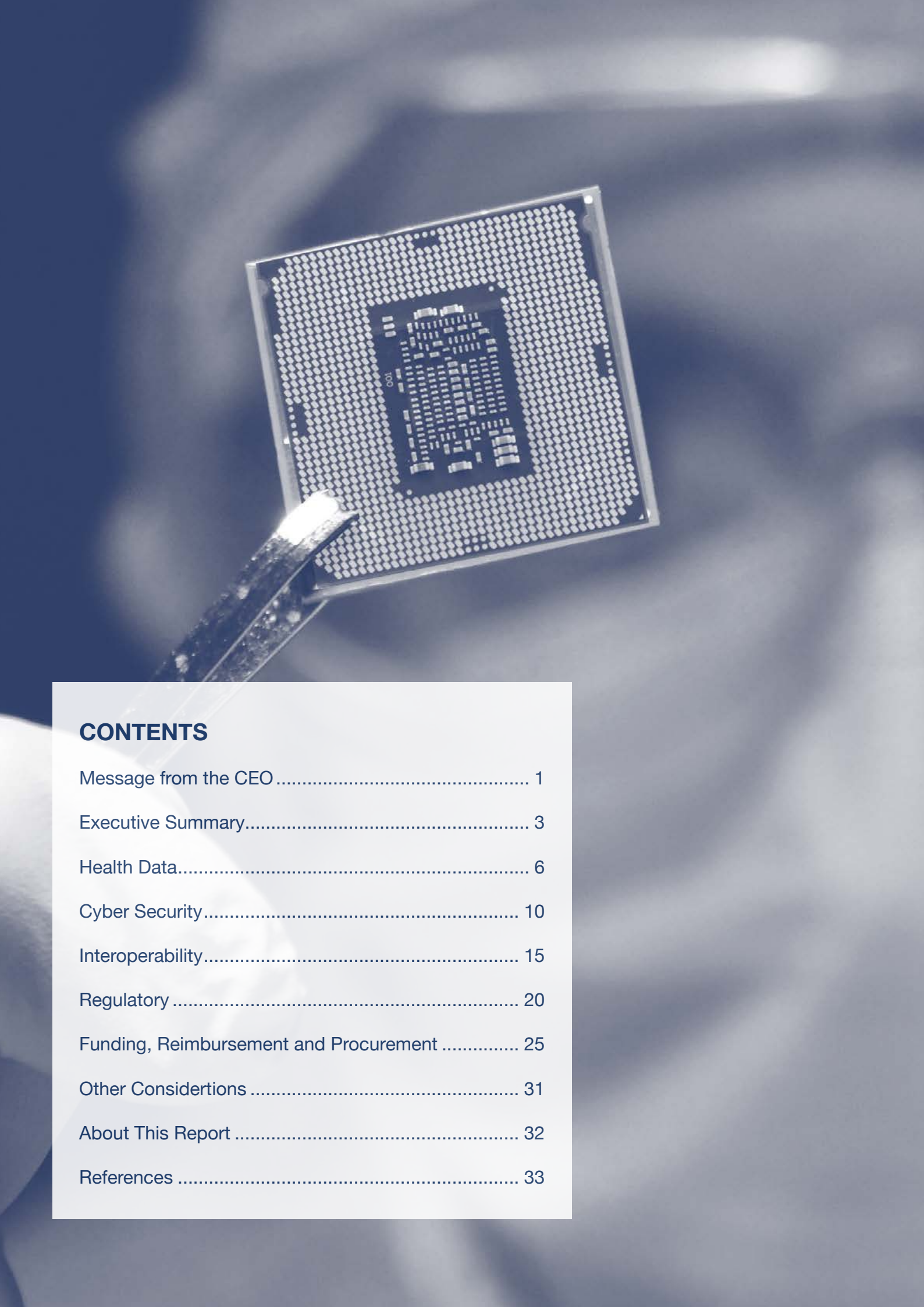
DIGITAL HEALTH

Breaking Barriers to Deliver Better Patient Outcomes

MTAA Medical Technology ASSOCIATION OF AUSTRALIA



CONTENTS

MESSAGE FROM THE CEO

IAN BURGESS

Chief Executive Officer
Medical Technology Association of Australia

Publicly funded healthcare systems around the world are facing increased demand due to ageing populations, rising levels of chronic disease, and expensive medical procedures. Set against this backdrop, digital health has long been seen as critical to improving care outcomes, patient experiences, and cost reduction.

Digital health is a key priority for Medical Technology Association of Australia (MTAA) and its members as reflected in the MTAA Strategic Plan 2022-2025. Our unrivalled understanding of therapeutics, care providers, and patients will play a crucial part in this next evolution of healthcare.

However, we are concerned that current approaches to regulation and reimbursement have not been updated to reflect advances in technology and models of care. Change is needed to support the adoption of specific digital health products and services in Australia.

To advocate for change and address the challenges facing Australia's healthcare system, MTAA commissioned research through the University of Newcastle. We wanted to better understand the digital health needs, opinions, and experiences of the MedTech sector via members, sister organisations and other key stakeholders.

The aim of this paper was to identify opportunities for digital health uptake and barriers that need to be overcome. It proposes practical policy solutions with an emphasis on current and emerging technologies.

MTAA is committed to ensuring all Australians have access to the health and wellbeing benefits delivered by digital technology. This health equity is the true value of digital health, facilitating evidence-based care for all, especially those in underserved and marginalised communities. Unlocking the true potential of digital health will not be possible without access to the full range of medical technologies the industry has to offer.

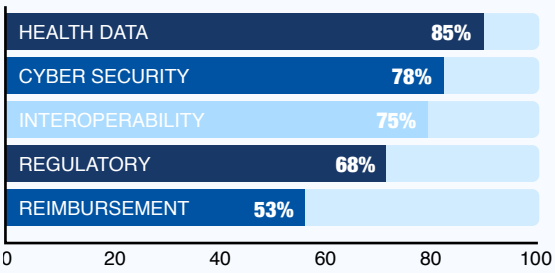
EXECUTIVE SUMMARY

Australia has many healthcare challenges to overcome, from lengthening hospital waitlists and unsustainable cost growth to an ageing population with rising levels of chronic disease. Care is often fragmented, and valuable health data generated across the system is underused.

Digital health has a central role to play in tackling these issues. Technologies including telehealth, electronic health records, wearable devices, mobile health applications and digital therapeutics are increasingly being embedded in the healthcare system. These provide an opportunity to improve patient outcomes and reduce costs by increasing the availability of relevant information, allowing better diagnosis, treatment and care.

This is reshaping how healthcare products and services are developed and delivered, changing the relationship dynamics between patients, healthcare providers, health institutions, and regulators. But we need the right policy settings in place to accelerate this change if we are to maximise the benefits for patients and the healthcare system.

MTAA's Digital Health survey, research and stakeholder interviews have generated valuable insights into the challenges facing the healthcare sector in adopting digital technologies. Although the growth and advancement of digital health technologies has brought new opportunities for the improvement of healthcare services and patient outcomes, there are constraints on the uptake and effective use of these technologies. The five major areas of concern identified by survey respondents were:



Australia's healthcare system has a good track record of developing and adopting digital health technologies to improve healthcare delivery. However, uptake and effective use still lags other regions in some key areas. Digital health is also still evolving, which means that the healthcare system must be able to incorporate innovation into its workflows and treatment options. Our research shows that opportunities are still being missed to accelerate digital health uptake.

"With the right short and long term policy settings, incentives and appropriate regulatory framework, I believe digital health represents the single greatest opportunity to transform health care in Australia."

The Hon Mark Butler MP, Minister for Health and Aged Care, Summit on Clinical Governance in Digital Health C3.0 Connect. Care. Confidence, 7 Feb 2023

For Australia to remain a leader in an increasingly digital world, it must remain focused on addressing the challenges presented by regulatory and reimbursement processes. These include lack of coverage, inconsistent and outdated cyber security approaches, inadequate oversight and compliance of health data, and poor integration between health systems. Only by solving these problems will we be able to harness the full potential of digital health technologies to improve patient outcomes in Australia.

HEALTH DATA

The digitalisation of healthcare is rapidly increasing the volume of available data. Research firm IDC estimated a 50-fold increase in just 8 years. Effective governance will be crucial in maximising the effective use of this data while maintaining consumer confidence. Important considerations include secure storage, de-identification protocols, effective management strategies, well-defined consent frameworks, and permissible uses of data. While the Privacy Act 1988 (Cth) provides a national law on data privacy, there is a diverse range of data governance standards across governments, sectors, institutions, and organisations, each set up with good intentions. This increases complexity and heightens the risk of data misuse. A single, clear, best practice framework for health data governance would address this concern, encouraging appropriate data use and building consumer confidence.

CYBER SECURITY

To make best use of digital technologies, public confidence in the protection of health data needs to be high. This has been highlighted by recent well-publicised hacking events. Australia's regulatory framework for cyber security is considered best practice, but defences are only as effective as their weakest link. Organisations should follow the Australian Cyber Security Centre's Essential Eight guidelines, but additional policy initiatives are required. More consumer education is needed so people understand that moving to more modern technology systems will improve data security and access management rather than increasing risks.

INTEROPERABILITY

Effective data sharing is vital in improving patient outcomes and increasing operational efficiency. Interoperability is the cornerstone of sharing health data between patients, carers, practitioners, healthcare providers and health departments. The challenge is that patient data has been recorded across disjointed systems, with various terminologies, formats, and data standards in use. Technical and semantic standards and regulations need to be put in place to support the seamless exchange of health data between different systems and providers. This highly desirable goal is well understood but needs to be supported by agreed standards supported by incentives and/or mandates

REGULATORY

For many digital health technologies, regulatory approval is the first step to patient and provider access. Australia's Therapeutic Goods Administration (TGA) is recognised as a global leader in regulatory approaches, but the evolving nature of digital health technologies creates ongoing issues and the need for more flexible approaches. Rapid growth in the software as a medical device (SaMD) trend is expected and software upgrades for these devices will be frequent. There are opportunities for TGA to adopt faster and more flexible pathways used overseas. Clear distinctions between security upgrades and product recalls would help to avoid consumer and healthcare provider alarm.

FUNDING, REIMBURSEMENT & PROCUREMENT

As digital technologies become an increasingly essential component of healthcare, it is essential that all Australians have equitable access to their benefits. And yet unlike some other countries, there is no funding pathway for most regulated digital applications that patients would use at home. Furthermore, health technology assessment (HTA) pathways are not specifically constructed to account for the requirements of digital health, frequently demanding unrealistic levels of data. Slow and cumbersome purchasing processes fail to take the specific benefits of digital health into account. Coverage needs to be expanded and payment approaches adapted to ensure patient access and institutional support for digital health.

The digitalisation of healthcare is an essential element of reform in the next decade and beyond. Australia has made solid strides in this transformation, but vestiges of the pre-digital era and the peculiarities of our system still create roadblocks. This report highlights these challenges in five key areas identified by MTAA members and partners as priority issues and offers practical solutions for adoption. MTAA and its partners welcome further dialogue on these issues and collaborative implementation of agreed solutions that benefit patients and all stakeholders across the healthcare system.

MTAA RECOMMENDATIONS

HEALTH DATA

1. The implementation of a national data governance framework, including legislative measures that provide consistent guidance on data collection, management, and sharing across all states and territories.
2. Australian policy makers ensure Australia is aligned with data sharing principles outlined by global, cooperative networks.

CYBERSECURITY

3. The TGA consider a different approach to communicating and addressing cyber security vulnerabilities, changing the recall process and the language used to describe recall actions, as well as the reasoning behind the proposed recommendations.
4. That policy directives apply uniform provisions to all players in the supply chain to avoid an excessive and unnecessary burden for manufacturers.
5. Regulatory agencies and peak bodies across Australia promote efforts to enhance cyber security awareness through fundamental training programs for healthcare professionals and patients.

INTEROPERABILITY

6. The establishment of a national interoperability framework. In adopting global interoperability standards, technologies, protocols and guidelines, Australia can align with other regions and share best practices.
7. Introduce financial incentives and other benefits for healthcare organisations that encourage the adoption of these standards and technologies, and/or mandates that enforce adoption.

REGULATORY

8. TGA and other global regulators to keep up with international trends in AI/ML to ensure manufacturers and sponsors are provided with guidance and education in a timely manner.

