including telehealth and electronic prescription

systems. The ADHA has an advisory role to the Minister for Health regarding the implementation and delivery of national digital health initiatives and preventative healthcare campaigns.

Medical Services Committee (MSAC)

MSAC is an independent non-statutory committee established by the Minister for Health in 1998. MSAC's main function is to advise the Australian Minister for Health on evidence relating to the safety, effectiveness and cost-effectiveness of new medical technologies and procedures. This advice informs Australian government decisions about public funding for new, and in some cases existing, medical procedures.

The Australian Competition and Consumer Commission (ACCC)

The ACCC is Australia's competition and consumer protection regulator. It is a non-healthcare regulatory authority that applies to preventative healthcare. The Commission oversees the conduct of medical healthcare providers and ensures that common law and practice obligations are adhered to and that anti-competitive conduct, such as market sharing or price fixing, are not adopted as part of a preventative healthcare campaign.

The ACCC has an important role to play in policing conduct directed at consumers, including those arising from preventative healthcare campaigns. Its role includes:

- ensuring that health campaigns and devices are not in breach of competition and consumer laws;
- protecting consumers from misleading and deceptive conduct in relation to health services, advertising and fees; and
- undertaking enforcement action in relation to the misconduct of healthcare providers.

The increase in government-funded, preventative healthcare campaigns and subsidies provided to medical clinics and practitioners who participate in them has meant that the ACCC has needed to focus on the healthcare industry to ensure that doctors or suppliers do not act in an anti-competitive way to obtain the exclusive benefit of such campaigns.

The Office of the Australian Information Commissioner (OAIC)

The OAIC is the national regulator for privacy and freedom of information. With respect to healthcare, the OAIC has a range of responsibilities regarding data management, such as:

- handling complaints associated with the collection, use and disclosure of personal health information (including the power to make compensation orders);
- conducting privacy assessments to ensure that personal information, such as health information, is handled in accordance with legislative requirements; and
- reporting on data breaches where personal information, such as health information, is accessed or disclosed without authorisation, or lost.

The Privacy Act recognises information about an individual's health as "sensitive information", meaning that it is subject to additional protections above and beyond those which apply to personal information generally.

The OAIC also has a statutory role under the Privacy Act in approving guidelines for the use of personal information in medical research, which often informs or forms part of certain preventative medical campaigns.

4.5 Challenges Created by the Role of Non-healthcare Companies

COVID-19 has accelerated the entrance of non-healthcare companies into the market. The companies and their services are diverse, including the entry of certain telecommunications providers and their provision of data-oriented services, e-commerce providers and their provision of entertainment and other services, and certain prominent software companies offering virtual reality technologies.

Non-healthcare companies who develop digital healthcare products find themselves confronting a more thorough regulatory regime than that which may apply to their consumer products. This may mean that the companies lack the necessary specialist skills to navigate that regime. It may also mean that the companies' supply chains are not well adapted to meeting the challenges of health product manufacture. By way of example, a company that moves from the production of consumer electronic products to medical devices may find that its existing suppliers are not able to meet the requirements of Good Manufacturing Practice necessary for the device to satisfy Australian regulatory requirements.

Furthermore, because the provision of health services is highly subsidised in Australia, non-healthcare companies need to identify and navigate the appropriate reimbursement pathways, a process which can take multiple years for some products.

5. Wearables, Implantable and Digestibles Healthcare Technologies

5.1 Internet of Medical Things and Connected Device Environment

Connected devices relating to healthcare have become one of the fastest growing categories of the internet of medical things (IoMT) revolution. Many technological developments have contributed to the advent of the IoMT; however, three of the most distinct enablers of the internet of things (IoT) in the medical sector have been improvements in connectivity, advancements in device-embeddable technologies, and greater sophistication in the applications which connect to, control and receive data from those devices. In relation to each of these the following factors are notable:

- improvements in the quality and affordability of connectivity have become central to the IoT, enabling connections across networks between remote devices and front-end applications;
- miniaturisation of sensors has vastly expanded the range of devices which can be connected and enabled; and
- innovations in applications' functionality are rapidly expanding the range of commercially useful IoMT developments that can be pursued.

To date, the most prevalent commercial adoption of IoMT is in monitoring applications and data collection. Sensors embedded in devices can be used to collect and transmit information in relation to heart rate, blood pressure, glucose levels and even information from which a patient's mental state can be determined. Other innovative applications in the development stages include ingestible sensors which can collect

information in relation to stomach pH levels and digestive health, smart asthma inhalers and even smart contact lenses. Remarkably, in addition to monitoring functionality to bolster diagnostic capabilities, IoMT applications are also being conceived and developed for robotic surgery applications, making complex interventional decisions in real time during procedures.

In relation to healthcare developments regarding remote health and in-home care after discharge from hospitals, technologies and regulatory changes enabling telehealth consultations, videoconferencing and remote monitoring through at-home devices has meant that patients can be consulted by medical professionals remotely.

5.2 Legal Implications

The Australian Consumer Law

The principal law governing product safety in Australia is the Australian Consumer Law, which codifies a single set of consumer protection laws for the whole of Australia, including but not limited to laws relating to product safety and product liability.

