Enabling Digital Health Adoption in the Asia-Pacific

A White Paper based on a virtual Digital Health Roundtable organised by the Duke-NUS Centre of Regulatory Excellence on the 18th and 19th of November 2020

DukeNUS Medical School | Centre of Regulatory Excellence

Table of contents

Executive summary

In November 2020, the Centre of Regulatory Excellence (CoRE) at the Duke-NUS Medical School in Singapore convened a virtual two-day Roundtable on Digital Health in the Asia-Pacific to address and discuss issues in the context of evolving digital health regulation. Government, NGO, academic and industry stakeholders from countries in the region, primarily from Southeast Asia, participated in the event with different experts sharing their expertise on a variety of topics, including telemedicine, personalised and integrated care, capacity building, healthcare data policies, data security and cybersecurity, and digital health regulation. Three of these areas - *healthcare data policies*, *data security and cybersecurity*, and *digital health regulation* - were identified as key enablers of digital health adoption and discussed in more detail during the breakout sessions. In addition to information from the Roundtable, supplementary data from relevant literature has been integrated while preparing this White Paper.

The Roundtable highlighted the importance of *digital health and relevant policies* to create a secure environment that facilitates its safe and effective adoption. Digital health uptake and implementation of healthcare data policies differ significantly among ASEAN[1] countries. There is also a lack of information about the status of digital health adoption in individual economies within Southeast Asia and the wider Asia-Pacific, impeding effective collaborations across the region. Other issues include the lack of streamlined regional healthcare data policies and the rapidly changing healthcare data environment, both hampering drafting policies for interoperability in a timely manner.

Regarding *data security and cybersecurity*, improved security structures in the healthcare sector are needed as evidenced by the increasing number of data infringements and cyber threats. As cyberattacks can occur at different levels, it is important to protect all layers of the technological ecosystem and obtain timely insights to identify potential threats and reduce further damage from cyberattacks. If attackers break through the first line of cyber defence, organisations should immediately implement pre-prepared incident response plans. Another issue identified during the Roundtable is the need for essential principles and frameworks concerning the verification processes for safety and performance requirements for data, information-capturing devices and other digital health tools.

A major issue discussed during the Roundtable concerned the *frameworks for regulating digital health technologies*. Conventional regulatory frameworks are not well suited for the fast-evolving, iterative nature of software and digital health technologies. Therefore, regulators should adopt risk-based and agile regulatory paradigms. In addition, there is a need for a consistent approach to software qualification, Software as a Medical Device (SaMD) classification, and total product lifecycle approaches for the Asia-Pacific. An opportunity exists to scale adoption of rapid digitisation of clinical trials, catalysed by the COVID-19 pandemic, through fit-for-purpose regulatory frameworks for digital technology use in research and development. Lastly, cooperation among regulators will help to increase convergence of global standards for digital health regulation and facilitate expedited regulatory pathways through reliance.

Several recommendations were made for governments and organisations to enhance the overall digital health policy, data security and cybersecurity, and regulatory environment:

[1] Association of Southeast Asian Nations

- In response to challenges related to healthcare data policies, countries should consider appointing governing bodies that will focus on their digital health strategy, improve transparency about their digital health uptake by participating in regional digital health initiatives, and collaborate with one another to develop a standardised and harmonised regional data-sharing framework;

- Regarding data security and cybersecurity issues, governments and organisations should conduct thorough risk assessments, establish standard safety and performance requirements to assess digital health technologies, and develop incident response plans;

- In terms of digital health regulation, countries should adopt innovative risk-based regulatory approaches, increase regulatory cooperation, accelerate convergence to internationally recognised standards, and promote public-private collaborations. As a fundamental enabler, capacity-building approaches should be adopted to improve countries' digital health uptake.

To realise the full potential of digital health in the Asia-Pacific, continued engagement among local and regional stakeholders to clarify and coordinate regulatory frameworks is essential. CoRE will continue to provide a neutral academic platform to strengthen capacity and facilitate discussions, collaboration and follow-through.

1. Introduction

This chapter explores the emergence of digital health and the potential opportunities of digital technologies to address global health challenges. The issues discussed during CoRE's 2020 Digital Health Roundtable are presented, including the benefits of digital health, telemedicine, personalised and integrated care, and the degree of adoption and application. An overview of this White Paper and the scope of the subsequent chapters is provided.

Digital health as an accelerator of health systems strengthening

The 2020 CoRE Digital Health Roundtable opened with a keynote address by Mr Bernardo Mariano Jr, WHO's[2] Chief Information Officer who shared on the WHO global strategy for digital health. The vision of WHO's global strategy is to improve health for everyone everywhere by accelerating the development and adoption of appropriate, accessible, affordable, scalable and sustainable person-centric digital health solutions. A collaborative effort is required to develop the infrastructure and applications that enable countries to unlock the power of health data to promote health and well-being, and to achieve the health-related Sustainable Development Goals.

Sixteen years after the ratification of WHO's initial eHealth resolution, the need for countries to implement strong digital health structures is more urgent than ever. The COVID-19 pandemic has shown the importance of information and communication technology (ICT) in prevention, detection and response to epidemics and pandemics. Even prior to the current COVID-19 pandemic, emerging disease outbreaks, such as Ebola and Zika, had led to calls from numerous leading institutions to push for widespread and rapid data availability across the globe and resilient digital health infrastructures for pandemic preparedness (Kozlakidis et al., 2020). Since the start of the current pandemic, many countries have started or ramped up large-scale deployment of digital health technologies, such as advanced data analytics, enhanced electronic medical record and monitoring systems, telemedicine programmes and virtual consultations and mobile health applications (Perez Sust et al., 2020; Scott et al., 2020).

Telemedicine[3] and mobile health applications empower individuals to better manage their own health and well-being through technology, a key focus area for digital health implementation according to the WHO. Teleconsultations can facilitate greater patient safety and convenience without the need for travel, and rapid advancements in sensor-based technologies and wearables enable patients to continuously monitor their health in between appointments. As discussed at the Roundtable, the COVID-19 pandemic has been a major catalyst for accelerating adoption of telemedicine due to the need for patients isolated by lockdowns to continue consulting their healthcare providers. However, there is still a need to further enhance the adoption of these technologies by patients and healthcare workers. Governing institutions and policymakers should also focus on developing telemedicine-related policies, such as financing structures and payor models for the utilisation of telemedicine, and clarifying the regulatory frameworks.

Another important focus area for digital health implementation is enabling the transition to integrated, personalised care and facilitating the shift from treatment to prevention. The ubiquity of large amounts of medical and health-related data means that truly personalised and integrated care is within our reach. Despite tremendous medical advancements, standard treatments for diseases or syndromes do not always result in optimal or desirable outcomes for individual patients. With the use of healthcare data, data analytics and scientific breakthroughs, such as genomics and innovations in targeted therapeutics, personalised care aims to fill this gap by providing the treatment that is best suited for the individual patient and addresses their specific needs (Roche, 2020; National Health Service, 2019).

Beyond a personalised approach to therapeutics, health data can further be merged with other social and economic data from payors and social agencies to achieve precision public health

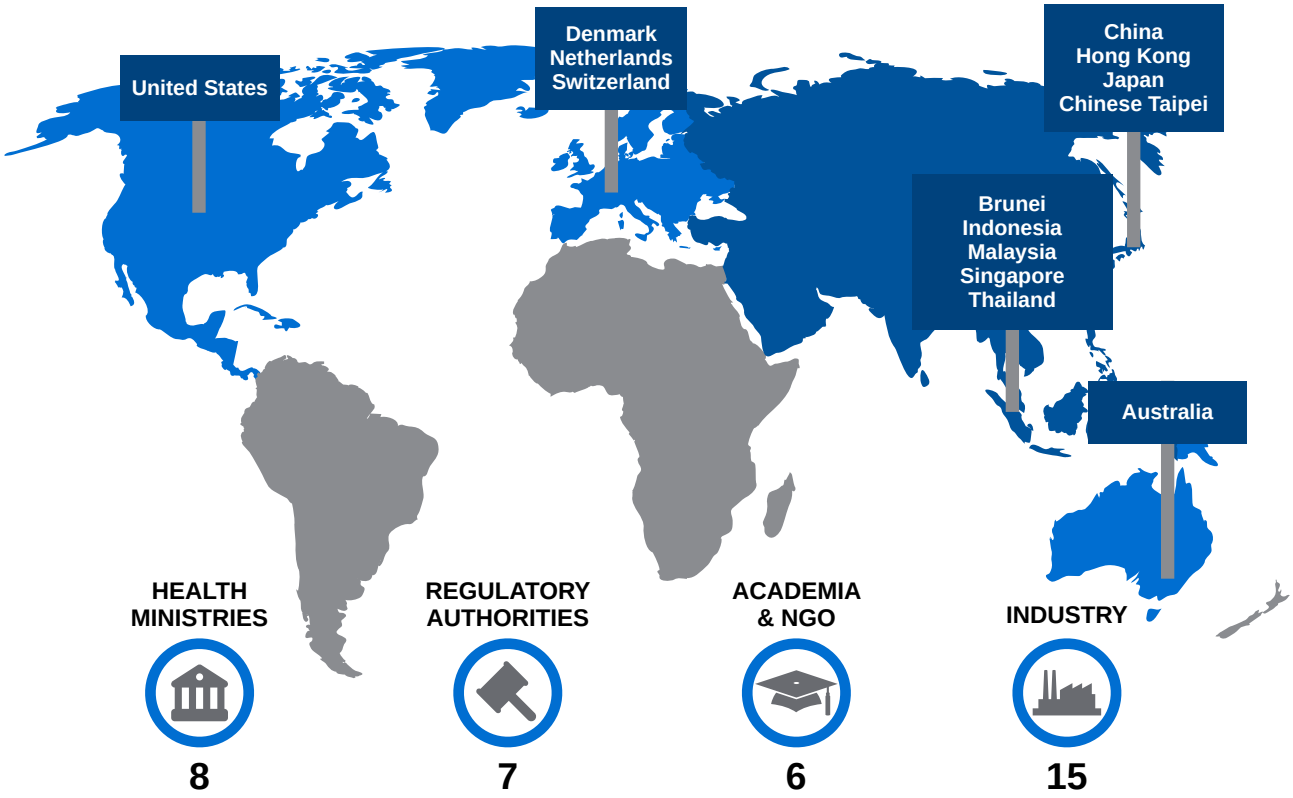
[2] World Health Organization

[3] Telemedicine refers to carrying out health services remotely through technological means (American Academy of Family Physicians, 2021)