REIMBURSEMENT

9. A review of current activity-based funding models, MBS fee for service arrangements and limitations on private health insurance providing out-of-hospital care. These disincentivise digital health purchasing in favour of driving down costs.
10. The Australian Government commence a process to develop a value-based assessment framework specifically for digital health, as part of the current HTA review.
11. The Australian Government develops and commits to a reimbursement pathway for digital health apps, so Australians are have subsidised access for to health apps that have demonstrated health benefits.

HEALTH DATA

Healthcare devices produce huge amounts of data. Research firm IDC estimates the volume of global healthcare data grew fiftyfold to 25,000 petabytes between 2012 and 2020.[1] There is an urgent need to address key questions related to storage, deidentification, management, consent frameworks, and permissible uses in ensuring safe data governance.

The implications of proper data governance procedures affect the MedTech industry, government, research organisations, and most importantly, patients and consumers. Shared responsibilities include safeguarding privacy, ensuring the secure and ethical use of health data, advancing medical knowledge, and empowering patients and consumers to better manage their health.

Striking the right balance between protecting consumers with policies and regulations while giving organisations the ability to access and share health data is challenging. Global harmonisation of health data governance policies is an emerging trend aimed at addressing these challenges.[2]

However, the lack of a national data governance framework and the fragmented way states operate are proving burdensome for industry, healthcare providers and research institutions. The focus in this section of the paper is on ensuring the privacy, security, and safety of health data through effective data governance and regulation.

MTAA aligns with the Australian Digital Health Agency's proposed delivery roadmap, which prioritises using health information for research and public health purposes, planning for emerging data sources and technology, and monitoring and evaluating outcomes and progress.

OVERVIEW

Australia has a complex data privacy and secondary use of health data model governed by laws, regulations, and guidelines at national and state and territory levels. At the national level, the Australian Privacy Principles set out in the Privacy Act 1988 (Cth) apply to the handling of personal information, including health information, by Australian government agencies and private sector organisations.[3]

At state and territory level, health information is subject to privacy and confidentiality requirements set out in various privacy laws and regulations that vary across jurisdictions. The fragmented nature of Australia's privacy and data governance landscape was apparent during interviews with industry stakeholders, with the lack of national harmonised strategies surfacing as a common theme.

The health data landscape presents significant challenges, placing unnecessary strain on MedTech organisations and healthcare institutions that hinders advancements which would benefit patients and consumers. Unlocking the full potential for the secondary use of health data while ensuring its privacy and security presents an enormous opportunity to improve the health outcomes of all Australians.

Consent agreements, the right to erasure, and secondary use of health information definitions and requirements are all governed under Australia's Privacy Act. At the time of writing this report, consultation regarding reforms to the Act are underway.

The Privacy Act includes provisions for the secondary

Five Safes Framework

use of health data for research purposes, which aligns with consumer sentiment. In a 2016 study, 91% of respondents said they were willing for their health data to be used for research. Another survey in 2017 found that 93% supported their medical records being used for similar reasons.[4]

To ensure that health data is used in a safe, responsible, and productive manner, Australia should adopt a comprehensive national data governance framework. While various data governance frameworks exist across the nation, such as the Australian Institute of Health and Welfare (AIHW) framework, it has not been implemented nationally and is not legally binding.[5]

The national data governance framework should encompass legislative measures that provide consistent guidance on data collection, management, and sharing across states and territories. It should also clarify the roles and responsibilities of all stakeholders and data custodians, ensuring that privacy and security protections are well-defined, transparent, and accountable. The framework should streamline data collection and management processes, establishing clear principles for data sharing that promote collaboration and innovation across the health sector.

Embedding the Five Safes framework into national data governance would help to ensure that health data is collected, managed, and used in a secure and responsible manner.[6] This widely recognised framework includes strategic, privacy, security, ethical, and operational considerations to ensure a complete and thorough evaluation of the risks involved in data sharing or release. The Data Availability and Transparency Act 2022 incorporates data sharing principles based on the Five Safes framework.[7] This framework has been widely adopted by organisations including the Australian Bureau of Statistics, multiple Australian government agencies, and international statistical organisations such as the Office of National Statistics in the UK and Statistics New Zealand.[8, 9]

The governance and protection of health data varies significantly in terms of legal frameworks, ownership, and sharing principles. These variations are reflected in the diverse approaches to safeguarding personal data through legislative measures, as well as in the ownership rights of individuals over their health information. Increasing efforts to harmonise approaches are seen in the European Union (EU) and other markets.

The General Data Protection Regulation (GDPR) was adopted by the EU to protect the privacy and personal data of individuals. It came into effect in 2018.[10] As a set of minimum standards, the GDPR sets out strict requirements for how personal data must be collected, processed, and stored. It gives individuals significant control over their personal data, including the right to access, rectify, or erase their information.

These strict requirements have some drawbacks, making regulation onerous for small to medium organisations that lack the resources and expertise to fully understand and implement necessary measures. Concerns have also been raised around the potential to stifle innovation and hinder the development of new technologies due to its strict requirements for data protection and privacy.

Although the GDPR acts as a baseline for EU countries to follow, individual nations including France and Germany overlay their own requirements that go beyond it. If Australia was to go down the road of harmonisation, it would be prudent to create an approach that balances individual rights with the potential benefits for all in using health data for research and service improvement. It should also consider the cost of compliance in this relatively small market.

The establishment of the Global Digital Health Partnership (GDHP) is a broader effort to standardise global digital health approaches.[3] Launched in 2018, the GDHP is a cooperative network

of governments, government agencies, and international organisations. It aims to enhance the use of digital technology in healthcare and foster a more interconnected and interoperable global health system. The partnership has 33 member countries and territories at the time of writing, as well as three international bodies, including the World Health Organization (WHO).[3]

The GDHP and the Global Medical Technology Alliance (GMTA) jointly advocate for a global framework that promotes and facilitates international health data exchange, encompassing a broadly acknowledged framework for responsible health data sharing that emphasises legitimate purposes and appropriate safeguards.[11] For instance, multi-regional clinical trials, which regulatory authorities such as the US Food and Drug Administration and the European Medicines Agency recognise, are no longer restricted to particular states or countries. The effectiveness of such trials depends on the ability to share and access data across borders, which should be encouraged because access to international datasets conforming to Australian requirements is cost-effective and secure.

The COVID-19 pandemic illustrates the importance of cross-border data sharing as real-time health data from multiple sources and countries was critical in limiting the spread and impact of the virus. More broadly, this cross-border sharing is pivotal for improving healthcare outcomes, informing policies, and addressing global health challenges.

CHALLENGES

The effective management of health data is crucial to ensuring the privacy and security of sensitive information, as well as its quality and accuracy. The barriers faced in the governance of health data in Australia include data privacy and security concerns, lack of standardisation, and complex legal and regulatory frameworks. These must be carefully considered and addressed to realise the full potential of digital health technologies.

The lack of a national harmonised data governance framework hinders the safe and effective use of health data. Challenges associated with collection, management, and sharing are exacerbated by the many inconsistencies between states and territories. This hampers efforts to unlock the full potential of health data. It is imperative that these challenges are addressed.

The absence of a harmonised data governance framework and comprehensive guidelines for data sharing undermines patient trust, putting sensitive health information at risk of unauthorised access and misuse. Breaches of privacy can result in serious harms, including reputational damage and financial loss. Effective governance must include robust security measures, including encryption and access controls, to minimise the risk of unauthorised access.[12]

Legal and regulatory requirements including data privacy laws, health insurance regulations, and intellectual property laws can be complex to navigate, particularly for emerging digital health technologies.[2,13,14,15] This creates uncertainty around the roles and responsibilities of different stakeholders, often causing delays and increasing costs. A comprehensive national data governance framework would remove the need for different approaches within states and territories.

Australia faces numerous challenges due to strict data sharing practices which stifle the use of health data. These data sharing practices also create inefficiencies, as data is often siloed and duplicated in multiple formats across different healthcare organisations. This goes against the global trend of cross-border data sharing, hampering collaboration and innovation.

RECOMMENDATIONS

Australia needs a harmonised approach to data governance. One respondent during interviews with MTAA members emphasised the need for a “do it once, do it everywhere” approach with nationally aligned policies and regulations that reduce legislative complexities.

This national data governance framework is an important first step if Australia is to unlock the full potential of health data. The Health Data and

Information Governance and Capability Framework developed by the Canadian Institute for Health Information is a prime example.[16] This framework serves as a comprehensive guide to managing health data in Canada, offering guidance on all aspects of governance, from data quality and privacy to access and interoperability.

A harmonised framework enhances collaboration and interoperability across healthcare organisations and systems. By enabling standardised approaches to data collection, coding, and classification, the framework promotes more meaningful analysis and better patient outcomes. Moreover, it increases consumer confidence and patient trust by ensuring that health data is managed transparently, securely, and ethically.

Recent data breaches have eroded national public trust in institutions and organisations regarding data privacy, as highlighted by research from the Australian National University. Between August 2022 and October 2022, national public trust fell more than 4%.[17] This decline was observed in technology and telecommunication companies, universities and other academic institutions, and the Australian Bureau of Statistics (ABS).

These findings have important implications for health data privacy, particularly given the role that universities and the ABS play in its collection and analysis. By adopting a standardised approach to health data governance, Australia can address concerns raised by recent data breaches and promote greater public trust in the institutions and organisations responsible for managing health data.

Australia would also benefit from aligning with data sharing principles outlined by the GDHP and GMTA. Australia's regulations are stricter on the transfer of personal information outside of Australia, requiring the consent of the individual concerned. The GMTA proposes a more harmonised approach to cross-border data transfer, based on common standards and a risk-based approach. This provides a more flexible and practical framework for cross-border data transfers, while maintaining high standards of privacy protection.

Adopting key data protection and privacy principles, along with customised security measures for data processing, would establish a baseline of lawfulness and fairness that spans international borders.[11] This would simplify the process of international data transfers while protecting patient privacy rights. Increasing the global availability of research data enables the identification of patterns that may not be visible within a single country's data pool. The insights gained from such data analysis accelerates the development of new treatments and contributes to disease prevention efforts, resulting in better patient outcomes.

This would simplify the process of international data transfers while protecting patient privacy rights. Increasing the global availability of research data enables the identification of patterns that may not be visible within a single country's data pool. The insights gained from such data analysis accelerates the development of new treatments and contributes to disease prevention efforts, resulting in better patient outcomes.

CASE STUDY

Real-time health data enables better care for Australians with chronic illness

Tunstall's Brightwater Connected Health Project provides self-monitoring capabilities to people with chronic health conditions through tablet devices and monitoring software. It uses an integrated care platform (ICP) to transmit health data. If this health data produces readings outside of a patient's monitoring plan range, a nurse can coordinate an appropriate response.

The live monitoring and reporting of a patient's health data is done in a way that empowers nurses to easily identify trends or changes in their patient's health – and share this vital information with the patient's GP. It demonstrates the importance of accessible and meaningful data when and where clinical decisions are being made.

CYBER SECURITY

The internet has fundamentally changed how the world interacts and operates, with a wide range of activities from banking to shopping performed online. There is a growing need for digitalisation of the healthcare sector, and for medical devices to be connected. This brings new opportunities for innovation that will improve patient outcomes, but risks need to be managed. This includes the security of medical devices and the privacy of data they collect

Cyberattacks are a growing threat to healthcare and There have already been significant cyber security incidents. In one example, more than 78 million health records were stolen from US-based Anthem.[18] The WannaCry attack back in 2017 infected more than 200,000 computers in more than 100 countries.[19] In the UK, the National Health Service reports that WannaCry infected 25 acute care hospitals, disrupting medical systems, and devices including MRI machines. At five of the infected hospitals, emergency ambulance services were diverted to other non-affected centres.[19]

Here in Australia, recent high-profile attacks on Optus and Medibank have brought cyber security to the forefront of public consciousness. However, it's important to remember that the cyber security risks associated with digital health applications are not new. All health data at every level, from a GP's laptop to a hospital's records system, carries risks that needs to be effectively managed.

OVERVIEW

The focus of this section will be on the various regulatory aspects related to the development and maintenance of safe and secure medical devices throughout the entire product lifecycle. When surveying MTAA members and relevant industry stakeholders, 78% of respondents said cyber security was a pertinent concern to their organisation.