The Australian Consumer Law is Schedule 2 to the federal Competition and Consumer Act 2010 (Cth). However, its operation across Australia also depends on state and territory laws, which provide that it has effect as a law of each Australian state and territory.

In addition to statutory obligations, product manufacturers and suppliers are subject to obligations under the common law. In particular, persons who are injured by a product may have a right to sue the supplier of the product in negligence (as well as under statutory causes of action created by the Australian Consumer Law). An analysis of a supplier's duty to users of their product in negligence will often be important in assessing the appropriate response to a potential product safety risk.

The Australian Competition and Consumer Commission (ACCC)

The principal Australian product safety regulator is the Australian Competition and Consumer Commission (ACCC), which is responsible for administering the Competition and Consumer Act 2010 (Cth), including the Australian Consumer Law.

The ACCC has regulatory, investigatory and prosecutorial powers granted to it under the Act. In relation to product safety, those powers include the power to require the production of documents or the provision of information, including the power to examine witnesses and to enter premises, conduct searches and seize consumer goods, equipment and documents.

The ACCC also has powers to take a range of actions to protect consumer safety, including commencing compulsory recall actions and issuing product safety notices. Finally, the ACCC can issue penalty notices for breach of Australian Consumer Law or commence proceedings seeking declaratory and injunctive relief as well as civil penalties. It may also refer certain breaches of the Australian Consumer Law to the Commonwealth Director of Public Prosecution for consideration of criminal prosecution, with associated criminal penalties.

Subject to certain carve-outs, the regimes are not exclusive, so that a product that falls, for example, within the TGA's remit, may also be, in some circumstances, a consumer product that is regulated by the ACCC and subject to Australian Consumer Law.

5.3 Cybersecurity and Data Protection

The ever-increasing connectivity between medical devices, applications, healthcare IT systems and other technologies and networks unsurprisingly produces additional cybersecurity risks. These range from device malfunction and loss of data to hacking, information theft and even manipulation of the relevant device. A weakness in any aspect of these connected technologies could result in considerable harm, whether to an individual or more broadly through crippling the vital healthcare infrastructure. New technology also lends itself to new targets, and cybersecurity approaches need to be sufficiently dynamic to combat these emergent threats. Conversely, many healthcare providers also rely on legacy technology without adequate vendor support and updates, exposing those organisations to additional vulnerabilities. This creates a challenging cybersecurity scenario.

The foregoing necessitates a keen focus on, and investment in, cyber-attack prevention and response measures. From a contractual perspective this is being addressed through the introduction of specific cybersecurity and related (eg, privacy, confidentiality) obligations on suppliers, their subcontractors and, where commercially feasible, their full supply chains. This often involves layering certification (eg, compliance with ISO 27001, NIST CSF), regulatory and compliance (eg, privacy requirements including in relation to the notifiable breach scheme, data location and disclosure), penetration and other testing, and cybersecurity insurance requirements, alongside provisions which clearly set out the supplier's day-to-day and other obligations (eg, data encryption, personnel background checks, third party audits).

Accompanying this is the preference of service recipients to impose indemnities for breaching cybersecurity and related obligations (eg, privacy, confidentiality) and to ensure that the supplier's liability in respect of such obligations is sufficient (eg, unlimited or subject to a sizable cap).

Healthcare providers using Australia's My Health Record electronic medical record system are required by the My Health Records Rule 2016 (Cth) to have a written policy addressing their security arrangements in respect of access to the system, known as a 'My Health Record system security policy".

With regard to medical devices, the TGA requires that, where relevant, medical devices should be appropriately cybersecure in order to comply with safety and performance standards under the Therapeutic Goods (Medical Device) Regulations 2002. More generally, where personal information is accessed or disclosed without authority and there is a risk that the breach will cause serious harm, the Privacy Act requires organisations to inform affected individuals and the Office of the Australian Information Commissioner that serious harm may occur.

In December 2022 the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Act 2021 (Cth) came into effect. It has amended the Privacy Act to introduce a binding online privacy code for social media and certain other online platforms as well as increasing penalties for breach of the Act and enhancing enforcement measures.

5.4 Proposed Regulatory Developments

On 31 July 2021, the Australian government opened consultation on options for regulatory reforms and voluntary incentives to strengthen the cybersecurity of Australia's digital economy. The discussion paper, Strengthening Austral-

ia's Cybersecurity Regulations and Incentives, sought views on how the Australian government could incentivise businesses to invest in cybersecurity, including through possible regulatory changes.

Submissions to the discussion paper closed on 27 August 2021. Submissions were made by a diverse range of interested parties including technology providers (eg, Amazon Web Services, Atlassian, Facebook and Telstra), regulators (eg, the OAIC, ACCC and Australian Energy Regulator), industry bodies (eg, the Australian Banking Association and Medical Software Industry Association), and other interested parties (eg, universities). This work formed part of Australia's Cyber Security Strategy 2020 and responded to recommendations of the 2020 Cyber Security Strategy Industry Panel.