(PPH)[4] and integrated care. Integrated care is facilitated by using technologies to ensure that people receive a continuum of health promotion and a wide range of other healthcare-related services, which are well coordinated among each other to meet an individual patient's needs (World Health Organization, 2016). Achieving personalised and integrated health systems that can deliver treatment and prevention tailored to peoples' needs requires a shift from the traditional medical curative model, where healthcare decisions come mainly from healthcare providers and institutions, to a model that allows the community to play a much more significant role in healthcare decisions. While there is more focus on the technology driving digital health, it is just as important to consider how users will engage with digital health technologies and how these will fit into their routine working and living environments.

The discussion at the Roundtable focused on the key enablers for adoption of digital health to support the goals of robust, person-centric and integrated health systems. These enablers are healthcare data policies, data and cybersecurity, and digital health regulation, supported by capacity building. In total, 36 representatives from 14 economies[5] participated in the virtual Roundtable that was held over two days on 18 and 19 November 2020. They were drawn from health ministries, regulatory authorities, academia, NGOs and industry[6] (Figure 1).

Figure 1. Overview of Roundtable participants.



*Industry participants did not participate in the breakout sessions.

[4] Although a universal definition of PPH has not been adopted, several complementary definitions have been proposed. One proposed definition from a recent editorial is *"the application and combination of new and existing technologies, which more precisely describe and analyse individuals and their environment over the life course, to tailor preventive interventions for at-risk groups and improve the overall health of the population"* (Weeramanthri et al., 2018).

[5] Economies included Australia, Brunei, China, Chinese Taipei, Denmark, Hong Kong, Indonesia, Japan, Malaysia, the Netherlands, Singapore, Switzerland, Thailand, the United States.

[6] The industry was represented by The APAC Consortium, which consisted of Merck Sharp & Dohme (MSD), Sanofi, Johnson & Johnson (J&J), Roche Pharmaceuticals, and Roche Diagnostics.

This White Paper draws on presentations and discussions at the Roundtable and is supplemented by further information and insights from literature searches. Chapter 2 describes the key enablers and related challenges of digital health adoption, and Chapter 3 outlines potential opportunities and recommended solutions to improve digital health governance in Southeast Asia and the Asia-Pacific. The key takeaways and recommendations are summarised at the beginning of each chapter.

> *"As we go through that transition, from traditional healthcare delivery to digital healthcare delivery, we need to find that 'techquilibirum,' which is the ideal point where traditional healthcare delivery and digital healthcare delivery complement each other to improve health and well-being for the world population. We must ensure that the digital health revolution is safe, sustainable and leaves no one behind."*
>
> (Mr Bernardo Mariano Jr, World Health Organization)

2. Key enablers of digital health adoption

This chapter discusses the key enablers of digital health adoption from a regulatory context – healthcare data policies and governance, data security and cybersecurity, and digital health regulation. These topics were highlighted by speakers during presentations at the Roundtable and discussed by participants in the breakout sessions.

Section 2.1 addresses the importance of healthcare data and relevant policies. An overview of the current status of healthcare data policies across ASEAN and the Asia-Pacific is provided and some of the most pressing issues highlighted.

Section 2.2 describes data security and cybersecurity in the region. The reasons why countries should improve security measures in the digital health space and what countries have been doing to date are described, followed by challenges that are still being faced.

Section 2.3 covers digital health regulation. The challenges of regulating digital health technologies and the need for adapting regulatory frameworks that can deal with the rapid changes in the digital health environment are described.

2.1. Healthcare data policies

KEY TAKEAWAYS

Adequate healthcare data policies need to be in place to create a secure environment that enables safe and effective data utilisation.

Although the status of digital health uptake and implementation of healthcare data policies in some countries within the Asia-Pacific region is available, lack of information about the situation in other countries impedes effective cross-border collaborations.

ASEAN nations do not have streamlined healthcare data policies in place to improve the regional data infrastructure and boost data-sharing.

Healthcare data exist in a rapidly changing environment and are often utilised by multiple stakeholders, making timely drafting of interoperable policies difficult.

The importance of clear and relevant healthcare data policies

Healthcare data are essential for a wide variety of purposes in the digital health field. High-quality data allow policymakers and clinicians to evaluate the effectiveness of interventions and treatment, resulting in better evidence-based decision-making. Moreover, healthcare data contribute to identifying gaps and limitations in existing healthcare systems and services, thus providing essential information to modify these structures (Organization for Economic Co-operation and Development [OECD], 2015). Healthcare data can also be part of a country's specific national health strategy, where each country uses data to accomplish its specific objectives.

While healthcare data can contribute significantly to the improvement of healthcare, data access can present a risk to individuals. If mishandled or not secured, data breaches can increase the risk of violating a person's right to privacy and equal treatment (OECD, 2015). Healthcare data gathered from patients can, for example, include personal and sensitive information, such as medical histories, which can potentially lead to identifying individuals and their health status. Hence, proper healthcare data policies need to be in place to create a secure environment that enables safe and effective data utilisation. Several Ministries of Health (MOHs) have established such policies, making it mandatory for their staff to sign confidentiality agreements before handling any health data. It was highlighted during the Roundtable that data policies should not be limited to a specific stage of the data lifecycle but integrated into the entire process (Figure 2)[7].

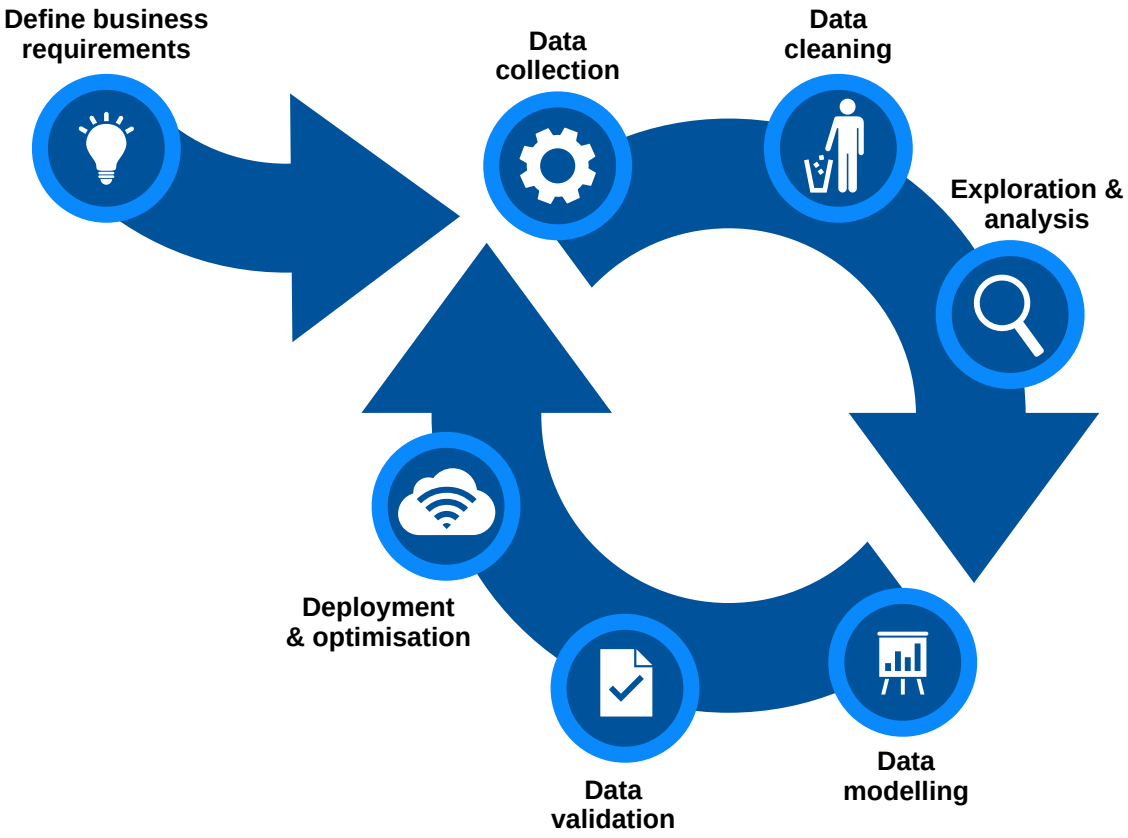
Current status of healthcare data policies across the region

During the Roundtable breakout discussions, it was stated that the *development and implementation of healthcare data policies across Southeast Asia differ widely*. Some countries are seen as global digital health leaders while others are taking their first steps into the digital health

[7] Figure 2 has been adopted from Mr Colin Lim's presentation at the Roundtable.

domain. To evaluate countries' levels of digital health uptake, the Global Digital Health Index (GDHI)[8] was created in 2016, which employs a large set of indicators to assess different digital health components, including healthcare data policy-relevant aspects (GDHI, 2021).