Governments and industry must minimise the likelihood of physical or psychological harm to patients and consumers. Thankfully, Australia's regulatory landscape for cyber security in medical devices is widely recognised as strong and well-established.

The TGA published an update to its industry specific guidelines in 2021 regarding cyber security for medical devices.[20] This aligns with existing overseas regulatory requirements and supports the implementation of risk-based regulatory approval pathways that are guided by the Australian Government's Cyber Security Strategy 2023-2030.[21] Adhering to international standards helps to demonstrate that medical devices meet cyber security requirements, promoting the safety and security of patients and consumers. Australia is an important player in the global MedTech industry, but as a relatively small market, cyber security strategies are typically developed overseas and adapted appropriately to meet Australian standards.

In the MTAA's digital health survey, 90% of respondents indicated that their cyber security strategies took a global approach rather than being developed for the Australia market. The TGA approval process allows for this approach. It does however signal the importance of continued collaboration in aligning Australia to international standards, including the relevant ISO standards.

The TGA is responsible for ensuring the safety and quality of medical devices in Australia. In cases where medical devices are found to have deficiencies or potential deficiencies related to cyber security

vulnerabilities, the TGA mandates recall actions.[20] The TGA's Uniform Recall Procedure for Therapeutic Goods (URPTG) provides guidance on the process for conducting recalls, including the roles and responsibilities of all stakeholders involved, and the steps manufacturers must take to notify the TGA and affected parties (see section Regulation).[20] It also provides recommendations for effective stakeholder communications during the recall process. This recall process, specifically the wording as it relates to cyber security and digital health products, was highlighted as an area of potential improvement during in-depth stakeholder interviews.

More broadly, organisations can protect themselves from cyber threats through prioritised mitigation strategies. The most foundational of these strategies is the Essential Eight defined by the Australian Cyber Security Centre.[22] The objective of the Essential Eight is to prevent the delivery of malware, reduce the likelihood of cyber incidents, and provide a foundation for organisations to tackle risks and safeguard online systems.

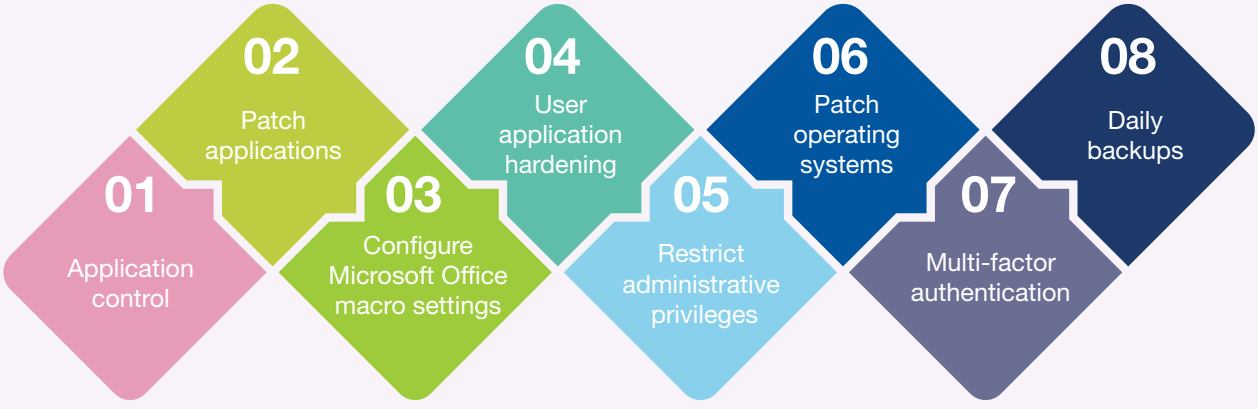
The Essential Eight was highlighted during the survey as an advantageous cyber security strategy, with its various applications widely used by participating organisations. Multi-Factor Authentication was the most heavily adopted principle (89%), while patching operating systems and contingency planning were the least popular (each 74%). Patching is a critical component of cyber security strategy as it helps to address vulnerabilities and protect against known threats, so this under-reporting highlights an obvious area for improvement.

Regions are adopting similar approaches to managing cyber security throughout the total lifecycle of medical devices, from design and development to end-of-life, but there is growing recognition of the need for global policy standards.

The International Medical Device Regulators Forum (IMDRF) harmonises regulatory requirements for medical products that differ from country to country.[24] It aligns with the European Commission and the FDA in efforts to draft a Cyber Security in Medical Devices guideline.[25,26] This forum emphasises the need for medical device manufacturers to focus on the entire product lifecycle. Recent changes to the TGA cyber security guidance for medical devices has brought Australia's policies up to par with other regions include the EU and US.[25]

The IMDRF promotes the use of relevant standards such as IEC 80001-1, ISO 31000, and the ISO 27000 series.[27,28,29] In particular, the IEC 80001 series of standards, promoted by organisations including the European Association of Medical Devices of Notified Bodies, provides guidance on the use of medical devices in a networked environment, helping to ensure they are integrated and used in a secure manner.[23] The relevance of the IEC 80001 series for medical device cyber security in acute care settings cannot be overstated. During knowledge discussions, one respondent emphasised that "cyber security vulnerabilities typically occur in systems which are poorly maintained". To ensure patient safety and minimise risks, it is crucial for healthcare organisations to prioritise cyber security and adhere to international standards such as the IEC 80001 series, especially when relying on networked medical devices for critical care. This protects patient data and maintains public trust in healthcare.

The ASD Essential Eight



Consumer trust is a significant consideration for the medical technology industry when it comes to designing and developing medical devices. To give consumers and patients peace of mind in using these devices, it is important to cultivate data privacy and security practices that build trust. Several global examples illustrate the work being done to instil the sense that medical devices can be used without trepidation.

Singapore's Cyber Security Labelling Scheme (CLS), developed in consultation with the Asia Pacific Medical Technology Association (APACMed) and Singapore Manufacturing Federation, is an excellent example of a voluntary regulation that helps to increase consumer trust in medical devices.[30]

The CLS assesses IT products and services against cyber security standards, grading them to one of three levels following a rigorous assessment covering access controls, cryptography, network and software security, and incident management. The scheme is encouraged but not mandatory, allowing consumers to make informed decisions about medical devices and providing participants with a competitive advantage.

Similarly, SOC 2 international certification was flagged by MTAA members and industry stakeholders as a process that would add significant value if implemented or encouraged in Australia: "The SOC 2 standard is well regarded internationally and demonstrates to our customers that we take cyber security seriously. It's almost as good a marketing tool as anything to say that we comply with those things." SOC 2 is based on the Trust Services Criteria – security, availability, processing integrity, confidentiality, and privacy. These define the system requirements that service organisations must meet to ensure the safety, security, and privacy of customer data.

Aligning regulatory policies with global best practices fosters an environment where patients and users build confidence in the organisations that are responsible for their safety and privacy. By leveraging the regulatory approaches of other regions, Australia can learn from their experiences and implement effective strategies to increase patient trust.

RECOMMENDATIONS

The medical technology industry faces various cyber security challenges that can hinder the secure and efficient use of devices. For Australia to sustain its status as a prominent player in the global arena, it is imperative for industry leaders and policymakers to collaborate and proactively address these challenges.

The rapid evolution of medical technology has resulted in an increasing number of interconnected components and a greater dependence on software and network systems.[31] This complexity has created new vulnerabilities to cyberattacks such as hacking, malware, and ransomware, which can have significant consequences in acute care settings that rely on older systems more susceptible to such attacks.It is crucial to implement robust cyber security measures that account for potential vulnerabilities and ensure the safety of patients. By way of example, ventilators in acute care settings are increasingly connected to hospital networks, making them hypothetically vulnerable to cyber threats.[32]

Although manufacturers can design secure products, the overall security of the system is only as strong as its weakest link. Older devices, software, or networks, in addition to inadequate cyber security knowledge among operators, increases the risk of cyberattacks. In the case of ventilators, a cyberattack could lead to altered oxygen flow or a change in functionality, resulting in severe harm to patients. It is essential to consider how legacy technologies could be updated or secured before scheduled obsolescence.

Lack of threat and vulnerability awareness poses an ongoing challenge for healthcare providers and manufacturers because the weakest link in defences is often human error.[33] To address this issue, it is crucial to implement appropriate cyber security training programs.

Current practices and the regulatory language used in the Uniform Recall Procedure for Therapeutic Goods (URPTG) guidance document, as well as the medical device cyber security guidance for industry document, does not distinguish between necessary performance upgrades and actions taken

to address device deficiencies.[20,21] This can lead to negative perceptions of recall actions among the general public. MTAA proposes changes to the recall process and the language used to describe recall actions, as well as the reasoning behind these recommendations.

While MTAA members acknowledge the value of aligning post-market cyber security guidance with the URPTG guidance, MTAA and its members have concerns that the public may misinterpret this terminology in the cyber context. MTAA recommends that future policy changes clarify that not every cyber security issue necessitates a product recall, and not every software-related product correction is linked to a cyber security issue.

Cybersecurity vulnerabilities in medical devices are not always due to software updates or other changes to a device's character. They can also be caused by changes in the environment surrounding the device, such as the introduction of external software that could compromise the device's integrity. This type of change can present a risk to patients, and it is crucial to communicate the risk stemming from changes in the environment separately from changes to the device itself. This is because the impact of such changes on device cyber security may not be immediately apparent, and their potential consequences could be severe, including data breaches or patient harm.

It is imperative that regulatory authorities adopt proactive measures to ensuring that the language used in these scenarios effectively communicates appropriate actions to consumers and patients. This will enable consumers and patients to make informed decisions about the safety and security of their medical devices and take appropriate action to mitigate any potential risks.

The medical device industry foresees a surge in the frequency and scope of cyber security-related software modifications. In interviews with industry experts, a respondent emphasised that as digital health products and services become a more significant component of their product offerings, so will the need for increased cyber security measures and resources. Consequently, companies that invest in software capabilities to enhance device performance and patient health outcomes will face significant regulatory implications. There will be a need for proactive software patching or upgrading to anticipate and address potential vulnerabilities, while implementing measures to mitigate identified risks.

Due to the likely increase in the frequency and scale of device-related software changes, MTAA suggests that the TGA consider a different approach to communicating and addressing cyber security vulnerabilities. This could include labelling software-related changes to prevent performance upgrades being conflated with actions to address device deficiencies. Such conflation could lead to excessive responses from consumers and patients, clinicians, and the media, causing misjudgements about the safety and quality of medical devices in Australia.

It is also important to acknowledge the shared responsibility among various stakeholders in the MedTech industry for ensuring patient safety and security. MTAA proposes a fair and balanced approach towards regulatory requirements that prevents excessive costs for manufacturers, while ensuring that medical devices are safe and secure for patients.

MTAA recommends that future policy directives consider the potential risks associated with cyber security within the MedTech industry and apply uniform provisions to all players in the supply chain. This proactive approach promotes innovation while ensuring that regulatory requirements are reasonable and not excessively burdensome for manufacturers.

Regulatory agencies and peak bodies across Australia should also promote efforts to enhance cyber security awareness through fundamental training programs for healthcare professionals and patients. Despite medical devices being designed in a safe and secure manner, much of this work comes undone if they are connected to networks or systems that are out of date or operated by individuals with poor cyber security awareness.

CASE STUDY

Protecting data to improve quality of life

Web-based symptom tracking has been shown to improve survival rates and quality of life among metastatic cancer patients undergoing chemotherapy. But concerns about cyberattacks and data breaches have been reported as barriers to adoption.

Elekta developed an adaptive symptom-tracking algorithm for the Kaiku Health web application. This first-of-its-kind platform incorporated industry best practice and regulatory guidance. This has proved to be an effective way of providing effective follow up whilst empowering patients to self-monitor symptom progression.

Elekta is investing in the security of its innovations, with a dedicated digital security team that keeps a dual focus on developing safe and secure products while also anticipating and responding to emerging cybersecurity threats – ensuring data remains secure and patients are confident in using technologies that ultimately extend and improve their quality of life.