On 8 December 2022, and following the above, the Minister for Cyber Security announced the development of the 2023–2030 Australian Cyber Security Strategy. The strategy is designed to help achieve the Australian government's vision of making Australia the most cybersecure nation in the world by 2030. The government is developing cybersecurity policy and initiatives under four key areas:

- a secure economy and thriving cyber ecosystem;
- a secure and resilient critical infrastructure and government sector;
- a sovereign and assured capability to counter cyber threats; and
- Australia as a trusted and influential global cyber leader, working in partnership with its neighbours to lift cybersecurity and build a cyber-resilient region.

The consultation regarding cybersecurity coincided with the Australian government's review of the Privacy Act. On 12 December 2019, the Attorney-General announced that the Australian government would conduct a review of the Privacy Act to ensure privacy settings empower consumers, protect their data and best serve the Australian economy. The review was announced as part of the government's response to the ACCC's Digital Platforms Inquiry. The review has involved obtaining submissions from stakeholders in response to two consultation papers, considering feedback obtained through discussions with stakeholders on specific issues, and through existing research and reports on privacy issues.

In February 2023 the Attorney-General released the final report of the review. The report makes 116 recommendations for amendments to the Act to bring it into line with global standards for data protection. The Attorney-General invited submissions on the report, which were due by 31 March 2023.

There has been a steady increase in the number of digital medical products available on the market – eg, wearable, implantable and digestible healthcare products. These products do not always fit easily into the existing regulatory pathways for review of the safety and efficacy of healthcare.

Amendments have been made to the TG Act and Medical Device Regulations to establish classification systems specific to these new classes of medical device and to exclude some devices (eg, wearable products whose primary focus is fitness) from the registration regime altogether. These amendments are described in more detail in **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Health-**

care Technologies and 5.1 Internet of Medical Things and Connected Device Environment.

6. Software as a Medical Device

6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies

Software will be a medical device (SaMD) if it falls within the definition of a medical device under Section 41BD of the TG Act unless it is the subject of a specific exclusion.

That definition provides that a medical device includes anything (including software) which is intended to be used for:

- human beings for the purposes of diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; and
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability,

providing it does not achieve its principal intended action by pharmacological, immunological or metabolic means.

There are different categories of software that could fall within the scope of a regulatory authority, including:

- software as a medical device (SaMD) – software that, on a standalone basis, meets the definition of a medical device;
- software in a medical device (SiMD) – software that is part of a device when it is integral to the functioning of that device and is usually supplied with the hardware device; and
- software that controls a medical device – software that can control or adjust a medical device through a connection, either physical or utilising wireless technology such as Bluetooth or Wi-Fi.

The TGA uses a risk-based approach to regulating medical device technologies by examining the evidence of product risk and comparing it to evidence associated with product benefit. The higher the potential risks of a medical device, the more they need to be examined and monitored.

There are five classifications depending on the level of risk a product poses, class I, IIa, IIb, III and IV.

As described in 2.2 Recent Regulatory Developments, from 25 February 2021, new classification rules were introduced into the Medical Device Regulations for software-based medical devices, providing specific guidance on the classification levels of various types of software-based medical devices, depending on their purpose.

The effect of those changes is, in summary:

- to exclude the following from the category of medical devices:
  - (a) consumer health products which do not provide specific treatment or treatment suggestions;
  - (b) enabling technologies (eg, systems which enable telehealth consultations or the transmission of health information);
  - (c) digitised patient records;
  - (d) population-based data analytics; and
  - (e) laboratory information management systems; and
- to introduce classification rules for:
  - (a) diagnostic or screening software;
  - (b) monitoring software;
  - (c) software which recommends a treatment or intervention; and

(d) software which provides treatment in the form of information,

with the classification rules based, in each case, on the potential consequences of the disease in question and the degree of involvement of a healthcare professional in the process.

The current regulatory regime does not specifically address the use of AI as part of the technology, nor does it deal with the status of software updates. However, a software update is capable of being a recall action in respect of a medical device if it is undertaken for a safety-related reason. Indeed, a 2020 review conducted by the TGA found that in the five years to April 2020, over 20% of medical device recalls were due to software faults.

7. Telehealth

7.1 Role of Telehealth in Healthcare

Please refer to **5.1 Internet of Medical Things and Connected Device Environment** for a discussion of connected devices and the IoMT.

Commercial Adoption of IoMT

To date, the most prevalent commercial adoption of IoMT is in monitoring applications and data collection. Sensors embedded in devices can be used to collect and transmit information in relation to heart rate, blood pressure, glucose levels and even information from which a patient's mental state can be determined. Other innovative applications in the development stages include ingestible sensors which can collect information in relation to stomach pH levels and digestive health, smart asthma inhalers and even smart contact lenses. Remarkably, in addition to monitoring functionality to bolster diagnostic capabilities, IoMT applications are also being conceived and developed for robotic surgery applications, making complex interventional decisions in real time during procedures.