Figure 2. Data lifecycle process.



In total, 22 countries participated in the GDHI, with five located in Southeast Asia – Indonesia, Lao PDR, Malaysia, the Philippines and Thailand. Malaysia has enacted consistently enforced laws and regulations concerning personal digital health data and protection of individual privacy. Thailand and the Philippines also have comparable laws and regulations although these are not yet fully implemented, while Indonesia and Lao PDR are still in the reviewing stages of proposed legislation. Apart from carrying out measures to protect patients' privacy, Malaysia is also a frontrunner in developing and implementing policies that contribute to safe cross-border data exchange, although these are not yet enforced consistently. Thailand has proposed a relevant policy that has not yet been implemented (GDHI, 2021).

A related issue to data exchange is *standards and interoperability*, focusing on a series of requirements that need to be fulfilled by all relevant stakeholders to facilitate the ability to work with each other (Standards and Interoperability Lab – Asia, 2021). According to the GDHI (2021), the Philippines and Malaysia have both created comprehensive national digital health architectural frameworks and industry-based technical benchmarks for health information exchange and other data-relevant aspects, and fully implemented these standards. Thailand has also created and

[8] The Global Digital Health Index was created by HealthEnabled and the Global Development Incubator. They collaborated with more than 20 countries and 50 international institutions, including the Bill & Melinda Gates Foundation and the Healthcare Information and Management Systems Society (HIMSS), to track global digital health uptake.

implemented relevant policies in this space but these are less extensive when compared to the first two countries. Indonesia and Lao PDR have some health information standards in place but a national digital health architecture is currently lacking in both countries.

Although Singapore did not take part in the GDHI, information presented at the Roundtable demonstrates that MOH has implemented various healthcare data policies and utilises data to support larger strategic goals as illustrated in Table 1[9].

Table 1. Singapore's 'Three Beyonds' health objectives and related healthcare data examples.

Beyond Healthcare to Health	Beyond Hospital to Community	Beyond Quality to Value
To build a caring and sustainable healthcare system for our future.	To increase accessibility to care across settings and build capabilities for the future.	To ensure quality healthcare remains affordable for all.
Example how healthcare data is used: Helps to understand patients' healthcare service consumption, resulting in a better overview of the entire patient experience.	*Example how healthcare data is used:* Enables proper allocation of healthcare services and other resources across the entire nation.	*Example how healthcare data is used:* Provides insights to improve cost-effectiveness models and strategic investments in healthcare.

Essential elements of healthcare data policies

According to Vayena et al. (2018), appropriate healthcare data policies should cover three critical 'pillars' or elements. The first pillar is *access and benefit sharing*, where policies should incorporate data protection elements to decide which information is accessible for whom. In addition, benefits obtained from using personal data should be distributed in a fair manner. The second pillar of *accountability and transparency* focuses on including sound accountability mechanisms as well as having high levels of transparency in place throughout the entire data collection and utilisation process to show who is responsible for different aspects. Lastly, the *quality and safety* pillar highlights the need for sanctions and incentives in policies to stimulate safeguarding of high-quality standards and system optimisation.

In parallel with these elements, the Singapore MOH approach to healthcare data governance policy is to ensure access to the *right information* at the *right time* and in the *right format*, so that the *right decisions* can be made. Related to *right information* is the type of data and level of anonymity. Patient data should be regarded as private and confidential, and treated as sensitive health information. Depending on the situation and information needed, data should be anonymised accordingly. Equally important is to choose the right platform to access data as different types of data require different clearance levels. For example, classified government information has a more stringent level of cybersecurity and relevant protective policies compared to less sensitive open-source data. Some data can be obtained by using a wide variety of platforms whereas the accessibility of other information is more limited.

[9] Table 1 has been adopted from Mr Colin Lim's presentation at the Roundtable.

Gaps in the healthcare data policy landscape

Publicly available databases and indices such as the GDHI and other maturity model assessment tools provide useful information on the progression of digital health implementation in countries. For countries that do not contribute to the GDHI or similar indices, the level of implementation and enforcement is less clear. Therefore, it would be helpful for countries to provide information to publicly available indices to help provide a comprehensive overview of the digital health uptake in the Asia-Pacific. In turn, this will improve mutual understanding of each country's situation and foster more effective collaborations within and across the region.

Another issue identified by stakeholders is the lack of streamlined healthcare data policies to improve the regional data infrastructure and boost data-sharing. To realise safe and efficient cross-border data exchanges, there is a need for a standardised and harmonised regional data-sharing framework (Infocomm Media Development Authority of Singapore [IMDA] and Personal Data Protection Commission [PDPC], 2019). However, Roundtable participants pointed out that several countries are still in the nascent stages of creating and implementing standards and operability policies, and lack proper data exchange frameworks. Countries that have more advanced digital health ecosystems might therefore focus on collaborations with countries that have similar digital health system profiles, potentially leaving behind less developed countries in the region.

A major gap in the regional healthcare data landscape is the lack of robust ethics frameworks. Despite the extensive use of big data, including patient data and related health information, adequate frameworks and guidelines to address ethical issues in the use of healthcare data are still scarce (National University of Singapore Yong Loo Lin School of Medicine, 2019).

Challenges in developing healthcare data policies

One of the challenges of defining healthcare data policies is the complex nature of healthcare data itself. As digital health and healthcare data do not exist in a vacuum, policymakers must apply a multiperspective approach that addresses the needs of all various stakeholders. This is affected by other issues, such as stakeholders applying or interpreting terminologies differently, or having their own differing priorities. This results in less coherence and commonality of objectives, thus diminishing the efficiency of the policymaking process and the efficacy of policies generated.

Another hurdle discussed during the Roundtable is the interoperability of healthcare data architecture and practicality of healthcare data policies in the larger digital health infrastructure. For example, in Singapore, if a COVID-19 case is detected during routine data collection, specific processes are in place to send the patient to hospital, track and trace the patient's contacts, and follow up with the patient after release from the hospital. This is feasible because of the coordination of data and relevant health and non-health systems. It would not be achievable if healthcare information was scattered due to healthcare system organisation issues such as sub-optimal collaboration and data sharing among public and private institutions.

The third challenge results from the interplay of the rapidly changing environment and the heightened demand for innovation and technological development. As policies usually entail formal bureaucratic processes to be finalised and require time for subsequent implementation, they could loose currency, effectiveness and alignment. Healthcare data and data policies therefore need to be subject to timely review and updating, especially if they have been crafted to address immediate but evolving concerns.

2.2. Data security and cybersecurity

KEY TAKEAWAYS

Improved data security and cybersecurity structures in the healthcare sector are needed as the number of data infringements and cyber threats are increasing.

Cyberattacks can occur at different levels and it is important to protect all layers of the technological ecosystem.

Essential principles and frameworks concerning the verification processes for safety and performance requirements for data, information-capturing devices and other digital health tools are needed.

Command, Control and Communication (C3) staff, chief information officers and chief security officers face the challenge of attaining timely insights and rapid updates of various elements in the digital health space.

Organisations should have incident response plans in place in the event that the first lines of cyber defence are breached.

The need for data security and cybersecurity

In addition to sound healthcare data policies, robust cybersecurity structures and data security measures need to be in place to create a safe and effective digital health environment. Although the terms “cybersecurity” and “data security” are often used interchangeably, they differ from each other as they operate on different levels. *Data security* focuses on protecting private and sensitive information, whereas *cybersecurity* refers to the larger digital infrastructure (Systems Solution Inc, 2021). Both play an essential role in protecting patients’ and stakeholders’ data, and operate interdependently to maximise security in the digital health space.

The need for strong data security and cybersecurity structures in the healthcare sector has become more obvious in recent years, with an increasing number of data infringements and cyber threats. In 2019, the healthcare industry suffered from 505 reported data breaches globally. As a result, 41.2 million people were affected by these breaches, as their records were stolen, exposed or illegally disclosed (Seh et al., 2020). Leaving data exposed allows for hackers and data thieves to sell personal and sensitive data with potentially devastating consequences. Health data often not only include patients’ medical histories but also their unique personal identifiers that can be used for identity theft-related crimes, such as opening bank accounts using someone else’s name, signing up for loans and obtaining passports (Martin et al., 2017). Apart from data exposure on a private level, cyberattacks can also directly affect health facilities, where criminals could possibly shut down entire systems and jeopardise the health of thousands of patients. In terms of financial implications, a data breach could cost on average USD 3.92 million as compared to an insider cybersecurity threat caused by people within the organisation potentially resulting in a loss of close to USD 11.45 million (IBM Security, 2019).