INTEROPERABILITY

Interoperability is the cornerstone of effective health data sharing between patients, carers, practitioners, hospitals, and health departments. Patient data has historically been captured across systems that use different terminologies, formats, and data standards. Medical records data storage also uses various mediums from physical paper to cloud-based electronic record systems.

Siloing health data leads to less informed diagnostic decisions, duplication of tests and procedures, increased opportunities for errors, and repetition of information gathering. This fragmentation often leads to additional costs, poorer patient experiences, increased clinical burden and the inability to use valuable data for public health research.

Interoperability allows timely access to accurate relevant health data for all stakeholders. From healthcare professionals dealing with data at the point of care for diagnostic purposes, through to patients and carers performing ongoing condition monitoring and management functions.

The rate and volume of health information being exchanged is ever-increasing, whether within local hospitals and health districts, to state and federal departments or across international borders, as well as between primary, tertiary, and aged care settings. When surveying MTAA members and relevant industry stakeholders, 75% of respondents said interoperability was a pertinent concern to their organisation.

The Global Digital Health Partnership (GDHP) defines interoperability as: The ability of a system or product to transfer meaning of information within and between systems or products without special effort on the part of the user. Interoperability is made possible by the implementation of standards.[34]

The European Coordination Committee of the Radiological (COCIR) identifies three levels of interoperability:

- **Organisationa**l – Laws, policies, procedures, and bilateral cooperation.
- **Semantic** – Precise meanings can be interpreted by any other system.
- **Technical** – Applications can accept data from each other and perform a given task in an appropriate and satisfactory manner.[35]

Technical standards and requirements are the most discussed elements of interoperability, but operational processes and procedures are equally crucial in achieving successful data exchange. People-based aspects of culture, leadership, vision, collaboration, trust, communication, and awareness are also essential for true interoperability.

MTAA's Digital Health survey identified all three levels of interoperability as vital, with technical interoperability deemed important by 96% of respondents, organisational by 84% and semantic by 72%.

Healthcare interoperability requires alignment and support from all stakeholders, including governmental bodies, hospitals, healthcare practitioners, device manufacturers and regulators. Device manufacturers enable medical device interoperability by adopting the required standards and protocols into their digital health product offerings. Regulatory requirements may be introduced to obtain certification in local markets. Hospitals and health services may also specify interoperability elements within their procurement processes.

Governments may enact mandates or introduce funding models – such as the US Office of the National Coordinator for Health Information Technology, or the German Federal Institute for Drugs and Medical Devices (BfArM) Digital Health Applications (DiGA) – that enforce or encourage interoperability. The ONC Cures Act Final Rule stipulates interoperability provisions to provide "better information, more conveniently, to patients and their providers" via standards and open APIs.[36] DiGA allows for the public or insurance funding of approved digital health apps available to patients via prescription.[37]

OVERVIEW

Australia is at the forefront of interoperability innovation, from the Commonwealth Scientific and Industrial Research Organisation's (CSIRO) work on wireless technology to the founding of Fast Healthcare Interoperability Resources (FHIR) by Grahame Grieve.[38] But although the development of interoperability is well supported in Australian healthcare, the implementation and use of these technologies often lags other regions.

Interoperability can improve healthcare access in rural and regional locations, which is key in addressing changes faced by Australia's diverse populations with geographic, cultural and socioeconomic variations.[39] Interoperability provides access to clinicians, systems, data, and knowledge previously unavailable to remote communities.

About 7 million people, or 28% of Australia's population, live in rural and remote areas.[40] The long distances they often travel to access medical services, combined with an ageing population and Indigenous health issues, pose serious challenges for health service providers. Interoperability has an important role to play in assisting with care collaboration, telehealth, and long-term monitoring that minimises patient transportation and improving access to clinical expertise.

Interoperability and digital health innovation in Australia is being led by a wide range of voluntary and not-for-profit organisations along with state and federally funded bodies. The CSIRO has developed tools for terminology services including the FHIR-based Ontoserver to enhance the effectiveness of SNOMED CT, OWL and other terminology/code sets for patient data.[41] State health providers are calling for a standards-based approach to core data and tasks.[42]

Interoperability is also a core component of the Australian Digital Health Agency (ADHA) developed National Digital Health Strategy 'Safe, seamless and secure: evolving health and care to meet the needs of modern Australia'.[43]

The ADHA has identified 7 strategic priorities[44]

The recent Strengthening Medicare Taskforce Report calls for the modernising of primary care with numerous interoperability related recommendations.[45]

- Modernise My Health Record (MHR) to significantly increase the health information available to individuals and their health care professionals,

requiring 'sharing by default' for private and public practitioners and services and making it easier for people and their health care teams to use at the point of care.

- Better connect health data across all parts of the health system, underpinned by robust national governance and legislative frameworks, regulation of clinical software and improved technology.
- Invest in better health data for research and evaluation of models of care and to support health system planning. This includes ensuring patients can give informed consent and withdraw it, and ensuring sensitive health information is protected from breach or misuse.
- Provide an uplift in primary care IT infrastructure, and education and support to primary care practices including comparative feedback, so that they can maximise the benefits of data and digital reforms, mitigate risks and undertake continuous quality improvement.
- Make it easier for all Australians to access, manage, understand, and share their own health information and find the right care to keep them healthy for longer through strengthened digital health literacy and navigation

MHR is a key component of the Australian government's view of an interoperable future. However, it has a chequered history and usage remains low.[46,47] MTAA's Digital Health survey found that only 12% of respondent products and services integrate with MHR and only 28% plan to integrate in the next five years.

Consumers are calling for greater interoperability across the healthcare systems they interact with, including an increased integration of MHR with primary care to allow greater access to their health data by clinicians, patients, and carers alike.

The most recent federal budget allocated $429 million over two years to modernise MHR including by creating a new National Repository platform which supports easier, more secure data sharing across all healthcare settings.[48]

There is great opportunity to further educate the industry and foster the uptake of standards that will ensure Australian healthcare infrastructure is best placed to realise the benefits and improved outcomes that digital health provides.

Promising initiatives are underway, including the ADHA working with HL7 Australia to provide free FHIR training courses for software developers.[49] The soon to be released National Healthcare Interoperability Plan is expected to provide a five-year roadmap for the development of a connected healthcare sector with digitally enabled models of care. A comprehensive national interoperability strategy and a digital health standards catalogue are pivotal steps towards a digitally enabled healthcare sector.

Australian jurisdictions are assessing their digital health maturity and infrastructure capability, benchmarking nationally and internationally with models such as those provided by the Healthcare Information and Management Systems Society (HIMSS).[50]

Healthcare interoperability is a global challenge, with attempts to address it through policies, practices, standards, and legislation. Much can be learnt from the avoidance of pitfalls to the adoption of successful initiatives in other regions. International collaboration is key to accelerating and harmonising efforts across all regions.

A GDHP survey of 22 GDP countries and in 2019 highlighted the lack of capability to act based on exchanged data, poor usability, and negative impact on provider workflows as key barriers. Governmental financial incentives have helped address economic barriers, with varying degrees of success.[35]

Harmonisation and consolidation of healthcare platforms and systems is essential. As an indication of the task ahead, 92 of the UK's 117 National Health Service (NHS) trusts are each using more than 20 different EHR systems.[51] Healthcare systems are typically a patchwork of different software and hardware systems implemented over the lifetime of the service. Healthcare providers are therefore dealing with older, unsupported, or outdated software and/or hardware that hamper interoperability.

Key technical and semantic standards are being called for across all regions, with many core components being identified globally. The most common include DICOM, FHIR & HL7 specifications

using non-proprietary APIs for data, data access, and interoperability.[52] There are also ISO/IEEE standards, IHI profiles and terminology/semantic coding standards such as ICD, LOINC and SNOED CT.[52]

The US ONC has developed "a standardised set of health data classes and constituent data elements for nationwide, interoperable health information exchange" known as the United States Core Data for Interoperability.[53] The ONC has also introduced mandates via the Cures Act for various interoperability requirements, including electronic health information, maintenance of certification, and minimising API efforts.[37]

The Centres for Medicare and Medicaid Services (CMS) established the Medicare Promoting Interoperability Program in 2022 to encourage the adoption, implementation, upgrade and meaningful use of EHR technology.[54]

CHALLENGES

Trust in the accuracy, validity and meaning of exchanged data is vital for operational interoperability to succeed. Shared terminology and definitions across systems through agreed standards will ensure data is usable and equivalent when exchanged between systems. Obtaining consent from patients or carers is an ongoing challenge for any health system, and often hampers the implementation and optimisation of integration between systems.

Additional overheads and upfront costs may be involved, and these could deter many financially focused healthcare organisations. Healthcare digitalisation also brings challenges around workforce capability and capacity issues, requiring the upskilling of existing staff and the training of new specialists capable of implementing and using these advanced technologies.

Interoperability involves the connection of additional systems and there are inherent complexities involved in the coordination of additional entities and stakeholders across jurisdictions.[35] Existing reimbursement models may need revision to ensure that they support data sharing as some actively discourage it by incentivising disparate and local activities. It is important to make sure that data is current, relevant, timely and can be used, while also ensuring that the systems involved have the capability to act on it.

RECOMMENDATIONS

The key recommendation involves the establishment of a national interoperability framework, which will be crucial if Australian healthcare is to fully benefit from digital health. By adopting global interoperability standards, technologies, protocols and guidelines, Australia can align with other regions and share best practices.

One way to achieve this is through financial incentives and other benefits for healthcare organisations that adopt these standards and technologies. This could be expanded to include the imposing of penalties for non-compliance, and mandates to further strengthen reasons for adoption.

By sharing lessons and knowledge from subject matter experts, the healthcare sector can reduce costs while and improving outcomes. Moreover, national assets will provide the necessary data to underpin public health efforts and leading-edge academic research. This can help inform public health decisions, enabling the development of new treatments, and facilitating academic research.

Mandating the use of certain technologies or capabilities may be the simplest method to achieving interoperability. However, the plethora of different, older, and minor systems means a more collaborative approach is necessary, particularly in areas where vendors do not have the capability or capacity to implement these standards and technologies.

For example, the primary care sector may require a more collaborative approach, where healthcare organisations collaborate with primary care software vendors to achieve interoperability. This may involve identifying common standards and technologies and working with vendors to develop the capabilities required to adopt them. By doing so, healthcare organisations can ensure that systems are compatible with each other, and that data is shared seamlessly across systems and platforms.

CASE STUDY

The promise of interoperability: Seamless, connected patient care across the system

The interoperability of health data is essential to ensure data – and in turn valuable health information – can be seamlessly shared across systems. For patients, this means their health practitioner can easily access and understand information that informs and improves their care. Many patients carry the burden of remembering or manually retrieving their health information as their care transfers across health providers.

My Health Story (MHS) is an example of where the MedTech industry is demonstrating the value of interoperability. MHS enables patients to manage and track their health data – including symptoms, treatments, and appointments – through its web-based platform and handheld app. MHS empowers patients to be more engaged in their health management and enables health teams to provide more personalised care, which is often impossible unless systems and application are interoperable across settings. This means patients will no longer have to 'start over' every time they see a new health professional.

REGULATORY

Healthcare technology is now a fundamental aspect of clinical care, from sharing patient data to monitoring, diagnosing, and anticipating prognostic outcomes.[55,56] The growing reliance on digital health is due to the evolution of the sector and changes to healthcare delivery associated with COVID-19 including Medicare subsidies. Software as a medical device (SaMD), artificial intelligence (AI) and other developments in the digital health sector require regulatory adjustments in Australia.[57]

Regulation associated with digital health products and services was important to 68% of MTAA Digital Health survey respondents. Three-quarters develop regulatory strategy and submissions in-house.

OVERVIEW

Housed within the Health Products Regulation Group (HPRG), the Therapeutic Goods Administration (TGA) is part of the Australian Government's Department of Health and Aged Care. The TGA is responsible for evaluating, assessing and monitoring therapeutic goods including medical devices. The 1989 Therapeutic Goods Act outlines the legal requirements for the import, export, manufacture, and supply of therapeutic goods in Australia.

The Act stipulates the requirements that all therapeutic goods including prescription medicines, vaccines, and medical devices must adhere to before being listed or registered on the Australian Register of Therapeutic Goods (ARTG). Various regulations, orders, and determinations including the Therapeutic Goods Regulations (1990), the Therapeutic Goods (Medical Devices) Regulations (2002), and the Therapeutic Goods Advertising Code provide additional granularity.