Associated Risks

The opportunities presented by the IoMT naturally come with associated technology and legal risks which, to some degree, correspond to the level of connectivity and functionality exhibited by the relevant solution. These range from device malfunction and loss of data to hacking, information theft and even manipulation of the relevant device. In this regard, modern security protection measures can be adopted to identify network vulnerabilities and moderate the risks of attack.

Legal risks can also arise, especially with respect to traditional legal liability.

- The extent of liability of an IoMT supplier to a healthcare institution, for example, for applications or devices that do not fulfil their stated purposes or that do not operate in the manner intended. This kind of liability may arise from misrepresentation, in negligence, under consumer law (eg, under an implied statutory warranty) or under contract (such as under an express contractual product warranty in the supply contract's terms and conditions). This is further discussed in **15.2 Commercial**.
- The liability to patients of medical or healthcare professionals who rely on the functionality and resilience of IoMT applications or devices, whether for diagnostic or interventional purposes. These issues are discussed in **15.1 Patient Care**.

Regulatory issues may also arise when IoMT applications reach a sufficient level of sophistication to be classified as medical devices. This

is explored further in **6.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technologies**.

7.2 Regulatory Environment

Many regulatory changes were made in response to the COVID-19 pandemic, with the focus on facilitating digital healthcare so that practitioners could respond to isolation requirements while continuing to offer consultations and treat patients.

Electronic Prescriptions

The National Health (Pharmaceutical Benefits) Regulations 2017 (Cth) were relaxed to permit electronic prescriptions or "e-prescriptions" under the Pharmaceutical Benefits Scheme (PBS). As explained in **1.5 Impact of COVID-19**, this allowed digital copies of prescriptions to be sent directly to pharmacies. The process still allows the patient to nominate their preferred pharmacy, as long as it has the facilities required to receive the e-prescription. These arrangements ended on 31 March 2023. However, arrangements are now in place in most Australian jurisdictions (although there is not consistency in the form of those arrangements) which permit prescriptions to be delivered by electronic token.

Videoconferencing Platforms

Videoconferencing platforms such as Zoom and Microsoft Teams have not been subjected to any regulation specifically aimed at telehealth. In fact, Allied Health Professionals Australia recommends Zoom and Skype as having useful features for telehealth. It does, however, also recommend the platforms designed specifically for telehealth, Coviu and Cliniko. Nonetheless, all telehealth consultations remain subject to the Privacy Act 1988 (Cth). While the Privacy Act does not specifically govern telehealth, practitioners must remain aware of their statutory obligations under it, as well as any relevant state and territory regimes.

7.3 Payment and Reimbursement

As discussed in **4.1 Preventative Versus Diagnostic Healthcare**, most medical practitioners' services are subsidised by the federal government through Medicare. From 13 March 2020 to 30 June 2022, temporary MBS items were introduced allowing many reimbursed services to be provided by telehealth. The federal government also increased certain incentives for medical practitioners, to encourage an increased uptake of telehealth appointments for suitable issues.

From 1 July 2022 permanent arrangements were put in place which preserved many, although not all, of the telehealth MBS items. Those arrangements were further modified on 1 October 2022 and 1 April 2023, including by the introduction of rules intends to prevent the overservicing through telehealth.

8. Internet of Medical Things

8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

Please refer to **7.1 Role of Telehealth in Healthcare**.

9. 5G Networks

9.1 The Impact of 5G Networks on Digital Healthcare

The key distinguishing feature of 5G networks as compared to their predecessors, most relevantly 4G networks, is the ability to transfer greater volumes of data at significantly higher

speeds, across lower latency connections. For example, 5G networks can reach speeds of up to 100 times faster than 4G networks and can reduce the delay between sending and receiving data from 200 milliseconds to 1 millisecond.

These advances mean that more data can be transmitted between the healthcare provider and the patient, and also that the provider can see such data in close to real time. At a basic level, provided that the hardware exists to measure a patient's physiology, this opens the possibility to remote consultations moving closer to what is currently possible in a face-to-face consultation, including in terms of a healthcare provider's ability to test the patient's symptoms and diagnose the patient by way of a virtual experience that more closely resembles a traditional physical consultation. Once these technologies exist, it is possible to imagine many applications for them.

For example, it is possible to imagine first responders to medical emergencies being equipped with portable patient monitoring systems. Data from those systems could be relayed to appropriate specialists who could advise about critical treatment needs and assist to triage the patients.

Of course, the more dependent a healthcare service becomes on a particular technology, the more difficult it is to cope with a failure of that technology. If 5G technologies come to be relied upon to facilitate the delivery of critical health services, those who are providing those services will have high expectations of the reliability, reach and security of those services, as well as critical service-level expectations in the event of a service failure. Equally, however, tensions may arise between the service-quality expectations of those administering the services and the risk appetite of upstream suppliers of standard products and services. These are matters which will need to be considered in entering into any contract for the provision of 5G services to support critical health infrastructure.

10. Data Use and Data Sharing

10.1 The Legal Relationship Between Digital Healthcare and Personal Health Information

The Privacy Act

The collection, storage and use of health information is regulated by the Privacy Act, as well as by health information-specific legislation in some of the Australian states and territories (NSW, Victoria and the ACT). State and territory legislation generally agrees with the Privacy Act, as least with respect to the manner in which consent to the collection and use of personal information is obtained.