The level of data security in ASEAN

According to the GDHI (2021), out of the five participating ASEAN countries, Malaysia is the only nation that has a legal framework for data security and that has been properly administered. The framework addresses matters such as data storage, transmission and utilisation. Similar to Malaysia, Indonesia has created and implemented data security legislation, but more consistent enforcement is still required. The other three countries - Thailand, the Philippines and Lao PDR - have all passed laws regarding data security but these remain to be implemented. Again, it should be noted that data from the other five ASEAN countries, including Singapore and Brunei, are not available in the GDHI. Other relevant data security measures and its challenges, such as cross-border data exchanges, national and international standards and interoperability for healthcare data, have been discussed in the previous section on Healthcare Data Policies.

Cybersecurity and its surrounding issues

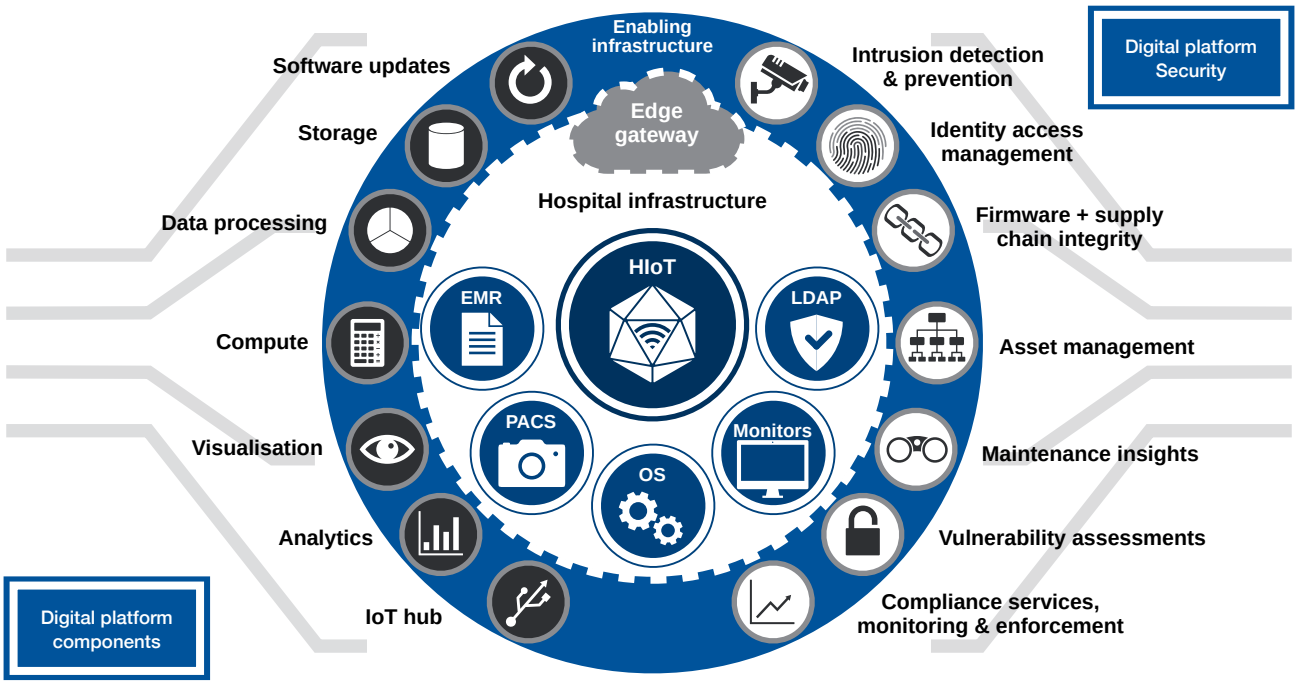
The Roundtable noted that since cyberattacks can occur at different levels, it is important to protect all layers of the entire technological ecosystem (Figure 3)[10]. However, due to the extensive nature of the digital infrastructure, interconnectivity of various digital health products, and delivery of digital health services that happens outside hospital walls (e.g. telehealth), building these security structures poses a tremendous challenge. As attackers can find different paths to break through, a thorough evaluation of the existing nexus is required to identify cyber threats at each level. This all-inclusive approach implies the need for a multistakeholder effort, where IT personnel should collaborate with doctors and healthcare staff to carry out both technical vulnerability assessments and clinical assessments. This combination will lead to the creation of a new risk paradigm that allows stakeholders to pinpoint shortcomings in the security chain more promptly and act accordingly to decrease the risk of potential cybercrimes.

One of the promising technologies that can support the vulnerability management system and improve the level of protection in the digital health environment is the application of artificial intelligence (AI). AI can play a vital role in the enhancement of security structures across the entire network by detecting vulnerabilities and providing timely insights of cyber threats. However, Roundtable participants highlighted that AI comes with the associated risks of autonomous or semi-autonomous operation that could potentially manipulate data inappropriately or produce misleading information. Therefore, additional security measures need to be in place, such as the validation of generated data and other AI-produced outcomes by experts in the field.

In line with this, participants shared the need for establishing essential principles and frameworks concerning the verification processes for safety and performance requirements for data, information-capturing devices and other digital health tools. Apart from providing guidance on issues such as data storage and verification of manufacturers' product performance claims, these frameworks could contribute to creating a common understanding on digital health-related matters among different stakeholders and allow them to speak the same language. As various players are involved in one or more stages of the digital health management lifecycle, developing relevant policies and frameworks requires a highly coordinated effort by multiple stakeholders.

[10] Figure 3 has been adopted from Mr Ralph K Ramsey's presentation at the Roundtable.

Figure 3. Overview of the entire technological ecosystem in relation to the health system.



*IoT = Internet of Things; EMR = Electronic Medical Records; PACS = Picture Archiving and Communication System; OS = Operation System; LDAP = Lightweight Directory Access Protocol; HIOT = Health Internet of Things.

Incident preparedness and response

The Command, Control and Communication (C3) workforce needs to apply a holistic approach and constantly monitor all the various elements in the digital health space to react promptly to a security threat. These elements include medical devices, systems that support these devices, as well as services and workflows. One of the challenges impacting the ability of C3 staff, chief information officers and chief security officers to respond promptly to any threat is attaining timely insights and rapid updates. There is a need for a single interface that connects all these different technologies in order to allow C3 personnel and clinical staff to work together seamlessly to secure all layers of the digital environment. In addition, there is a need to deal with data sensitivities and ensure that patient privacy and personal information are protected, which makes the task increasingly complex.

Health facilities face the risk of criminals breaking through their first lines of defence, hackers cracking cybersecurity structures and finding their way into systems, or even their own staff causing data breach incidents due to ignorance or not conforming with security protocols. As such, it was recommended by Roundtable participants that all organisations should have proper incident response plans to expeditiously address any attacks or breaches to prevent further damage. The main aim of the plans should focus on getting the services back online rapidly to maintain the care continuum without significant interruptions that could affect patients' health and care. Clear communication plans to inform relevant authorities, address patient and public concerns, and minimise erosion of trust also need to be formulated.

2.3. Digital health regulation

KEY TAKEAWAYS

Regulators should adopt risk-based and agile regulatory paradigms. Conventional regulatory frameworks are not well suited to the fast-evolving, iterative nature of software and digital health technologies.

There is a need for a consistent approach to software qualification, SaMD classification and total product lifecycle approach for the Asia-Pacific.

A significant opportunity exists to adopt the approach of rapid digitisation of clinical trials catalysed by the COVID-19 pandemic through fit-for-purpose regulatory frameworks for digital technology use in research and development.

Regulators should cooperate to increase convergence of global standards for digital health regulation and facilitate expedited regulatory pathways through reliance.

Regulation as an enabler for innovation

Good and "smart" regulation is a key enabler for healthcare innovation with positive socio-economic outcomes. Digital health products and solutions play a vital role in the acceleration of evidence-based solutions and data-driven decisions, strengthening the overall effectiveness and safety of hospitals and other healthcare institutions. The dynamic nature of digital health technologies demands a smart balance between ensuring safety and supporting innovations that improve patient outcomes and benefit the entire health system. Hence, it is important that regulators adopt fit-for-purpose regulatory approaches to regulate digital health products and ensure their safety, quality and efficacy without impeding innovation. This requires risk calibration to identify higher risk products and adjust the level and type of regulation accordingly. It is also important for regulators to cultivate an agile development environment through continuous dialogue with developers from concept to post-market.

Challenges of regulating digital health technologies

Health product regulatory agencies would find it extremely hard to develop regulations faster than the rapid advancements of digital technology. Conventional regulatory frameworks crafted for pharmaceuticals and more traditional medical devices are not well suited to the unique considerations for digital health technologies. According to the United States Food and Drug Administration (USFDA), digital health technologies can be defined as the *"use of computing platforms, connectivity, software and/or sensors for healthcare and related uses. These technologies span a range of products, from general wellness applications to medical devices, and may also be used to develop or study medical products and monitor disease"* (USFDA, 2020). Digital health products have a short development time and lifecycle and undergo frequent updates. There are also unique cybersecurity considerations for connected devices and data transmitted to

the cloud. Regulators therefore need to adopt agile frameworks to implement targeted strategies for new or updated digital products in a timely manner before the challenges and risks of technology become too pervasive. Rather than being reactive, regulators should take novel and forward-thinking approaches to regulation, to anticipate and prepare for future challenges. The commendably agile response of international and regional regulators during the COVID-19 pandemic to facilitate emergency use authorisations of innovative diagnostics, therapies and vaccines demonstrates that this is eminently feasible.