The TGA has a rigorous approval process designed to ensure that only safe, effective, and high-quality therapeutic products are supplied in Australia. It also monitors the performance of products once they are in use to ensure they continue to meet regulatory requirements.[58] The TGA has two branches dedicated to medical devices – the Medical Devices Authorisation Branch (MDAB) and the Medical Devices Surveillance Branch (MDSB).

Medical devices are rated in a four-tier classification system based on the risk posed to patients and users. Class I devices are considered low risk, Class IIa and Iib are medium risk, while Class III are high risk. The higher the risk, the greater the regulatory oversight to ensure safety and efficacy. The evaluation process typically involves pre-market assessment of clinical data and risk management documents followed by post-market monitoring. The TGA may take regulatory action if a product is found to pose a risk to the patient or user.

A comparison of the regulatory authorities in Australia, Canada, Saudi Arabia, Singapore and Turkey for the approval of medicines showed that the TGA's evaluation guidelines have greater precision and rigour.[59] The Administration has recently made efforts to address criticism that its processes lack transparency. The TGA is perceived favourably by MTAA members as supporting the Australian government's broader aims of providing equitable access to personalised and preventative healthcare through the expansion of digital products and services.

The TGA and other global regulators use national

requirements to guide their decisions. Although this is understandable, cross-border comparisons and the sharing of best practice approaches are essential in improving patient outcomes.[59] The TGA and other regulatory agencies have well-established collaboration pathways including a range of Mutual Recognition Agreements (MRAs). The TGA recognises evidence from comparable overseas regulators including the US Food and Drug Administration, Europe's CE marking, the Singapore Health Sciences Authority (HSA), Health Canada and Japan's Ministry of Health, Labour and Welfare/Pharmaceutical and Medical Device Agency.

The Medical Device Single Audit Program (MDSAP) certification was launched to support regulatory convergence and eliminate the need to duplicate regulatory audits across jurisdictions. The TGA was a founding member of the program and participates in the development of relevant International Organization for Standardization (ISO) standards.[60]

The TGA is also a founding member of the International Medical Device Regulators Forum (IMDRF). This voluntary group of medical device regulators works collaboratively on the convergence of regulatory approaches including new and upcoming digital health challenges.

The IMDRF defines SaMD as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device".[61] It encompasses clinical software to facilitate diagnosis, mitigation, treatment, and prevention of disease. Examples include remote surgery for medical providers or implantable interface software for patients.

The amount of SaMD registrations in Australia is still relatively insignificant but is showing substantial growth.[62] It has increased by 15% since 2020 and is expected to continue.[63] Globally, the SaMD category is expected to grow from $US18 billion in 2019 to $US86 billion by 2027, with artificial intelligence playing an increasingly important role.[64] MTAA's Digital Health survey supports the growth in the sector, with 65% of responders saying SaMD was part of their five-year growth plan.

The regulations were amended in 2019 to include new classification rules, provide greater specificity on the requirements of software-based medical devices and clearer delineation on the boundaries of regulated software products. TGA also excluded many software products from being medical devices (for example, self-assessment apps) and exempted others (for example, clinical decision support software). The revised SaMD guidelines were informed by its involvement in the IMDRF and the consensus recommendations of its working definition of what constitutes digital therapeutics that require regulation. The recommendations included revised guidelines for the clinical evaluation of the safety, effectiveness, and performance of digital therapeutics by the SaMD Working Group.[65]

CHALLENGES

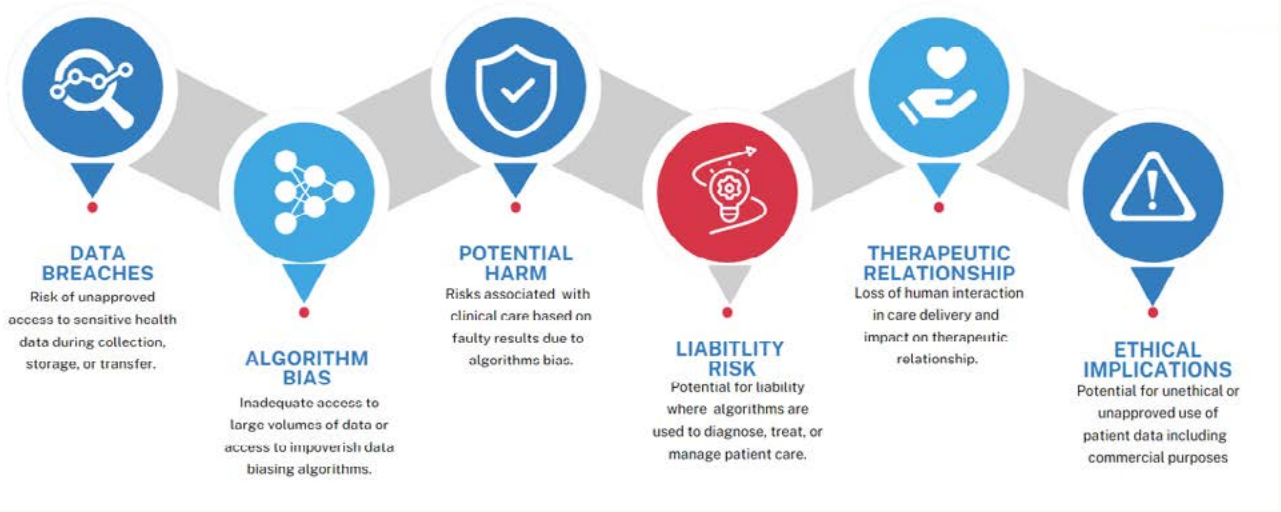
Some MTAA members felt that TGA regulators were ill-equipped to support the new SaMD guidelines when they were released. The TGA has since made substantial efforts to provide resources with classification decision trees, flowcharts, and case examples. The revised TGA guidelines for SaMD have been well received.

The pace of innovation and widespread adoption of SaMD have expedited the clinical application of digital technologies. This necessitates regulatory strategy innovations to fully harness the potential benefits of these emerging technologies. Several targeted modifications could enhance the current regulatory oversight while facilitating continued innovation.[66] Global regulatory authorities are encouraged to continue ongoing reform and review of SaMD regulatory approaches and processes to ensure even greater harmonisation.[67]

MTAA members would like more nuanced legislation within digital health due to the cascading impact on other aspects of their business, including marketing materials and promotional campaigns. Members were concerned about possible regulatory action concerning the Therapeutic Goods Advertising Code 2021, and a lack of clarity on some digital health products and services.[68] This highlights an area for further education and investigation in partnership with the TGA.

The TGA's Uniform Recall Procedure for Therapeutic Goods (URPTG) explicitly states the responsibilities and actions required of manufacturers and sponsors.[68] A review of the number of SaMD recalls and adverse events in the ARTG coincides with

Regulatory Challenges



the increase in registrations, but more details in the notification process would provide additional clarity. The reporting focuses on the software without additional granularity that may inform clinicians or patients.[63]

This issue is increasingly challenging for sponsors, particularly when a medical device incorporates a software-based component such as a wearable or app that principally supports clinical decision-making by doctors.[69] The software is typically considered distinct from the device and the TGA excludes these software components from its regulatory framework. Yet the TGA may issue recalls due to privacy or security breaches, placing the responsibility on sponsors to address these with manufacturers.[70]

Recalls and the potential for disputes between regulators and industry was a recurrent theme during in-depth interviews with MTAA members and other stakeholders. There would be merit in developing device approval guidelines for when software issues arise, or updates are required.

Current applications of AI/ML in healthcare including clinical decision-making, remote monitoring, and robotic surgical procedures are seeing substantial growth.[71] AI/ML was part of the anticipated regulatory applications over the next five years for 45% of survey responders. The use of AI and ML in healthcare poses new regulatory challenges. Principal concerns include:

- Data breaches during collection, storage, or transmission of private patient data to enable an analysis of results or to enable model and algorithm development.
- Biased algorithms due to inadequate access to large volumes of data or access to impoverish data due to condition or population constraints.
- Potential harm due to faulty algorithms making inaccurate diagnoses that negatively impact patient management or treatment.
- Liability risk due to reliance on or use of faulty algorithm recommendations or the provision of erroneous results that lead to inadequate clinical decisions.
- Therapeutic impact from the loss of human interaction in care delivery and the doctor-patient relationship.
- Ethical concerns as patient data may be used in unethical ways or without patient approval, including commercial use.

The Regulatory Horizons Council (RHC) conducted a review of AI/ML in 2022 to provide the UK Government with independent and impartial regulatory guidance on the implications of technological innovation. The RHC review indicated a lack of confidence in accurately evaluating the effectiveness of AI/ML technologies due to the limited evidence of their use outside of pilot studies or at scale. The RHC is concerned about the limited consensus on how to detect, analyse, report, or address any errors associated with the technology. More importantly, the RHC was concerned about the implications of algorithm errors including associated harms because of their use in clinical care.[72,73]

MTAA members responsible for cloud-based solutions have indicated a particular interest in AI/

ML technologies. Although the TGA has alluded to the need for special provisions for AI/ML, it has yet to make any formal changes. The TGA's response is consistent with the feedback from the survey, with 71% of organisations indicating that they understood the regulatory pathway for AI/ML approval.

The US has published proposals for regulating the rapidly growing AI/ML sector, with the FDA launching its AI/ML SaMD Action Plan, while the European Union approved draft legislation in June 2023 that could see its Artificial Intelligence Act become the global standard. The programs aim to maintain stringent regulatory oversight, without stifling innovation and investment.[74]

The FDA has launched a pilot pre-certification program for digital health software which provides a fast-track pathway for approval of new products by granting a companywide 'certification' and subsequent collection of 'real world' data.[75] Australia does not have an equivalent program, but the Australian National Digital Health Initiative (ANDHealth) has encouraged the adoption of one.[76]

Another approach has been taken by the Singapore Ministry of Health, which launched a regulatory sandbox initiative in 2018 that allows companies to test and develop healthcare products and services in a controlled environment.[77] The Licensing Experimentation & Adaptation Programme (LEAP) provides a streamlined regulatory process for companies to obtain temporary exemptions from certain regulatory requirements, without jeopardising patient safety and data privacy. LEAP subsequently resulted in the provision of additional licensing measures under the Healthcare Services Act (HCSA). Sandbox approaches are increasingly being used in healthcare, with recommendations for wider adoption.[78]

RECOMMENDATIONS

Although adaptative regulatory approaches being adopted by the TGA and other regulatory bodies around the world are helpful, more is needed. MTAA recommends greater harmonisation with international regulators relating to digital health therapeutic products. Members would also like to see greater granularity and consistency in regulatory guidelines, including those with a wider impact such as the advertising code and recalls.

It is important for the TGA and other global regulators to keep up with international trends in AI/ML to ensure manufacturers and sponsors are provided with guidance and education in a timely manner. There would be great value in TGA education programs to ensure the guidelines are clearly understood and correctly implemented.

Australia should also consider novel approaches like Pre-Cert and LEAP being adopted internationally to streamline the approval process. Alternatively, the TGA could develop a similar program especially for the Australian regulatory environment.

CASE STUDY

Software-based medical devices can improve patient care

Whilst there are opportunities to strengthen Australia's regulatory environment, Australians are already benefitting from SaMD that have experienced a path to market that is not overly burdensome.

The BD Alaris™ Guardrails™ Suite was approved for use by the TGA in 2014. This software-based device is used by hospitals to write drug protocols (or 'libraries') that are then loaded onto "smart" IV pumps effectively providing "guard rails" to prevent, or at least minimize, incorrect drug doses from being programmed, and ensure the accurate delivery of fluids, blood and blood products.

The approval process for the BD Alaris™ Guardrails™ Suite demonstrates how patients can benefit in a timely way through mechanisms such as the Mutual Recognition Agreement with the European Union – with this SaMD already approved for use by Europe's regulations agency. Aligning with international regulators, and trends, will see Australian patients continue to benefit from technologies that ensure a higher quality of care – and improve health outcomes.