The Privacy Act contains some specific provisions which deal with the use of health information for medical research. While it is preferable that the collection of health information for research purposes is the subject of specific consent, Section 16B of the Privacy Act provides for an exemption for private industry from the usual requirements of consent if a "permitted health situation" exists. "Permitted health situations" include situations where:

- the collection, use or disclosure of data is necessary for research or the compilation or analysis of statistics relevant to public health or public safety;
- in the case of collection, the purpose cannot be served by the collection of de-identified information;

- it is impracticable to obtain individuals' consent to the collection, use or disclosure of their data; and
- the collection, use or disclosure of data is undertaken in accordance with the relevant guidelines published under the Privacy Act.

Guidelines

The guidelines in question are the guidelines approved under Section 95A of the Privacy Act published by the National Health and Medical Research Council (NHMRC) and approved by the OAIC. The guidelines provide, among other things, that any proposal to use personal information in medical research must be approved by a Human Research Ethics Committee.

There are also separate guidelines published by the NHMRC and approved by the OAIC pursuant to Section 95 of the Privacy Act which relate to the use of personal information in medical research by public agencies.

De-identified Information

The Privacy Act does not apply to the use of de-identified information. However, the NHMRC also publishes the National Statement on Ethical Conduct in Human Research which deals with the appropriate conduct of medical research in Australia (and is the standard against which Human Research Ethics Committees approve the conduct of such research).

Clause 2.2.7 of the National Statement provides that, "Whether or not participants will be identified, research should be designed so that each participant's voluntary decision to participate will be clearly established." While this provision should not be read as a blanket prohibition on the use of de-identified data for research purposes, it does mean that it is preferable that patients are aware of how their health data will be used.

There are no specific rules or guidelines as to how consent to the collection or use of personal information must be obtained in a digital context. The collection of sensitive information, including health information, is subject to stricter requirements for obtaining consent than is the case for other forms of information. However, there is no need under Australian law for a specific collection statement. Rather, what is required is that in all circumstances it can be shown that the individual has provided unambiguous and specific consent to the collection of their health information for a specific purpose.

The Privacy Act also includes a data breach regime, administered by the OAIC. It requires organisations to report unauthorised access to or disclosure of personal information which may result in serious harm to any of the individuals to whom the information relates. The Privacy Act also permits individuals to complain to the OAIC in respect of interference with their privacy. The OAIC has the power, following investigation of a complaint, to declare that a breach has occurred and that a person or entity must perform certain acts or pay compensation by way of redress.

Finally, as the HealthEngine case discussed in **3.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies** makes clear, undisclosed use of personal information may give rise to breaches of general consumer law prohibitions on false, misleading or deceptive conduct.

11. AI and Machine Learning

11.1 The Utilisation of AI and Machine Learning in Digital Healthcare

AI's Present Role

According to some, AI is demonstrated when a machine becomes capable of emulating and applying true cognitive decision-making, self-learning from its own prior decisions and adaptively adjusting its own future decisions based on historical experience. In the IoMT context, many of the applications and devices initially deployed (such as the remote monitoring and assistive technologies referred to in **8.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things**) are, at least for now, better described as assisting and augmenting human decision-making as opposed to completely replacing it. In this respect, the primary role of these types of technologies is to provide a richer basis for the exercise of human judgement.

The Next Era of AI

Equally, however, there is also emerging recognition that significant potential exists for the next era of AI to expeditiously problem-solve, rigorously reason and apply judgement within appropriate decision parameters. Furthermore, significant resources are being furiously applied to developing independent machine learning capability – ie, machines which can improve and define their own decision processes without the need for specific human enhancement. If this can be achieved, then the implications for IoMT are significant. New IoMT applications could lead to continuously improving diagnostic capabilities, reduction in error rates, improved procedural success rates and better patient outcomes. Another key hope for digital healthcare is that IoMT will come to provide robotic assistance to interventional clinicians during medical procedures and even generate model data sets for training purposes.

The processing and interpretation of data is closely linked to the future of AI in modern healthcare. A significant advantage of computer-assisted technology over human clinicians is the capacity to analyse, process and determine patterns in vast data sets with a speed and consistency of approach that would not otherwise be possible. This would enable a new era of deductive or predictive medicine, in which systems can review data and identify patterns and characteristics which would be unrecognisable by a clinician. For instance, in Mount Sinai Hospital, New York in 2016, a computer program was trained using the electronic health records of 700,000 patients and then used to predict disease in a select sample of 76,214 patients in the "Deep Patient" initiative. Researchers noted that the results significantly outperformed those obtained from alternative learning strategies applied to original raw health records.

Risks Associated With AI in IoMT

Commentators have highlighted various risks associated with the overly rapid adoption and implementation of AI-based technologies, including the influence of machine and algorithmic bias, a failure to appreciate non-quantitative nuance and the possibility that future over-reliance on technologies may lead to a lower level of skills in future generations of medical professionals. These risks will need to be cautiously approached and managed as technologies are tested and deployed.