Another challenge in digital health regulation is that the boundaries between various regulators may be unclear. The regulation of digital health technologies tends to fall under the responsibility of different governing bodies. Regulatory authorities would typically focus on digital health medical devices while health ministries and other health authorities oversee digital health services and systems. Some digital health applications such as AI are cross-cutting and do not neatly fit into any single agency's scope. AI may be regulated within an inter-agency national framework that includes regulatory authorities, MOHs, data governance authorities, clinicians and other stakeholders. Effective regulation of complex digital health technologies therefore requires close coordination and collaboration of multiple health agencies and stakeholders.

For many areas of digital health, such as telemedicine, use of digital health technologies in drug development, and use of digital measures to develop novel endpoints, there are no existing global regulatory frameworks that national regulators can reference due to the nascent and fast-evolving nature of digital health regulation. In those few areas where they do exist, they are often inconsistently applied with variations across different jurisdictions. One important area with existing international regulatory frameworks is the regulation of Software as a Medical Device (SaMD) , which is discussed in the next section.

Regulatory frameworks for SaMD in the Asia-Pacific

Regulatory oversight on digital health products is determined by the respective intended purposes and functions assigned by their developers. The International Medical Device Regulators Forum (IMDRF) created one of the earliest international regulatory frameworks for digital health with a focus on SaMD. It defined 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. The guidance includes the usage of harmonised vocabulary, risk classification guidelines, quality management systems for SaMD, and highlights the need for clinical evaluation (IMDRF, 2014).

As the Asia-Pacific region has wide variation in economic development and regulatory maturity, digital health regulations differ across countries. In most ASEAN countries, there is no specific guidance for SaMD which are regulated using general medical devices regulatory frameworks. The regulatory authorities in Australia, Japan and Singapore have been active in the development and advancement of SaMD-specific regulatory frameworks. These three agencies have implemented international best practices in providing opportunities for pre-submission consultations with innovators as well as developing approaches to regulatory review that are tailored to the unique needs of digital health products (Carrington, 2021).

However, there is still room for better alignment of regulations with IMDRF's N12 guidance for risk classification of SaMD. Traditional device risk classifications are linear in progression from low to high risk and classify SaMD based on the disease state or clinical condition associated with its intended use. The IMDRF SaMD classification, however, is two dimensional and considers the

“state of healthcare situation or condition” and the “significance of information provided by SaMD to the healthcare decisions” (IMDRF, 2014). Using the traditional device risk classification, most SaMD are misclassified, as the significance of the information they provide is largely ignored in the classification decision. As the functionality of SaMD becomes more complex and used for medical purposes, applying traditional device classification may not accurately reflect the actual risk level of these products. Thus, the IMDRF classification would give a more accurate risk assessment.

There is also a need to consider specific regulatory approaches tailored to the unique and iterative nature of SaMD solutions, particularly those that use AI or machine learning (ML). Among the countries that do have SaMD regulatory frameworks, some also have specific guidelines for AI and ML. Singapore, South Korea and Japan have guidelines addressing AI and ML in SaMD while Australia does not currently have AI-specific guidance. China’s National Medical Products Administration (NMPA) medical device classification catalogue also includes AI-assisted diagnostic tools (Leong et al, 2020).

The newly formed IMDRF AI Working Group was created to achieve a harmonised approach to the management of AI medical devices. The Working Group is tasked with developing an initial guidance document on standardised AI terminology and definitions for AI medical devices which is planned to be released in January 2022. The IMDRF AI Working Group includes industry and WHO representatives as well as regulatory agencies from Australia, Brazil, Canada, China, the European Union (EU), Japan, Russia, Singapore, South Korea and United States (US) (IMDRF, 2021).

Overall, it is encouraging to see that Asia-Pacific regulators in Australia, China, Japan, South Korea and Singapore are moving forward with their development of SaMD regulatory frameworks. There is an opportunity to better align with global standards, such as the IMDRF SaMD Risk Categorisation Framework, further develop guidance on AI devices, adopt use of predetermined change control plans, and increase convergence of regulations across the region. There is also an opportunity for greater regulatory convergence and harmonisation on SaMD regulatory frameworks through the Asia-Pacific Economic Cooperation (APEC) Regulatory Harmonisation Steering Committee’s (RHSC) Medical Device Priority Work Area (PWA).

While there are still many regulatory agencies in the region that may not have their own SaMD-specific regulations, all regulators should work towards creating expedited regulatory pathways for SaMD, including those based on reliance mechanisms that take into account assessments done by regulatory authorities in trusted countries with more developed regulatory frameworks. This will enable timely access to digital health technologies for their populations. Regional regulatory authorities should continue to collaborate with their global counterparts and stay abreast of best practices emerging in the US, EU, Canada and other more advanced regulatory authorities. One model for regional regulators to track is the USFDA Software Pre-certification programme which is piloting total product lifecycle approaches to regulation rather than the current linear pre-market to post-market framework (USFDA, 2021).

Regulatory frameworks for digital technologies for use in clinical research and development

The COVID-19 pandemic has accelerated the acceptance of the use of digital health technologies in clinical trials by regulatory bodies. However, Roundtable participants involved in clinical trials were of the view that global regulatory guidance involving the use of digital health technologies still

lacked clarity in the context of decentralised trials, digital technologies for data collection, and novel endpoints derived from digital measures. There is an opportunity for regulators to engage with stakeholders to develop guidances which will help bring the clarity needed for developers to embrace this emerging digitalisation of clinical practices.

Digital health technologies offer a range of potential applications in the drug development lifecycle. Novel endpoints derived from digital measures may be more objective or sensitive than current assessment tools (Coravos, 2019). Digitally enabled decentralised clinical trials offer a more patient-centric trial experience as they reduce patient travel requirements, reduce trial attrition, reduce costs of trials, expand access and optimise recruitment. Remote monitoring can provide a more holistic view of the patient experience through continuous data collection using sensor-based technology. Digital technology enables generation of earlier evidence about treatment performance in real-world settings and also early detection of adverse events for timely intervention.

Current US and EU regulations do not address digital technologies used in clinical trials. In the US, a digital technology for use in clinical trials does not need to be approved or cleared as a medical device, but the USFDA requires verification and validation of the technology as per existing investigational regulations (Leptak, 2020). The USFDA also has a Digital Development Tool (DDT) Qualification Program consisting of two programmes relevant to digital technology-generated data - the Clinical Outcome Assessment Qualification Program (COAQP) and the Biomarker Qualification Program (BQP) (USFDA, 2021). The European Medicines Agency (EMA) has released question and answer documents and qualification opinions on the use of digital technologies in clinical trials, most recently in 2020, however there is currently no formal guidance or regulation (EMA, 2020).

Regulatory guidance of digital technologies for use in clinical trials and acceptability of the data generated for regulatory submissions still lacks clarity. Hence, there is an opportunity to promote a collaborative approach and convergence using existing regional and global regulatory platforms to develop new international regulatory models. In developing relevant guidances, regulatory authorities have the opportunity to further improve on current evolving frameworks in the US and EU by incorporating the following recommendations which have been suggested for those regions (Pan, 2020):

- Provide more clarity on how data generated using digital health technologies in trials can be used in regulatory submissions;

- Increase coordination and communication between regulators for medicines and those responsible for medical devices;

- Clearly define the regulatory specifications for data security, privacy, data management and data sharing;

- Move towards more predictable, consistent regulatory pathways for use of digital technologies in trials, rather than the current product-specific approach;

- Adopt a multistakeholder approach to the development of guidances that involve the specific expertise of academics, industry and patients.

Digital transformation of regulatory processes

The disruption caused by the COVID-19 pandemic has increased regulatory agility in utilising digital technologies to accelerate internal processes while maintaining high standards. For example, regulatory authorities have used virtual site inspections, permitted electronic files for Certificates of Pharmaceutical Products and Good Manufacturing Practices, and encouraged use of digital technologies in trials as described in the previous section. These changes have reduced the administrative burden of regulatory processes and there is potential to incorporate such initiatives permanently (Stewart, 2020).

Current regulatory processes involving transmission of discrete datasets, documentation and submissions are resource intensive and limit information exchange between companies and regulators, and also across industry. Cloud-based systems for regulation have not been widely adopted for now but the concept is gaining momentum (Robertson, 2019). Ten global biopharmaceutical companies launched a cloud-based system in July 2020 under the Accumulus Synergy initiative, which is intended to support interactions between industry and health authorities worldwide (Accumulus Synergy, 2021). Accumulus Synergy is working with the USFDA's Oncology Center of Excellence (OCE) and other global health authorities to design, develop and deploy a full-scale, cloud-based parallel review solution enabling collaborative review by regulators (DIA, 2021).

There are potential benefits to cloud-based systems such as improving regulatory efficiency, reduced costs and ultimately speeding up patient access to new safe and effective medicines. However, there are important legal and policy challenges to implementing cloud-based systems, including concerns about data privacy, cybersecurity, anti-trust practices and allocation of management and administration responsibilities (Robertson, 2019). Technical capabilities may also be a barrier for some regulatory authorities that do not currently have IT infrastructures to support cloud-platform requirements. A collaborative approach between industry and health authorities is key to making cloud-based systems feasible and safe for use in regulation.