FUNDING, REIMBURSEMENT AND PROCUREMENT

Australia's healthcare system has long faced the same challenges as other publicly funded healthcare systems around the world – increased need due to an ageing population, rising levels of chronic disease, and expensive medical procedures paired with high community expectations and an outdated funding system.[79]

Digital healthcare has the potential to transform the system, delivering better patient outcomes and more affordable care. Advantages include more accurate diagnosis, better monitoring of conditions, supporting clinical decision making and patient self-care, augmenting non-digital interventions, providing remote care, and generating research data. However, these digital health benefits will only be realised if the healthcare system pays for them.

Australians expect that healthcare will be broadly accessible to everyone and that patients will not have to pay for important technologies to maintain health. But those assumptions are being tested, with the 2022 Consumer Price Index noting that the cost of healthcare has risen 40% in a decade.[80] A 2021 national survey reported that 24% of Australian's did not fill a prescription or omitted a dose due to cost, while 14% of responders with chronic conditions said they were unable to pay for healthcare or essential medicines.[81]

OVERVIEW

There are multiple ways of paying for healthcare throughout Australia, most notably through state and territory hospitals, federally funded MBS items for professional services, and private health insurance including the Prostheses List, usually for implantable physical devices. Additional schemes like the National Diabetes Services Scheme (NDSS) are important for specific disease states. There are many other payers, with each facing challenges in paying for and using digital health technology.

Digital Health survey respondents said their digital products are funded/purchased as below:

This makes funding, reimbursement, and procurement a critical component of a successful digital health strategy. Digital health requires innovative funding solutions because the technologies have short lifecycles and are frequently updated, so they do not lend themselves to traditional evidence generation methods. They are also combined with other technologies or services in many instances.

MTAA's Digital Health survey identified that digital health products and services are typically offered "in conjunction with hardware medical devices" (93%), a no charge value-add to related hardware medical devices" (67%) and less commonly "without accompanying hardware medical devices" (46%). It should also be noted that the healthcare system is sometimes geared to the assumption that health interventions are not digital.

Digital Health Survey Results

PURCHASING & FUNDING	%
PUBLIC HOSPITALS/SYSTEMS (STATE AND TERRITORY)	77%
PRIVATE HOSPITAL/SYSTEM	65%
PRIVATE HEALTH INSURANCE PROSTHESES LIST (PL)	35%
MEDICARE BENEFITS SCHEDULE (MBS)	29%
UNFUNDED	29%
CONSUMERS OUT-OF-POCKET	24%
PRIVATE HEALTH INSURANCE (EXCLUDING PL)	24%
COMMUNITY-LOCATED CLINICS OR DIAGNOSTIC CENTRES	18%
AGED CARE FACILITIES	12%
NATIONAL DIABETES SERVICES SCHEME (NDSS)	12%
HOME CARE PACKAGES (HCP)	6%
OTHER	6%

There is an important distinction between three types of payment:

1. Reimbursement for distinct items used by a particular patient based on addition to a regulated list following an assessment process (for example, MBS or Prostheses List).
2. Payment from a general funding pool accessed by a patient or consumer, usually with an approved list (for example, Home Care Packages or NDIS).
3. Purchasing by an institution or payer as part of an episode of care or after care support (for example, public or private hospitals, community clinics).

Importantly, the table above shows that a significant amount of digital health technology is either unfunded or paid for by consumers. Since much digital health is provided in conjunction with hardware, the path to fund it may primarily be for the hardware and would not fund the digital component in isolation. This is true for digital health related to the Prostheses List (for example, remote monitoring) and the National Diabetes Services Scheme (for example, continuous glucose monitoring). Likewise, the Medical Benefits Schedule (MBS) is only designed to fund professional clinical services (for example, pathology) and would only incidentally fund digital health technology.

CHALLENGES

Digital Health survey respondents noted the lack of adequate funding, with most organisations saying that funding coverage is either poor (53%) or partial (41%). None said coverage was good or complete.

When asked about funding barriers, the main limitation (94%) was a lack of specific funding or reimbursement schemes. If a physician prescribes a pharmaceutical, the patient can access it through the Pharmaceutical Benefits Scheme. If the application is attached to hardware, it may be funded through the Prostheses List for private patients or National Diabetes Services Scheme for eligible patients. If it is associated with a service provided in a lab or a clinic it would often be covered through the MBS.

However, there is often no coverage for digital devices. This gap is increasingly being addressed by overseas governments through specific funding pathways, most notably in Germany[82] and France.[83] This largely explains our survey result that 29% of respondents had unfunded technologies and 24% had technologies requiring consumer payment. Two in three providers (67%) offer some medical device software at no cost.

There are also funding challenges around the provision of equipment and sharing of data that need to be addressed. For example, how would funding be managed for hospital-in-the-home equipment that is provided by a state health department when the

patient moves into an aged care facility? And what would be the funding arrangements when an aged care provider shares remote equipment data with the patient's GP or a hospital?

Australia's fragmented system of medical devices payment generally increases the likelihood that patient needs will be missed. State, territory, and private health insurance systems remain strongly geared toward hospital treatment and are not incentivised to actively invest in digital health that would enable consumers or providers to manage health outside of hospital. The lack of institutional funding was reported by 69% of survey respondents as the main funding challenge for digital health.

Likewise, fee-for-service payment approaches like MBS may not encourage investment in patient care that results in digital health purchasing and use.

It has been well documented that the Federal Government responded quickly to COVID-19 by temporarily creating multiple MBS telehealth items covering a broad range of medical services. Although scaled back as the pandemic eased, a much greater range of available telehealth items reflected the principles outlined by the MBS Review Taskforce.[84] This is the most obvious increase in digital health use, but in many cases these are little more than using phone or video calls rather than in-person consultation.

Technologies like remote diagnostics and telemonitoring are generally not incorporated in the payment despite successful CSIRO trials for aged care patients resulting in substantial system savings.[85] Also, current MBS items don't provide sufficient coverage of GP or healthcare professional time for monitoring high-risk patients even though there are now digital capabilities that allow them to do this.

An ageing population is the most significant economic, health and social challenge that we face today, with elderly people most likely to suffer from one or more chronic and degenerative diseases. These in turn are often associated with some level of disability.[86] Ageing, chronic disease and disability combined represent a vulnerable population with significant assistive needs that are highly likely to be admitted to hospital or be moved to expensive nursing home care without adequate support.

Remote monitoring of chronic disease among vulnerable elderly people helps them remain at home, improves their quality of life, and saves on hospital admissions or residential aged care costs. While this is notionally covered in Commonwealth Home Care Packages, there is virtually no mention of it on any official websites and it is unclear how elderly people gain access to it.

More than 27% of people in Australia over the age of 65 live alone.[87] Falls are considered the most preventable injury in aged care, representing 42 per cent of hospitalisations and 40 per cent of deaths.[88] Medical alarm services enable rapid responses and make elderly people more confident to live at home. However, the funding for such programs limits the number of people who have access. Of more than 1 million elderly people living alone[89], MTAA estimates that less than 200,000 have used available funding for a medical alarm[90].

The sophistication of this technology will only grow. AI can already learn a person's normal body movements and alert staff to changes so they can intervene before an emergency happens. Programs like this are mainly funded via special grants or pilot programs. To enable and recognised the full potential of these technologies, broad funding access and delivery is required.

The NDIS also provides some coverage of digital and remote monitoring technology if it assists in managing a disability, although this has come under recent criticism. There are no provisions for ongoing chronic disease management.

All new purchasing of health technologies requires evaluation. The evaluation for reimbursement lists in Australia is typically a form of health technology assessment (HTA) that systematically reviews the relative clinical and cost effectiveness of a technology against other interventions and makes a recommendation on price. Examples include the Pharmaceutical Benefits Advisory Committee (PBAC) process for pharmaceuticals and the Medical Services Advisory Committee (MSAC) process for most other types of new health intervention. The Prescribed List of Medical Devices and Human Tissue Products (formerly known as the Prostheses List) also has an evaluation process.

HTA grew out of the assessment of pharmaceuticals and is well suited to their evaluation. They have long development times and lifecycles with typically larger paybacks that lend themselves to the generation of large amounts of evaluation data. If taken as prescribed, they also tend to work relatively

independently of the prescribing clinician or the patient.

Medical device hardware already challenges this model, but digital health provides even further challenges. Lifecycles are very short with regular software updates. Returns are typically far lower than for pharmaceuticals and the product may not be sold globally. Effectiveness may be dependent on the user. Consequently, there is less reason to invest in large-scale evidence generation and well-regarded randomised controlled trials are more difficult to run.

Digital health technologies generate large amounts of valuable data. They also offer other benefits such as patient empowerment that aren't well measured or assessed in HTA approaches. If a traditional HTA model is applied to most digital health technologies, there is a high likelihood of failure due to lower levels of available evidence. This has been pointed out by APACMed in its 'Harnessing the Potential of Digital Health Technologies – Policy Pathways for Value Assessment & Reimbursement' paper.[91]

Four in five (81%) Digital Health survey respondents said the current approach to demonstrating the value of digital technology, including evidence requirements, is a key barrier to obtaining funding. Difficulties in generating data or providing proof of concept required by funders or purchasers was reported as a barrier by 63% of organisations.

There is currently no value assessment framework for digital health technologies in Australia as recommended by APACMed. Furthermore, current MSAC Guidelines provide no tailored information on how to assess digital health technologies given their unique characteristics.[92] There is no provision in the Australian HTA system for digital health technologies to receive a provisional listing. Importantly, listing processes in Germany, France and elsewhere have been specifically tailored to evaluating digital health.

Procurement processes by hospitals and institutions are a critical factor in whether digital health technologies are effectively paid for. Frequently bought and lower cost items are typically part of routine contracting and tender arrangements. Digital health technologies are less likely to be in the latter category and so are not often purchased in a routine way.

Procurement issues can be broadly grouped into two categories – a focus on cost rather than value, and processes that are difficult to navigate. There are several drivers for the cost over value mindset, including pressure for savings, lack of capability to undertake value assessments or contract for value, funding models that reward lower costs not better patient outcomes, and systemic inertia. While these factors impact purchasing of all products, digital health technology is particularly vulnerable because it is often new, may take many different forms, and often requires integration into wider healthcare delivery and patient management.

The difficulty in navigating processes falls harder on digital health for the same reasons. Purchasers are often creating the process as they undertake the purchase. Furthermore, knowledge of digital health technologies is often low, particularly among procurement groups. Purchaser responses are often slow, which is a particular issue given the short cycle times in digital health technology. This means patients miss out on improved outcomes, while healthcare systems lose efficiencies that are sorely needed in the current climate.

RECOMMENDATIONS

A 2023 review of potential barriers to adoption and commercialisation of Digital Therapeutics (DTx) between Australia, France, Germany, the UK and the US highlighted the importance of government provisioned reimbursement pathways.[82] The lack of funding in Australia for digital health applications used by patients in their home is becoming a glaring omission, particularly as more countries implement clear pathways and others put plans in place to do so.

There is no good reason why a consumer should get subsidised access to a pharmaceutical for home consumption and not to a digital health app if it has demonstrated benefits. In the French and German schemes, it is a requirement that relevant apps be registered as a therapeutic or diagnostic device. Although there are many digital health apps on the market, few would qualify, and the cost would be very manageable. Only 53 apps are listed for prescription in Germany, either permanently or temporarily.[93] A patient would only be able to get subsidised access if prescribed by a clinician.

Importantly, access pathways in France and Germany

are specifically designed for evaluating digital health technologies. They allow the sponsor to gain temporary listing based on a foundational set of evidence to justify ongoing listing through collecting data once they are on the market. MTAA recommends Australia establish national funding for registered digital health applications like the French and German approaches.

Assessing digital health in the same way as any other health intervention will inevitably lead to underfunding and limited patient access. MTAA recommends that federal government commence a process to develop a value-based assessment framework specifically for digital health.

This will involve a consultation and assessment process about the current HTA approach, key aspects of digital health and the final elements of the framework. The Evidence Standards Framework (ESF) for Digital Health Technologies created by the National Institute of Health and Clinical Excellence (NICE) is an excellent example of a model to follow, especially for considering relevant types of evidence in evaluation.

Value assessment frameworks are useful for HTA processes, particularly for relatively discrete devices, but will not address all aspects of purchasing. Value-based healthcare is increasingly considered the key plank of healthcare system reforms designed to improve patient outcomes while maintaining or lowering costs.[94] The great benefits digital health offers won't be realised unless institutional purchasing shifts focus from cost to value. It requires collective understanding and agreement on the principles of this approach. MTAA recommends government develop key principles for value-based procurement of digital health technologies.