11.2 AI and Machine Learning Data Under Privacy Regulations

Addressing Potential Bias in AI and Machine Learning

Despite its benefits, the use of AI comes with several unique risks and challenges. The use of AI raises a number of ethical considerations, especially where AI is deployed to make decisions which can potentially adversely impact the rights and interests of individuals. Although AI can reduce the element of human cognitive biases, it has the potential to introduce algorithmic biases and to operate unfairly based on flawed algorithms. For example, there was a flawed algorithm in the Commonwealth's "RoboDebt" scheme where the process used by the AI algorithm made certain incorrect assumptions resulting in some requests for the payment of money which was not in fact owed.

The potential for bias in AI and machine learning is being increasingly considered by Australian state and territory governments, human rights bodies, and other commentators. In June 2023 the Australian government released its "Safe and responsible AI in Australia" discussion paper which seeks comments regarding the Australian government's regulatory responses to AI. This paper refers to the Royal Australian and New Zealand College of Radiologists (RANZR's) "Ethical Principles for Artificial Intelligence in Medicine" which contains nine ethical principles to "guide the development of professional and practice standards regarding the research and deployment of machine learning systems (ML) and artificial intelligence tools (AI) in medicine".

Further, the New South Wales (NSW) government's AI Policy and Assurance Framework provides guidance on the safe use of AI, finding the balance between opportunity and risk, while putting in place those protections that would apply for any service delivery solution.

There also exist AI Ethics Principles and Policies at both a federal and state and territory level in Australia. Australia's AI Ethics Principles set out eight principles designed to ensure AI is safe, secure and reliable. Further, the NSW government's AI Ethics Policy (August 2020) sets out mandatory ethical principles for the use of AI, including that the use of AI must include safeguards to ensure that potential data biases are identified and appropriately managed and that data models are designed with a focus on diversity and inclusion. The Australian Human Rights Commission's technical paper "Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias technical (24 November 2020)" identifies that algorithmic bias can cause real harm, that there is a legal imperative to address this risk, and that rigorous design, testing and monitoring can avoid algorithmic bias.

The dialogue continues, with Australia's Chief Scientist Dr Cathy Foley last year sharing her thoughts on the importance of ethics and diversity when creating next generation technologies, and that algorithms can use flawed datasets which contain inherent biases because of the inequalities in society.

12. Healthcare Companies

12.1 Legal Issues Facing Healthcare Companies

In the recent High Court decision of Calidad [2020] HCA 41 (here), the Court affirmed for the first time in Australia the doctrine of exhaustion of patent rights, and in so doing, overturned

more than a century of jurisprudence under the alternative "implied licence" doctrine.

The Court confirmed that once a patentee (or someone with the patentee's authorisation) sells or supplies patent-protected goods, the patent rights in respect of the sale or supply of those goods are exhausted, which means that (as a matter of patent law) there is nothing preventing the customer from improving the product (eg, to extend its useful working life), and then selling/supplying the products commercially without the patentee's authorisation.

Following this landmark decision, patentees (and their licensees) who sell or supply patent-protected goods to third parties should now seek greater contractual protections in respect of what the customer can do or – more importantly – cannot do, with the acquired goods, if the patentee would seek to restrict the customer's ability to improve and re-sell the products.

13. Upgrading IT Infrastructure

13.1 IT Upgrades for Digital Healthcare

The enhanced digital healthcare solutions of the future will require the coalescence of a range of enabling factors, including accessibility to robust and resilient telecommunications connections, modern software solutions, data transfer and storage solutions, and ongoing advancements in nanotechnologies to enable further miniaturisation of "smart devices". In Australia, various steps are being taken to enable these developments.

The Australian government is currently undertaking a landmark national broadband network (NBN) roll-out, which involves the deployment of a multi-technology mix of telecommunications infrastructure across the country. This is a major transformative initiative in the Australian telecommunications industry. Relevantly, significant commentary in relation to the business proposition for the NBN project focused on the potential benefits of improved access to telehealth solutions, particularly for regional Australians, and the richness of new health-related applications that could be supported by high-bandwidth connectivity. At the customer's end, the IT infrastructure of healthcare institutions, medical centres and other organisations will need to evolve to be capable of receiving and benefiting from this improved connectivity.

The Australian healthcare sector is experiencing a steady proliferation of new software and applications which are designed to support or facilitate diagnostic activities. Based on industry commentary, there appear to be mixed views among Australian medical professionals in relation to the utility of machine or software-based diagnostic tools. One view is that advancements in AI and software-based tools represent a vital tool in improving diagnostic reliability, by offering an invaluable initial assessment for further human interrogation or by way of a useful cross-check against human-based primary assessments. The contrary view is that, for seasoned medical professionals, the need to have regard to machine-based assessments and navigate false-positive machine-generated diagnoses simply adds to case review time without necessarily improving substantive diagnostic or patient care outcomes. As machine learning and medical software solutions evolve in functionality and sophistication, it is likely that confidence in AI-based tools will continue to improve, encouraging their adoption.