Regulatory sandboxes for digital health

Singapore is a pioneer in the area of regulatory sandboxes for digital health. The Licensing, Experimentation and Adaptation Programme (LEAP) was a regulatory sandbox for telemedicine and mobile medicine service delivery models created by Singapore's MOH (MOH Singapore, 2021). This sandbox ran from 2018 to February 2021, providing a controlled environment to better understand the risks and co-create corresponding risk mitigation measures with the industry in the use of these service delivery models prior to licensing under the new Healthcare Services Act (HCSA) in 2022[11].

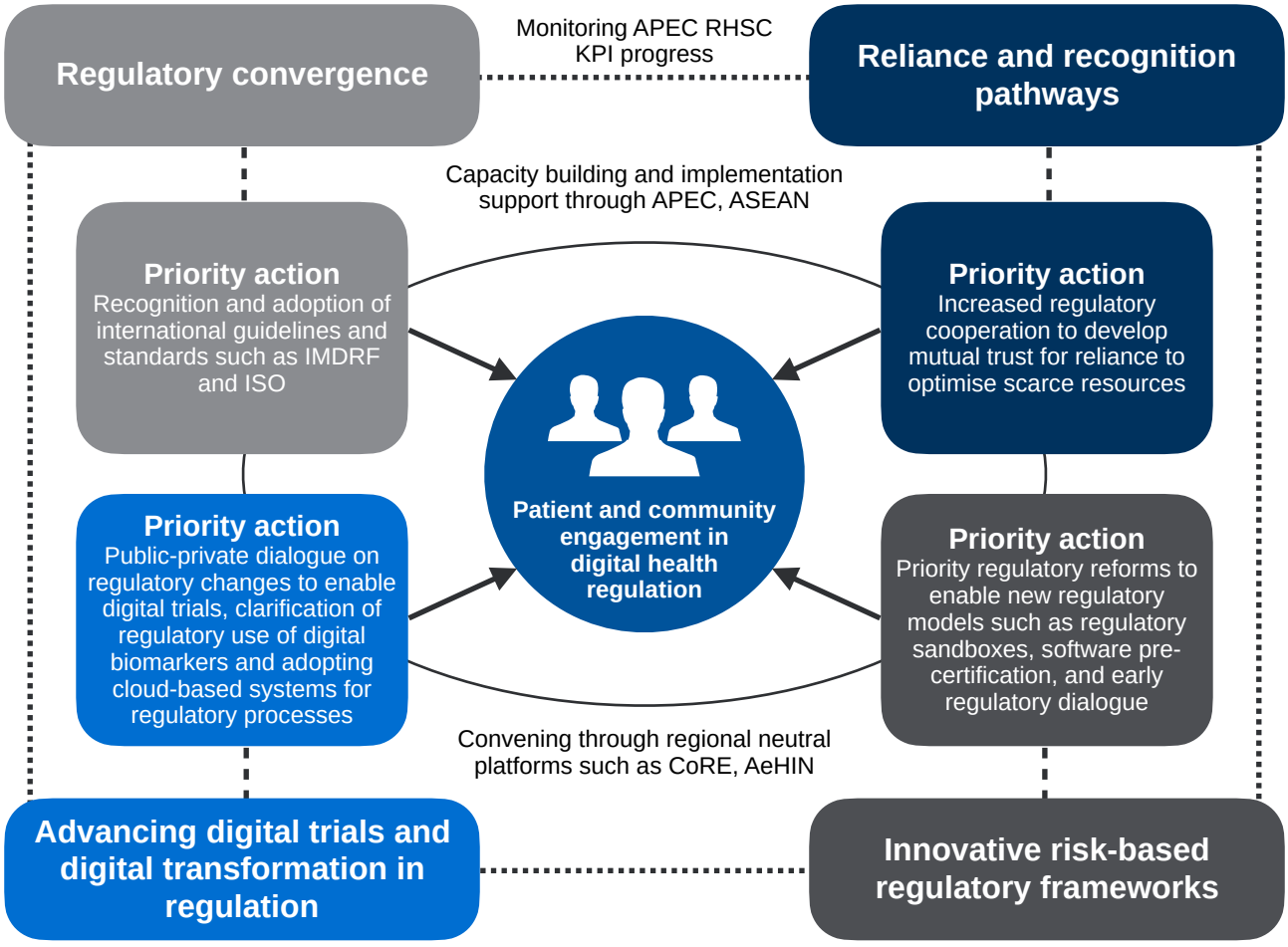
Health professionals providing telemedicine are regulated but the service itself is unregulated as current legislation is based on premises-licensing. Telemedicine which is not confined to any specific premises therefore makes the current licensing paradigm outdated. The data from the LEAP sandbox will help inform Singapore's planned shift away from premises-based licensing to a service-based licensing regime under the HCSA and facilitate updating of clinical practice guidelines for telemedicine.

[11] Telemedicine apps that only facilitate communication between registered medical professionals and patients but are not used for diagnosis, treatment or patient monitoring are not regarded as medical devices by Singapore's HSA and are not currently regulated in Singapore.

The sandbox approach can potentially be used for a wide range of regulatory questions beyond telemedicine. Regional collaboration to identify other potential cases for regulatory sandboxes in other areas of digital health is worth exploring. More evidence is needed on the impact of sandboxes on innovation ecosystems and in ultimately improving patient outcomes.

A multistakeholder and collaborative approach that includes the perspectives of patients themselves is required to enhance the regulatory environment for digital health to enable innovation while ensuring patient safety and privacy. CoRE, as an applied academic centre focused on regulatory capacity building through training on digital health and medical devices, is well positioned to facilitate such collaboration. Moreover, CoRE also provides a neutral platform for stakeholders who do not normally have the opportunity to discuss global regulatory trends and their implications for the Asia-Pacific region. The key aspects of implementing digital health regulatory innovation in the Asia-Pacific are summarised below (Figure 4).

Figure 4. Implementation path for digital health regulatory innovation in the Asia-Pacific.



3. The (digital) way forward

This chapter presents recommendations addressing issues and gaps identified during the Roundtable to improve digital health uptake within and across the Asia-Pacific region.

Sections 3.1 to 3.3 contain recommendations related to issues that were discussed in Chapter 2, addressing challenges in healthcare data policies, data security and cybersecurity, and digital health regulation.

Section 3.4 presents additional recommendations based on collaborative approaches that countries and organisation can take to improve digital health uptake, including capacity building and ongoing engagement in digital health discussions.

Section 3.5 concludes the White Paper.

3.1. Enable healthcare data usage

RECOMMENDATIONS

R1 *Appoint governing bodies that will be responsible for countries' digital health uptake by creating national digital health strategies, drafting relevant policies and implementing these policies.*

R2 *Improve the transparency of countries' digital health uptake by participating in digital health initiatives and sharing their status on healthcare data governance.*

R3 *Develop a standardised and harmonised regional data-sharing framework that includes streamlined terminology and guidance for different stakeholders.*

R1. Appoint governing bodies responsible for digital health uptake

An important factor to advance healthcare data usage would be the appointment of governing bodies responsible for defining digital health strategies, as well as drafting and implementing healthcare data policies. For example, Australia is one of the countries in the Asia-Pacific region that has established a dedicated digital health authority. The Australian Digital Health Agency was founded in 2016 and is responsible for patients' electronic health records, digital prescriptions, telehealth services and other digital health programmes falling under Australia's digital health strategy (Australian Digital Health Agency, 2021).

Recognising that the development of healthcare data policies benefits from different perspectives and multistakeholder insights, a designated agency that institutionalises and oversees these procedures could significantly help to implement and enforce new initiatives and existing policies. Specific appointed governing bodies would clearly appreciate that this task falls within their scope of responsibilities and be accountable for the effective implementation of digital health strategies and management of healthcare data policies. In addition to the responsibilities that such designated institutions would have on a national level, they should also aim to collaboratively address these issues at a regional level. Appointed governing bodies should serve as the national digital health representatives that participate in regional initiatives to improve digital health and effectively collaborate and communicate with countries in ASEAN and the wider Asia-Pacific.