Healthcare systems are much more likely to invest in innovative health technologies including digital health when they are funded in ways that reward better patient outcomes and cost management. Current activity-based funding models, MBS fee for service arrangements and limitations on private health insurance providing out-of-hospital care all disincentivise digital health purchasing in favour of driving down costs.

A review is needed of funding models to ensure they are fit for purpose to promote digital health uptake. Where recommendations have already been made, such as the Strengthening Medicare Taskforce proposal to move further away from fee-for-service payments toward blended funding models, these should be implemented as has begun to occur in the recent Federal Budget.

Likewise, approaches being developed by the Independent Hospital and Aged Care Pricing Authority (IHACPA) to institute capped and bundled payments for suitable patients should be advanced. Private health insurers should also be given access to the reinsurance pool for out of hospital coverage. MTAA recommends a review of funding model incentives to invest in innovation including digital health and implement models that encourage uptake for patient and system benefits.

CASE STUDY

Managing chronic disease with connected care

The CSIRO Telehealth Trial tested the impact of introducing at-home telemonitoring to patients suffering from chronic conditions in five locations across different states and territories. It was the largest telehealth trial of its kind ever attempted in Australia.

CSIRO conducted a comprehensive technology assessment analysing a wide range of health and wellbeing outcomes, as well as health economic metrics derived from MBS, PBS, and hospital data.

Analysis of this model suggested that for chronically ill patients, an annual expenditure of $2,760 could generate a saving of between $16,383 and $19,263 per year, representing a potential 6x return on investment.

OTHER CONSIDERATIONS

Numerous additional factors require consideration for digital health success. Although not a primary focus of this paper, they will play an important role in delivering a digitally enabled healthcare system.

DIGITAL HEALTH WORKFORCE

Technology, no matter how sophisticated, is a tool to support the people delivering healthcare services, ranging from frontline clinicians to back-office support staff. Digital technologies bring new staffing, training, and retention requirements to ensure that there is capability and capacity to implement and support the technologies. The Australasian Institute of Digital Health and others provide training to build the necessary workforce capability. In-person training may also be needed for sections of the population including older Australians who are not digitally literate or lack access to technology.

A VOICE FOR CONSUMERS

Patients are becoming more involved in the management of their own care, expecting healthcare to be as readily available as banking, entertainment, and other services. Patients are better informed and want to have a say in their treatment, as well as access to their health data. They will play a critical role in the successful adoption of digital health products and services that provide them with greater control and the ability to voice their needs and concerns.

However, not all individuals have equal access to digital health resources or the same level of digital literacy. People living in rural or remote areas with poor internet connections may not be able to access telehealth consultations and other services requiring high-speed and stable internet connections. This digital divide highlights the importance of ensuring that everyone, regardless of their location or economic status, has equal access to technologies and services.

In a multicultural country like Australia, which is home to a wide range of diverse communities, language barriers and inadequate translation services can result in gaps and potential harm. This can lead to a lack of access to essential healthcare services and information, hindering the ability of individuals to make informed decisions about their health. It is imperative that steps are taken to address these barriers.

CLOSING THE INDIGENOUS GAP

Digital health technologies including mobile health apps, telehealth, electronic medical records and electronic health records have the potential to significantly improve the health outcomes for Indigenous communities facing numerous health challenges, particularly those in remote locations.[95,96] The dynamic nature of digital health can help necessitate culturally appropriate care, which can often be a barrier for communities to seek out and engage with health services.

The far-reaching advancements digital health can facilitate is evidenced by the Warakurna Health Centre implementation of electronic medical records, telehealth consultations, and a mobile app that allows patients within the remote Aboriginal community of Tjuntjuntjara in Western Australia to access their medical records and communicate with healthcare providers.[97] This technology has allowed for more efficient and coordinated care, reduced travel for patients and providers, and improved health outcomes.

However, there are also challenges associated with implementing digital health solutions for Indigenous communities.[98] Digital health initiatives need to be culturally sensitive and respectful of customs and practices. This includes overcoming language barriers, ensuring materials and communication tools are inclusive of local dialects and cultural practices.

Listening and engaging with Indigenous communities and leaders in the design and implementation of these initiatives may help align these activities with Indigenous values and priorities. Data privacy and security are also concerns. As such, it is crucial that digital health initiatives are designed with these concerns in mind, and that measures are taken to ensure the security and privacy of patient data.[99]

AUSTRALIA'S AGEING POPULATION

Australia's ageing population will place additional demands on the current the model of care far outweighing the current capacity of hospitals, GPs, and residential aged care facilities. Digital technologies offer potential solutions to allow healthcare to be addressed within home and community-based care or aged care facilities. Much work is being undertaken on home-based care models including the NSW Smart Sensing Network's Ageing Forum Taskforce's Healthy At Home.

QUADRUPLE AIMS OF HEALTHCARE

This paper draws upon similar work by other industry organisation dedicated to furthering the innumerable benefits of digital health. It reflects the Quadruple Aims of Healthcare to:

- reduce costs and improve productivity.
- improve population health.
- improve patient experience.
- ensure provider/team wellbeing.

INDUSTRY DEVELOPMENT

The calibre of Australia's healthcare system is due in part to a willingness to innovate and adopt new approaches. Launching its digital health strategy in 2008 as part of a broader approach to solving the rising healthcare costs by using technology to streamline processes, improve efficiency, and reduce duplication. Other invests in digital health initiatives that improve the quality, safety, and efficiency of care have included prescribing software in the early 1990s (for example, MedicalDirector, Genie Solution), information sharing in the early 2000s (for example, MediConnect, HealthConnect), MyHealth Record in 2019, and electronic prescriptions in 2020.[78]

Medical devices undergo constant development based on feedback from medical practitioners and advances in other sciences relevant to medical technology. Small Australian firms often play the major role in research and development of new medical devices, with large firms providing organisational and capital assets that help ensure the commercial success of new products.

Notwithstanding recent progress, Australia's lack of a unified health policy and inherent cost-shifting between state and federal budgets only serves to complicate an already difficult task.[100] MTAA members and our sister organisations face several challenges in assessing the value, funding, and reimbursement of digital health products and services.

The draft National Digital Health Strategy 2023-2028 aligns with the major themes of this report in in identifying four key enablers:

1. Policy and regulatory settings that cultivate digital health adoption, use and innovation.
2. Secure, fit-for-purpose and connected digital solutions.
3. A digitally ready and enabled health and wellbeing workforce.
4. Informed, confident consumers and carers with strong digital health literacy.

Addressing these challenges is critical to realising the potential of digital health technologies to improve healthcare outcomes in Australia.

ABOUT THIS REPORT

MTAA, its Connected Health Advisory Group (CHAG) committee, and the University of Newcastle set out to understand the current digital health landscape in Australia, and to develop recommendations that would improve it. This involved desktop research, survey questions, and in-depth research with MTAA members and other key stakeholders.

Digital health products and services in this report refer to a broad range of digital technology solutions designed to improve healthcare delivery and patient experiences. Although the report focuses primarily on the role of medical technology, it cannot be isolated from the broader digital health environment. A total of 40 organisations completed the Digital Health survey, providing an overview of the challenges facing the sector.

REFERENCES

1 International Data Corporation (IDC). *The Digital Health Market*. 2020; Available from: https://www.idc.com/getdoc.jsp?containerId=US45415720

2 Global Digital Health Partnership. *Who's Involved*. 2023 [cited 2023; Available from: https://gdhp.health/about/whos-involved/.

3 Australian Government. *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. 2014; Available from: https://www.legislation.gov.au/Details/C2014C00076.

4 Research Australia, *Research Australia Opinion Polling 2017*. 2017.

5 Australian Institute of Health and Welfare (AIHW), *Data Governance Framework.* 2021: Canberra, ACT, Australia

6 Desai, T., F. Ritchie, and R. Welpton, *Five Safes: designing data access for research.* Economics Working Paper Series, 2016. **1601**: p. 28.

7 Australian Parliament. *Data Availability and Transparency Bill 2020*. 2022; Available from: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6649.

8 Australian Institute of Health and Welfare (AIHW). *The Five Safes framework*. 2021; Available from: https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework.

9 Australian Bureau of Statistics. *The role of the Australian Bureau of Statistics in data governance and stewardship in Australia - a regulatory perspective*. 2021; Available from: https://www.abs.gov.au/about/our-organisation/australian-statistician/analytical-series/role-australian-bureau-statistics-data-governance-and-stewardship-australia-regulatory-perspective

10 European Parliament, C.o.t.E.U. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* 2016; Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

11 Global Medical Technology Alliance, *White Paper on Data Protection, Privacy and Global Health Data within the Medical Technology Industry*. 2022, Global Medical Technology Alliance

12 Kruse, C.S., et al., *Challenges and Opportunities of Big Data in Health Care: A Systematic Review.* JMIR Med Inform, 2016. **4**(4): p. e38

13 U.S. Department of Health & Human Services. *Health Insurance Portability and Accountability Act (HIPAA)*. 2022 [cited 2023; Available from: https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html.

14 Centers for Disease Control and Prevention. *HIPAA Privacy Rule and Public Health.* 2018; Available from: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

15 Personal Data Protection Commission, *Advisory guidelines on key concepts in the PDPA.*, PDPC, Editor. 2021: Singapore.

16 Canadian Institute for Health Information, *CIHI's Health Data and Information Governance and Capability Framework*. 2020: Ottawa, ON.

17 Biddle, N., I. McAllister, and J. Sheppard, *ANU Poll 52 (August 2022): COVID-19, mental health, population issues, data privacy and coercive control*. 2023, ADA Dataverse.

18 Balbi, A., *Massive cyber attack at anthem: Up to 80 million individuals affected*, in *Strategic Finance*. 2015. p. 11.

19 National Audit Office, *Investigation: WannaCry cyber-attack and the NHS*. 2017.

20 Therapeutic Goods Administration, *Medical Device Cyber Security Guidance for Industry*. 2022: Australia, ACT.

21 Department of Home Affairs, *Australia's Cyber Security Strategy 2020*. 2020: Australia, ACT.

22 Australian Cyber Security Centre, *Essential Eight Maturity Model*. 2022: Australia, ACT.

23 The European Association Medical devices of Notified Bodies, *Team-NB Position Paper - Cyber Security*. 2022: Sprimont, Belgium.

24 International Medical Device Regulators Forum, *Principles and Practices for Medical Device Cybersecurity. Final Document.* , M.D.C.W. Group, Editor. 2020, International Medical Device Regulators Forum (IMDRF).

25 European Commission, *MDCG 2019-16 - Guidance on Cybersecurity for Medical Devices. [Guidance]*. 2020.

26 Food and Drug Administration (FDA), *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.*, in *Draft Guidance for Industry and Food and Drug Administration Staff.* 2022.

27 International Electrotechnical Commission. *IEC 80001-1: Health informatics - Risk management of medical devices incorporating software - Part 1: Principles and framework.* 2011; Available from: https://www.iso.org/standard/44863.html.

28 International Organization for Standardization. *ISO 31000:2018 Risk management - Guidelines.* 2018; Available from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

29 International Organization for Standardization. *ISO/IEC 27000 series - Information technology - Security techniques - Information security management systems.* 2020; Available from: https://www.iso.org/standard/73906.html.

30 APACMed, *Cybersecurity*. 2022.

31 World Health Organization, *Global strategy on digital health 2020-2025*. 2021: Geneva.

32 Williams, P.A. and A.J. Woodward, *Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem.* Med Devices (Auckl), 2015. **8**: p. 305-16.

33 Nifakos, S., et al. *Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review*. Sensors, 2021. **21**, DOI: 10.3390/s21155119.

34 Global Digital Health Partnership, *Advancing Interoperability Together Globally*. 2020.

35 Digital Health CRC, *Digital Transformation Of Healthcare In Australia Constrained A Call To Action For A National Data Governance Framework*. 2023.

36 The Office of the National Coordinator for Health Information Technology, *The ONC Cures Act Final Rule*. 2020.

37 Devices, F.I.f.D.a.M. *DiGA Digital Health Applications*. Available from: https://www.bfarm.de/EN/Medical-devices/Tasks/DiGA-and-DiPA/Digital-Health-Applications/_node.html.