Data storage solutions are becoming an increasingly essential part of modern healthcare applications, including those applications which rely

on the hosting, management and retrieval of large data sets. The uptake of these kinds of applications has been accelerated by the move to cloud-based solutions and the growing mobility of medical professionals, as distinct from the traditional approach of hospitals, medical centres and other institutions maintaining local storage solutions for their healthcare and patient information.

Focus on Safeguarding and Protecting Healthcare Information

The corollary of greater levels of patient and healthcare information being held in and communicated through third-party data services is a higher level of sensitivity in relation to the safeguarding and protection of that information from unauthorised use and disclosure. To the extent that such services are relied on to maintain the sole repository of an organisation's healthcare information, this also places a greater focus on ensuring that mechanisms exist to enable the recovery or restoration of that data in the event of loss or corruption. For this reason, many contracts in the healthcare space have come to include comprehensive provisions relating to privacy, security, data protection and recovery, which bolster the statutory obligations applying to health information (being a sensitive category of personal information) under the Privacy Act.

13.2 Data Management and Regulatory Impact

We are not aware of any proposed or enacted regulations that specifically concern the implementation of IT upgrades. However, it can be the case that IT upgrades are necessitated by other regulatory developments (eg, the implementation of privacy and data protection requirements). Further, it is clear that software is treated as "goods" under Australian Consumer Law meaning that manufacturers and suppliers of software will be subject to, among other things, consumer guarantees in respect of their software which cannot be excluded by contract.

14. Intellectual Property

14.1 Scope of Protection

Patent Law

Patent law may protect an invention in digital health that meets the standard requirements under the Patents Act 1990 (Cth). An invention must be a manner of manufacture that is new, useful and involves an inventive step. This means business methods will not be patentable unless they involve the direct application of a physical form or device, in a technically innovative way, to bring about a useful result. Mere schemes implemented using generic software will not constitute patentable subject matter (eg, Encompass Corporation Pty Ltd v InfoTrack Pty Ltd (2019) 145 IPR 1).

Copyright Law

Copyright law will protect an original literary work (such as computer code) that is the product of an identifiable human author or authors. This means the original literary work must be the product of independent human intellectual effort directed to the creation of the material form of that work (eg, Telstra Corp Ltd v Phone Directories Co Pty Ltd (2010) 90 IPR 1).

Databases

There is no database right under Australian law per se. Australian law also offers no protection for databases that are created without direct human authorship. Works of authorship created by AI technologies, without any substantive human input, are not protected or owned by anyone, even if the computer code behind an AI was authored by a human and is itself protected.

Secrets

Trade secrets can be protected as confidential information by way of contract or equity. By ensuring anyone with access to trade secrets is bound by appropriate obligations of confidence, such as in the terms of an employment contract or non-disclosure agreement, the confidentiality claimant can enforce any breach of those contractual obligations. If no contractual obligation exists in relation to the trade secret, a confidentiality claimant may be able to bring an equitable action for breach of confidence.

14.2 Advantages and Disadvantages of Protections

Different forms of IP protection will be better suited to different types of innovation/creation. Commercialisation strategy also plays an important part in deciding what form of protection to seek and when to do so. The following comments give a high-level overview of some of the relevant considerations.

Copyright

Where innovation lies in the way in which an idea has actually been expressed, in material form, copyright protection may be a suitable form of protection to prevent third parties from copying that work. An advantage of copyright is that it subsists upon the creation of an original work; there is no requirement to register any copyright claims in Australia. A disadvantage of copyright is that it does not protect the idea itself (as opposed to the expression of the idea), which means it is generally ill suited to protecting new and valuable ideas that can be easily replicated in material form by third parties without copying the original work itself.

Patents

Where value lies in an inventive concept itself, which can be applied industrially in one or more ways, patent protection may be a better suited form of IP. Patents offer a patentee a limited monopoly to exploit the claimed invention (generally 20 years for a standard Australian patent), in exchange for the patentee disclosing to the public at large the nature of the invention and how to perform it. Patents have the advantage of protecting different embodiments of the claimed invention. They are also generally well suited for technology where details of the working of technology will need to be disclosed publicly in order to commercialise the product (as is typically the case with healthcare products, where lots of information is disclosed publicly through the regulatory approval process). A particular disadvantage of patent protection is the cost involved in enforcing patent rights. The limited duration means patents are also generally ill-suited to innovations in respect of which 20 years is insufficient time to realise the commercial value before exclusivity is lost.

Trade Secrets

Trade Secrets (ie, information bound by obligations of confidentiality in contract or equity) are another important form of protection. The primary advantage of trade secrets is that they do not expire. Thus, if confidentiality obligations are enforced rigorously, the information may in theory be protected from third parties indefinitely. Trade secrets are generally ill-suited to products or inventions where the act of commercialising the product will necessarily involve the disclosure of its working to the public (as is typically the case with healthcare products). In those circumstances, patent protection may be more appropriate.