R2. Improve transparency of countries' digital health uptake

One of the conditions that should be met to advance healthcare data utilisation and improve data exchange across Southeast Asia and the Asia-Pacific is increasing the transparency of digital health uptake in individual countries. Digital health initiatives and resources, such as the GDHI, are positioned to provide neutral platforms for countries to share their status on the different digital health-related elements, including healthcare data governance, legislation and policies, infrastructure, and standards and interoperability. By providing this information, digital health pioneers such as Singapore and Malaysia could support and empower other countries in

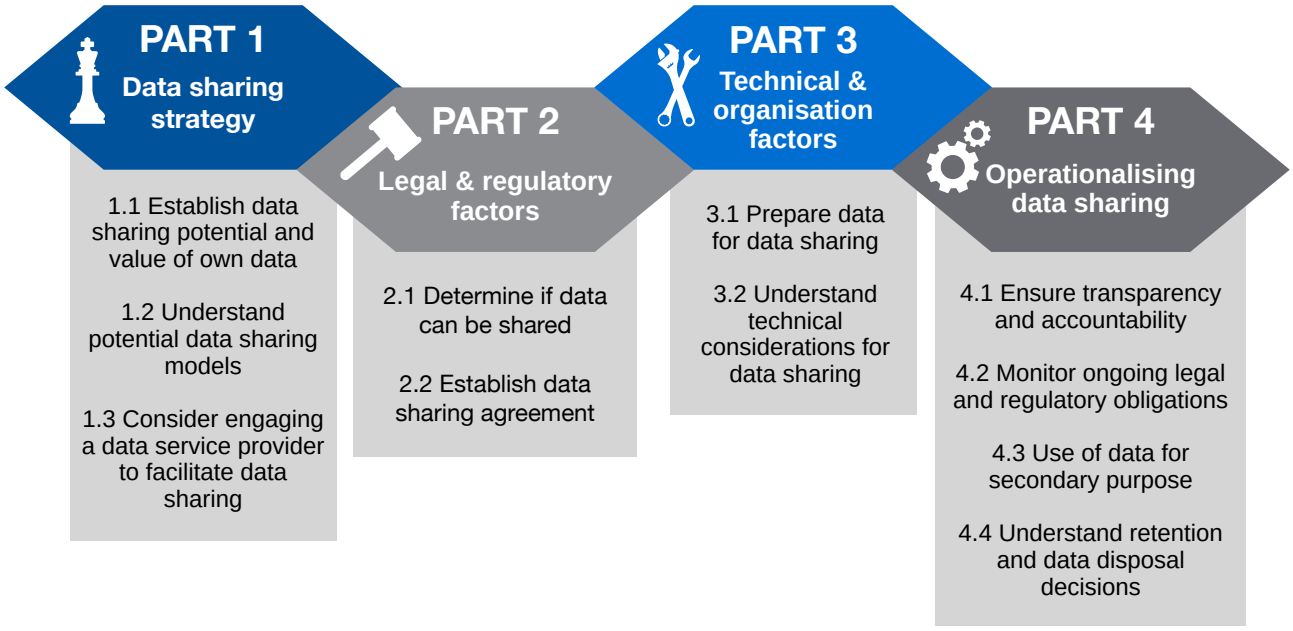
Southeast Asia to draft and implement best-practice data governance policies. In addition, sharing information allow countries to compare their national digital health strategy with those in the region, and aids the individual countries to identify and strengthen their areas of weakness. Such increased transparency would help to enhance regional digital health convergence, improve cross-border data exchange, and help strengthen health systems in the region as a whole.

R3. Develop a standardised and harmonised regional data-sharing framework

For governing bodies to create and implement these healthcare data policies effectively, the Asia-Pacific region would benefit from developing a standardised and harmonised regional data-sharing framework that includes streamlined terminology and guidance for different stakeholders to improve regional collaboration. In Southeast Asia, it is proposed for the ASEAN Secretariat to consider the development of this framework. With the current situation of differing or lacking data-sharing systems, safe and effective data exchange within and across Southeast Asian countries cannot be assured. Therefore, a mutually agreed upon standard framework could not only enhance cross-border data exchanges but also strengthen countries' existing national data-sharing frameworks. This would also provide a standard model for countries that are taking their first steps in the digital health space and do not yet have a framework in place. In addition, a standardised and harmonised data-sharing framework would provide guidance to the various stakeholders and help close the gap between the public and private sectors, resulting in stronger government-industry collaborations.

The Trusted Data Sharing Framework developed by IMDA and PDPC is one of the models that ASEAN can reference in developing a regional framework (Figure 5). Although created for the commercial, non-governmental industry and therefore requiring additional personal data protection measures for the public sector, the Trusted Data Sharing Framework provides a comprehensive overview of the different elements that governments and other governing institutions need to take into account to enhance the data-sharing environment (IMDA & PDPC, 2019)[12].

Figure 5. Trusted Data Sharing Framework developed by IMDA and PDPC.



[12] Detailed information regarding the 'Trusted Data Sharing Framework' can be accessed via the following link: https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

3.2. Strengthen data security and cybersecurity resilience

RECOMMENDATIONS

R4 *Conduct thorough analyses by multiple stakeholders to identify the degree of risk at each level.*

R5 *Establish essential principles and standardised frameworks to assess the safety and performance requirements of digital health data and tools.*

R6 *Develop incident response plans to react promptly to cyber threats and data security breaches.*

R4. Conduct comprehensive risk assessments

Institutions should conduct thorough analyses to identify the levels of risk at each level to prevent potential detrimental data breaches or other forms of cyberattacks. Different cybersecurity specialists have different risk assessment frameworks in place. IBM Security's models are useful references because the multinational technology company is a cybersecurity pioneer and frontrunner across various digital security domains (IBM Security, 2020). According to IBM, there are three main security risk management pillars that should be addressed to minimise the impact of security breaches - *risk assessment*, *risk reduction* and *risk management* (IBM Security, 2020). As the cybersecurity ecosystem is extremely complex (see Figure 3 on page 16), professional security consultants might be needed to perform a comprehensive cybersecurity risk assessment.

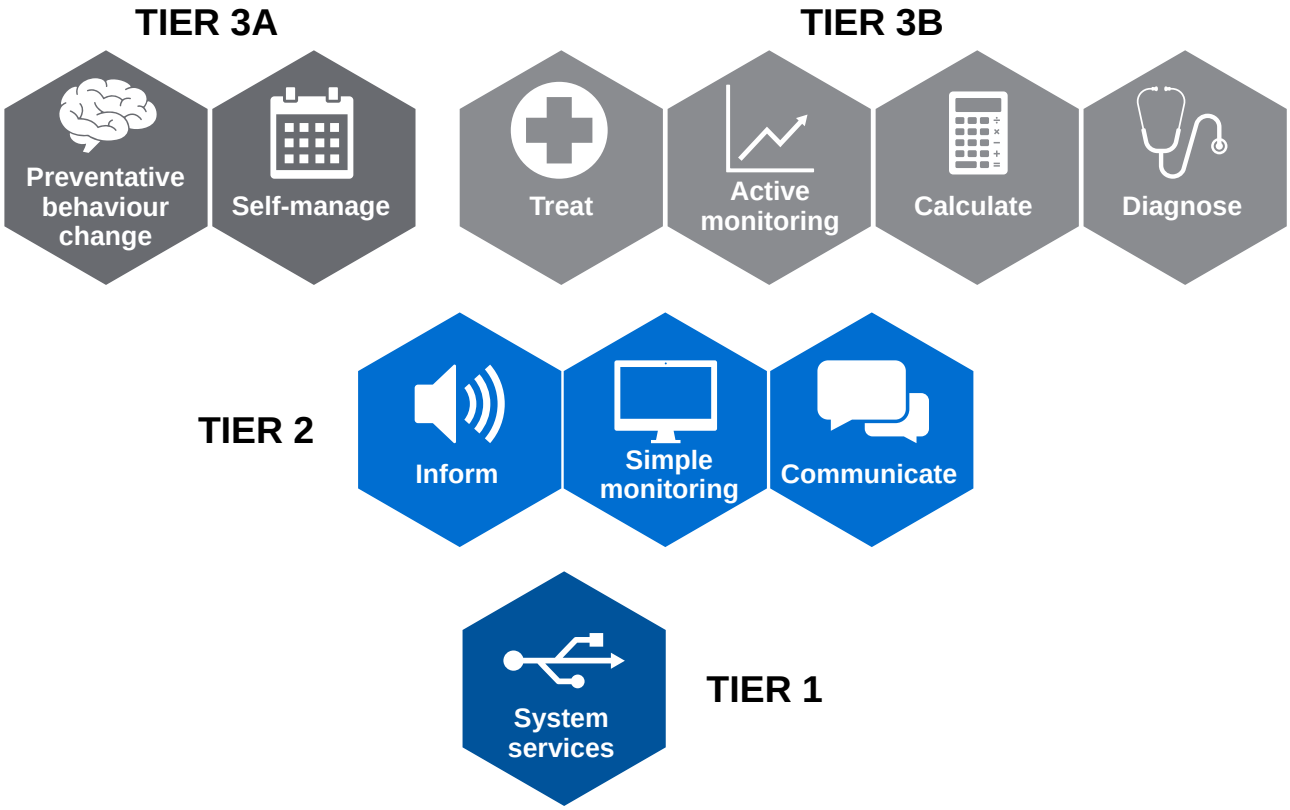
One of the frameworks that can be utilised to conduct this assessment is the PRISM approach: *Prioritise, Resource, Implement, Standardise and Monitor*. This model starts by assessing the different environments, such as the cloud, mobile devices and software, that can potentially be the institutional gateway for a cyberattack, and then calibrating the levels of risk associated with these attack vectors. Subsequently, the institution should evaluate and assign sufficient resources to deal with potential cyber threats and implement the means necessary to prevent further harm. In addition, agencies must standardise the procedures to prevent and cope with data breaches and cyberattacks, as well as continuously monitor the digital environment to identify unusual behaviour to act promptly if needed (Goel et al., 2018).

R5. Establish standardised frameworks for safety and performance requirements

Another important measure that strengthens data security and cybersecurity is the establishment of essential principles and standardised frameworks to assess the safety and performance requirements of digital health data and tools. These models are not only important at a national level, but multilateral standard frameworks are needed to enhance coherence across Southeast Asia and the Asia-Pacific to create a stronger regional digital health infrastructure. Similar to risk assessment analyses, different models exist to evaluate safety and performance requirements of

health products. However, the digital aspect in these frameworks is often lacking as the models are usually tailored towards more traditional health devices. One of the frameworks that does focus on digital health products is the Evidence Standards Framework for Digital Health Technologies from the UK-based National Institute for Health and Care Excellence (NICE) and is a potentially useful regional reference (Figure 6)[13].