38 CSIRO. *Bringing WiFi to the world*. [cited 2023.

39 Medicine, A.C.o.R.R., *Rural and remote aged care services Position Statement*. 2022.

40 Australian Institute of Health and Welfare (AIHW). *Rural and remote health*. 2022 [cited 2023]; Available from: https://www.aihw.gov.au/reports/rural-remote-australians/rural-and-remote-health.

41 CSIRO, *Clinical Terminology Tools*. 2017.

42 Health, N., *eHealth Strategy for NSW Health 2016–2026*. 2016.

43 Australian Digital Health Agency, *Australia's National Digital Health Strategy*, in *Safe, seamless and secure: evolving health and care to meet the needs of modern Australia.* 2022: Australia, ACT.

44 Australian Digital Health Agency, *What Are the Next Steps to Continue Advancing the Interoperability Agenda?* 2017: Australia, ACT.

45 Australian Government, *Strengthening Medicare Taskforce Report*. 2022.

46 Australian Digital Health Agency, *Australian Digital Health Agency Annual Report 2021-22*. 2022.

47 Guardian, T. *My Health Record: after 12 years and more than $2bn, hardly anyone is using digital service*. 2022.

48 Australia, C.o., *Budget 2023-24, Budgert Measures, Budget Paper No.2*. 2023.

49 Agency, A.D.H., *Australian Digital Health Agency signs agreement with HL7 Australia to help connect Australia's healthcare system*. 2022, ADHA: digitalhealth.gov.au.

50 Woods, L., et al., *Show me the money: how do we justify spending health care dollars on digital health?* Medical Journal of Australia, 2023. **218**(2): p. 53-57.

51 Association of British HealthTech Industries, *DATA ACCESS AND USE: DISCUSSION DOCUMENT*. 2022.

52 APACMed Digital Health Committee Interoperability Working Group, *Harnessing The Power Of Interoperability Within Medical Devices, An Asia Pacific Perspective*. 2020, APACMed.

53 Office of the National Coordinator for Health Information Technology, *United States Core Data for Interoperability v3*. 2022.

54 Centers for Medicare & Medicaid Services. *Promoting Interoperability Programs*. [cited 2023].

55 Kwan, J.L., et al., *Computerised clinical decision support systems and absolute improvements in care: meta-analysis of controlled clinical trials.* The BMJ, 2020. **370**: p. m3216.

56 Zurynski, Y., et al., *The Voice of Australian Health Consumers: The 2021 Australian Health Consumer Sentiment Survey*. 2022, Consumers Health Forum of Australia.

57 Taylor, A., et al., *How Australian Health Care Services Adapted to Telehealth During the COVID-19 Pandemic: A Survey of Telehealth Professionals.* Frontiers in Public Health, 2021. **9**.

58 Therapeutic Goods Administration, *Clinical evidence guidelines - medical devices*, in *Version 3.1*. 2022, Commonwealth of Australia: Canberra.

59 Mashaki Ceyhan, E., et al., *The Turkish Medicines and Medical Devices Agency: Comparison of Its Registration Process with Australia, Canada, Saudi Arabia, and Singapore.* Frontiers in Pharmacology, 2018. **9**.

60 APACMed, *Digital Health Regulation In Asia-Pacific Overview And Best Practices APACMed Digital Health Committee Regulatory Working Group*. 2020: Singapore.

61 International Medical Device Regulators Forum, *Software as a Medical Device (SaMD): Key Definitions*. 2013, International Medical Device Regulators Forum (IMDRF).

62 Ceross, A. and J. Bergmann, *Evaluating the Presence of Software-as-a-Medical-Device in the Australian Therapeutic Goods Register.* Prosthesis, 2021. **3**(3): p. 221-228.

63 Precedence, R., *Digital Health Market Size, Growth, Trends, Report 2023-2032*. 2022, Precedence Research.

64 Research, B.C.C., *Software as a Medical Device: Global Market Outlook*. 2023, BCC Research: Boston, Massachusetts.

65 IMDRF, *Software as a Medical Device (SaMD): Application of Quality Management System*, in *IMDRF SaMD Working Group*. 2015, International Medical Device Regulators Forum.

66 Torous, J., A.D. Stern, and F.T. Bourgeois, *Regulatory considerations to keep pace with innovation in digital health products.* NPJ Digit Med, 2022. **5**(1): p. 121.

67 Shuren, J., B. Patel, and S. Gottlieb, *FDA Regulation of Mobile Medical Apps.* JAMA, 2018. **320**(4): p. 337-338.

68 Therapeutic Goods Administration, *Therapeutic Goods (Therapeutic Goods Advertising Code) Instrument 2021*, in *Instrument 2021*. 2022, Therapeutic Goods Administration: Canberra.

69 Stone, E.G., *Unintended adverse consequences of a clinical decision support system: two cases.* Journal of the American Medical Informatics Association : JAMIA, 2017. **25**(5): p. 564-567.

70 Webb, T. and S. Dayal, *Building the wall: Addressing cybersecurity risks in medical devices in the U.S.A. and Australia.* Computer Law & Security Review, 2017. **33**(4): p. 559-563.

71 Vignali, V., et al., *Health horizons: Future trends and technologies from the European Medicines Agency's horizon scanning collaborations.* Frontiers in Medicine, 2022. **9**.

72 Chothani, F., et al., *Regulatory Prospective on Software as a Medical Device.* International Journal of Drug Regulatory Affairs, 2022. **10**(4): p. 13-17.

73 Han, J.E.D., et al., *Opportunities and Risks of UK Medical Device Reform.* Therapeutic Innovation & Regulatory Science, 2022. **56**(4): p. 596-606.

74 Scott, I.A., et al., *What is needed to mainstream artificial intelligence in health care?* Australian Health Review, 2021. **45**(5): p. 591-596.

75 Therapeutic Goods Administration, Annual Performance Statistics Report. 2021, Therapeutic Goods Administration: Canberra.

76 Andhealth, *Regulation of Software, Including Software As A Medical Device (SaMD). Feedback to the TGA's Consultation Documen*. 2019: Melbourne, Victoria.

77 Walsh, C., *Regulatory Sandbox: A New Tool for Telehealth Innovation in a Post-Covid World.* Columbia Business Law Review, 2021.

78 Leckenby, E., et al., *The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review.* Applied Health Economics and Health Policy, 2021. **19**(6): p. 857-869.

79 Duckett, S., *Expanding the breadth of Medicare: learning from Australia.* Health Economics, Policy, and Law, 2018. **13**(3-4): p. 344-368.

80 Australian Bureau of Statistics, *Consumer Price Index, Australia, December Quarter 2022*. 2023: Australian Bureau of Statistics.

81 Mantovani, A., et al., *Access and reimbursement pathways for digital health solutions and in vitro diagnostic devices: Current scenario and challenges.* Frontiers in Medical Technology, 2023. **5**.

82 Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). *Digital Health Applications.* 2023; Available from: https://www.bfarm.de/EN/Medical-devices/Tasks/DiGA-and-DiPA/Digital-Health-Applications/_node.html.

83 Guichet National de l'Innovation et des Usages en e-Santé, the National Portal for eHealth Innovation. *Early access to reimbursement for digital devices (PECAN)*. 2023; Available from: https://gnius.esante.gouv.fr/en/financing/reimbursement-profiles/early-access-reimbursement-digital-devices-pecan.

84 Medicare Benefits Schedule. *MBS telehealth services from 1 July 2022.* 2022; Available from: http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/Content/Factsheet-telehealth-1July22.

85 Commonwealth Scientific and Industrial Research Organisation (CSIRO). *Home monitoring of chronic diseases.* 2021; Available from: https://www.csiro.au/en/research/health-medical/diagnostics/home-monitoring.

86 Australian Institute of Health and Welfare (AIHW). *People with disability in Australia.* 2022; Available from: https://www.aihw.gov.au/reports/disability/people-with-disability-in-australia/contents/health/chronic-conditions-and-disability.

87 Australian Bureau of Statistics. *Older people.* 2016; Available from: https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/4430.0main+features302015.

88 Australian Institute of Health and Welfare (AIHW). *Falls.* 2022; Available from: https://www.aihw.gov.au/reports/injury/falls.

89. Australian Bureau of Statistics*. Disability, Ageing and Carers, Australia: Summary of Findings, 2015*. 2016. https://www.abs.gov.au/ausstats/abs@.nsf/Lookup/4430.0main+features302015

90. Data on file

91 Asia Pacific Medical Technology Association. *Harnessing the Potential of Digital Health Technologies – Policy Pathways for Value Assessment & Reimbursement.* 2021; Available from: https://apacmed.org/harnessing-the-potential-of-digital-health-technologies-policy-pathways-for-value-assessment-reimbursement/.

92 Medical Services Advisory Committee (MSAC). *Guidelines for preparing assessments for the Medical Services Advisory Committee.* 2021; Available from: http://www.msac.gov.au/internet/msac/publishing.nsf/Content/E0D4E4EDDE91EAC8CA2586E0007AFC75/$File/MSAC%20Guidelines-complete-16-FINAL(18May21).pdf.

93 Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). *Cara Care for irritable bowel syndrome.* 2023. https://diga.bfarm.de/de/verzeichnis.

94 Australian Healthcare & Hospitals Association (AHHA). *Deeble Issues Brief No. 31: Value Based Health Care: Setting the scene for Australia.* 2019; Available from: https://ahha.asn.au/publication/health-policy-issue-briefs/deeble-issues-brief-no-31-value-based-health-care-setting.

95 Sansoni, J., *Health Outcomes: An Overview from an Australian Perspective*, in *Australian Health Outcomes Collaboration, Australian Health Services Research Institute, University of Wollongong*. 2016, Australian Health Outcomes Collaboration.

96 Moecke, D.P., et al., *Scoping review of telehealth use by Indigenous populations from Australia, Canada, New Zealand, and the United States.* Journal of Telemedicine and Telecare, 2023: p. 1357633X231158835.

97 Australian Digital Health Agency, *Technology brings better health care to one of the most remote communities in the world*. 2021.

98 Fitzpatrick, K.M., et al., *Understanding virtual primary healthcare with Indigenous populations: a rapid evidence review.* BMC Health Services Research, 2023. **23**(1): p. 303.

99 Clair, M.S., et al., *Telehealth a game changer: closing the gap in remote Aboriginal communities.* Medical Journal of Australia, 2019. **210**(S6): p. S36-S37.

100 Nygard, H.T., L. Nguyen, and R.C. Berg, *Effect of remote patient monitoring for patients with chronic kidney disease who perform dialysis at home: a systematic review.* BMJ Open, 2022. **12**(12): p. e061772.

ABOUT MTAA

Medical Technology Association of Australia (MTAA) is the national association representing companies in the medical technology industry. This includes manufacturers and suppliers of medical technology (MedTech) used in the diagnosis, prevention, treatment, and management of disease and disability.

MedTech industry products range from frequently used items like syringes and wound dressings to pacemakers, defibrillators, bone and joint replacements, and other prostheses. It includes hospital and diagnostic imaging equipment, such as ultrasound and magnetic resonance imaging (MRI) used in all settings, from the smallest rural clinic to the largest multi-site hospital.

MTAA members provide Australia's healthcare professionals with essential product information and training to ensure the safety and effective use of MedTech, delivering better health outcomes to the Australian community.

MTAA plays a critical role in facilitating collaboration, advocating for favourable policies, and promoting the adoption of digital technologies in healthcare. It supports members on important issues like regulatory compliance, market access, and trade opportunities. And it drives innovation through research and development funding that contributes to MedTech commercialisation that improves patient health and quality of life.

ABOUT CHAG

MTAA's Connected Health Advisory Group (CHAG) was established in 2020 to drive the implementation of an ICT-enabled service delivery framework for a healthier Australia. **CHAG** members represent health and community care, the medical device industry, peak bodies, research institutes, associations, and advocacy groups. This diversity of representation has enabled **CHAG** to work objectively with a common purpose, highlighting digital opportunities in the delivery of care for a healthier Australia.

4/97 Waterloo Road, Macquarie Park
Sydney, Australia

P +61 (0) 2 9900 0600
E reception@mtaa.org.au

www.mtaa.org.au