14.3 Licensing Structures

Contractual licensing arrangements for IP rights in digital healthcare can adopt a broad range of different structures. At a high level, licences to

exploit IP rights can be either exclusive, sole, or non-exclusive. For some IP rights, such as patent rights, an "exclusive licence" has a special meaning under the relevant legislation, as meaning a licence where the owner licenses all the rights to another person, to the exclusion of all others - including the actual owner. A properly constituted "exclusive licence" may enable the exclusive licensee to commence infringement proceedings against third parties, without needing the owner's consent (although the owner must generally be joined as a party to such proceedings).

Licensing structures may otherwise be customised to suit the needs and commercial objectives of the parties. They can be perpetual or for a limited term. They may be irrevocable, or revocable upon certain circumstances arising (such as non-payment of royalties). They may be royalty free or have a payment structure involving anything from the simplest per-unit royalty rate to the most complex formula for calculating costs and revenues and allocating them as between the parties to the licence.

14.4 Research in Academic Institutions

Inventions and works of authorship that are the product of joint inventors or authors may not be exploited by third parties without the consent of all of the co-inventors or co-authors. A single co-owner of copyright or a patent cannot authorise a third party to exercise the exclusive rights afforded by that copyright/patent without licence from the other co-owners. In practice, this means co-owned IP rights may be more difficult to commercialise, and therefore of lower commercial value, than such rights owned by a single entity.

14.5 Contracts and Collaborative Developments

Inventions and works of authorship that are the product of joint inventors or authors may not be exploited by third parties without the consent of all of the co-inventors or co-authors. A single co-owner of copyright or a patent cannot authorise a third party to exercise the exclusive rights afforded by that copyright/patent without licence from the other co-owners. In practice, this means co-owned IP rights may be more difficult to commercialise and, therefore, of lower commercial value, than such rights owned by a single entity.

15. Liability

15.1 Patient Care

Functional Approach to Regulation of Technology

Fundamentally, the traditional approach of the Australian legislature has been to avoid technology-prescriptive regulation and instead impose functional requirements in a technology-agnostic way. This has been a consistent theme across a range of sectors. This philosophical approach often stands in contra-distinction to European-based directives or statutory requirements in other countries, which can be more technology-specific in nature (eg, in relation to mandating particular technology standards relating to data transfer, encryption levels and electronic attestation). Generally, Australian laws, which are predicated on, or which relate to a base assumption of human decision-making have not evolved to mandate the adoption of particular technology standards as a substitute for that human decision-making process, nor to automatically alleviate responsibility for a human decision based merely on reliance on a prescribed technology process.

Liability for Decisions Based on AI Solutions

In Australia, liability for medical decisions with an impact on patient outcomes will often be determined according to the common law tort of negligence. Establishing negligence relies on demonstrating the existence of a duty of care, defining the appropriate standard of that duty, proving that such standard has been breached and showing that a certain measure of damages has flowed from the breach. The determination of these various elements will always depend on the specific facts and circumstances of a particular case; however, no general rule or principle exists to the effect that a medical professional who exclusively relied on an AI-based solution in substitution of their own judgement will be exempted from liability. Relevant factors will include the extent to which it was reasonable to rely on a machine-based assessment, the extent to which the medical professional was reliant (eg, whether in relation to the interrogation of specific data points or in relation to an overall AI-based recommendation) and potentially, to some degree, the level of sophistication of the solution provided by the AI and the proven integrity of its outputs.

It is also likely that the developers of such systems could be liable to patients for their consequences both under theories of negligence and under statutory liability regimes which impose liability on manufacturers of goods.

15.2 Commercial

Where a third-party vendor supplies products or services to support the operations of hospitals, medical centres or other healthcare institutions, the liability for the non-performance or non-conformity of those products or services with their intended requirements will typically be regulated by the applicable contract of supply. The terms and conditions of that supply contract will usually, assuming it is consistent with best practice:

- contain various warranties, performance and delivery comments in relation to the applicable products and services;
- outline security (including cybersecurity), data protection, disaster recovery and business continuity obligations owed by the vendor;
- include indemnities in relation to particular kinds of risks that could create exposure for the customer, including in relation to the third-party vendor's breaches of law or regulatory requirements and other types of third-party claims brought against the healthcare institution as a result of the vendor's activities; and
- set out a contractual allocation of risk in relation to legal claims arising in relation to the contract or its subject matter.

The extent of the vendor's liability and how risks are contractually allocated will largely depend on the parties' commercial understanding with respect to the relevant scope of the products and services. For instance, it may not be appropriate for a third-party vendor to indemnify the customer against all cybersecurity attacks if it is only responsible for providing a discrete solution for the customer's deployment and is not otherwise assuming responsibility for the security and integrity of the customer's network environment in which that solution will be deployed and implemented. In such circumstances, the vendor's liability may be more appropriately confined to security vulnerabilities in the solution itself. Conversely, if security management and network integrity fall within the scope of the professional services the vendor is supplying, then a greater level of contractual protection against such events would be justified.

The contract of supply will usually also outline how any limitations on the vendor's liability interact with any common law claims arising from its activities (eg, arising in negligence) and, to the extent that it can be legally altered by the contract, any statutory liability.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com