Figure 6. Evidence Standards Framework for Digital Health Technologies developed by NICE.



This categorisation system helps to assess the general level of clinical risk associated with a digital health product. In addition, contextual questions could be added to further specify the level of risk. Subsequently, tier-specific evaluation tables are used to assess the digital health technology and determine if the product meets the minimum evidence standards. Once the digital health technology meets the required minimum standards, the product is considered safe enough to roll out (NICE, 2019).

R6. Develop incident response plans

In the unfortunate event that a data breach or cyberattack is successful, institutions need to have a strong incident response plan in place to react promptly and prevent further harm. Similar to a professional cybersecurity risk assessment, institutions could collaborate with cybersecurity and risk management specialists to strengthen security core elements, such as trained cybersecurity staff, best-practice processes and integrated digital solutions. In order to construct a robust

[13] Detailed information regarding the 'Evidence Standards Framework for Digital Health Technologies' can be accessed via the following link: https://www.nice.org.uk/Media/Default/About/what-we-do/our-programmes/evidence-standards-framework/digital-evidence-standards-framework.pdf

incident response plan, institutions should first understand the cybersecurity landscape and explore potential external and internal threats. This ties in with the previously mentioned cybersecurity risk assessment, where existing weaknesses and gateways that allow prospective attacks to occur must be identified. The next step is to develop standard guidelines that should be followed if the breach has been successful, including specific steps that need to be taken and by whom, key communication channels that should be utilised during the incident, and permission and escalation procedures to prevent additional damage. Once these standards have been established, they should be proactively tested and revised in a timely manner. Another important element is to leverage threat intelligence and ensure close collaboration among security specialists. Furthermore, institutions should not solely rely on the incident response plan by itself but combine it with ongoing security monitoring and investigations to detect any breach earlier and respond adequately. Lastly, and in line with the previous step, is the need for coordination and smooth collaboration among the previously mentioned security cornerstones, including trained security personnel, best-practice procedures and state-of-the-art technologies (IBM Security, 2017).

3.3. Promote regulatory innovation

RECOMMENDATIONS

R7 *Adopt innovative risk-based regulatory approaches that are fit-for-purpose for the iterative nature of digital health.*

R8 *Promote regulatory cooperation, recognition and reliance to facilitate timely access to digital health products and overcome resource limitations.*

R9 *Accelerate convergence to internationally recognised standards and guidelines such as ISO and IMDRF.*

R10 *Promote public-private collaborations to accelerate digital transformation of health product development and regulatory processes.*

R7. Adopt innovative fit-for-purpose risk-based regulatory approaches

Regulation for software-focused health products needs to be adaptive and suited to the iterative nature of the technology. Although traditional regulatory frameworks are generally quite static, more health authorities are shifting to a risk-based approach to calibrate the regulatory approach based on potential risk to patients.

Innovative models are emerging in the region that enable governments to learn more about the risks of new digital health technologies before implementing them in the wider population. One example is Singapore's regulatory sandbox model for telemedicine and mobile medicine described earlier. Innovative approaches such as pre-certification models and using real world evidence are also being pioneered by the USFDA. Regional regulators should consider adopting elements of these innovative models and develop more regulatory cooperation and reliance approaches with global health authorities. An important enabler for such innovative models is close collaboration with software developers. It is important for regulatory authorities to develop platforms and avenues for early dialogue in development.

R8. Promote regulatory cooperation, recognition and reliance

The APEC Life Sciences Innovation Forum (LSIF) established the Regulatory Harmonisation Steering Committee (RHSC) in 2008 to advance regulatory convergence[14] among APEC's 21 member economies. Many regulatory agencies in the region face resource constraints due to lack of manpower and technical capacity. Judicious use of reliance on decisions of larger, more advanced agencies while maintaining independence in final decision-making is one way to overcome these resource constraints without having to re-invent the wheel.

[14] Regulatory convergence is defined by the APEC RHSC as "a voluntary process whereby the regulatory requirements across economies become more aligned over time as authorities adopt internationally recognised technical guidance, standards and scientific principles and common or similar practices and procedures".

Surveys to measure progress in achieving the overall KPIs for convergence have been conducted since 2018. The most recent survey done in 2020 shows encouraging improvements since 2008 and again since 2019 in the number of APEC members which have attained full Pharmaceutical Inspection Co-Operation Scheme (PICS)[15] and International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH)[16] membership (Chong et al, 2020). Some of the more advanced regulatory authorities like Australia and Singapore have also joined international groupings that facilitate reliance, such as the ACCESS Consortium[17] and the Project Orbis initiative driven by the USFDA. Another example is the Singapore-Thailand Reliance pilot, where Singapore's HSA shares medical device evaluation reports with the Thai FDA. Although this pilot does not exclusively focus on digital health products, it demonstrates existing opportunities for potential regional collaboration (Gill, 2020).

57% (12) of APEC economies have reliance pathways that take into account and give significant weight to medical product assessments performed by other regulatory authorities in reaching their own decisions within a shorter timeline than that of their standard pathways. Among the Asian economies, only Brunei, Hong Kong, Indonesia, Malaysia, Singapore, Chinese Taipei and Thailand have such pathways. More can therefore be done to promote reliance as recommended by the WHO, which is based on its most recently published guidance on Good Reliance Practices (WHO, 2021). Key enablers to support reliance that are relevant to Asia-Pacific include but are not limited to:

- Initiatives to foster trust among regulatory authorities are essential. Trust can be built in phases, starting with exchange of assessment reports and moving to work-sharing or joint assessments;
- Information sharing and dialogue among regulators;
- Economic or legal integration through regional platforms such as APEC and ASEAN;
- Engagement of all relevant stakeholders including health authorities beyond regulators, industry, academia, clinicians, patients and civil society.

R9. Accelerate convergence to internationally recognised standards and guidelines

Convergence and harmonisation of requirements, standards and guidelines are important enablers of regulatory cooperation and reliance. In APEC, the RHSC Priority Work Area for Medical Devices was established in 2018 to promote international harmonisation initiatives, such as the Global Harmonisation Task Force (GHTF) and IMDRF guidance documents, and support capacity building and implementation in APEC economies. Although there are positive initiatives toward convergence and capacity building, some gaps remain. Regional economies should continue to leverage existing platforms for convergence convened by the APEC RHSC to enhance convergence for digital health. The following specific measures would accelerate convergence:

[15] PICS is a non-binding, informal collaboration between regulatory agencies focusing on good manufacturing practice of medical products across the globe.

[16] ICH is an initiative that connects regulatory authorities and the pharmaceutical industry to create greater harmonisation in pharmaceutical product development.

[17] The ACCESS Consortium is a collaborative network of regulatory agencies from Australia, Canada, Singapore, Switzerland and the United Kingdom.

- Support regulatory global digital health convergence through the recognition and adoption of internationally recognised guidance documents and standards, such as those developed by IMDRF and ISO;

- Promote regulatory authorities' adoption and implementation of SaMD Risk Categorization Framework and SaMD guidance based on IMDRF SaMD documents, including clinical evaluation, application of quality management systems, risk categorisation, and key definitions;

- Increase regional collaboration to conduct assessments on the progress in achieving KPIs for the RHSC Medical Devices Roadmap similar to what has been done for biopharmaceuticals;

- Encourage RHSC Medical Device PWA to incorporate IMDRF SaMD and AI guidance into the Medical Device PWA Core Curriculum and train regulatory authorities and industry stakeholders through RHSC Centers of Excellence.

R10. Promote public-private collaborations to accelerate digital transformation of health product development and regulatory processes

Conversations on regulation of digital health tend to focus on medical devices but there is also an opportunity to digitise medicine development as well. The COVID-19 crisis has accelerated the adoption of digital trials and remote monitoring. It has revealed that although the biopharmaceutical sector has innovation at its heart, many of the internal processes for development and regulatory communication are often manual. To make digital trials and future-ready regulatory processes a reality, several ecosystem changes are needed with public-private collaboration at the core:

- Collaboration between the standards development organisations and the regulatory authorities to reduce the disconnect between these two parties and accelerate digital transformation;

- Collaborative development, maintenance and cybersecurity support for cloud-based systems for trial data-sharing and regulatory submissions;

- Develop regulatory guidance specific to use of digital health technologies in clinical development;

- Develop international guidance for a regulatory framework for the use of novel endpoints derived from digital measures;

- Systematic and meaningful involvement of patients and the public in the development and approval of digital health technologies and policy decisions around regulatory data sharing.

3.4. A collaborative approach

RECOMMENDATIONS

R11 *Improve the digital health environment by strengthening ICT infrastructure and architecture, the health workforce's digital competency, and the public's digital literacy through capacity building.*

R12 *Leverage CoRE as a neutral academic platform to connect different types of stakeholders and move discussions on digital health regulation forward.*

R11. Improve the digital health environment through capacity building

ICT infrastructure and architecture, a *digitally competent health workforce*, and a *digitally literate public* are three key domains that should be strengthened through capacity building to improve digital health adoption.

In improving the ICT infrastructure and architecture, public organisations have to ensure that these digital structures contain up-to-date internet protocols with an emphasis on conformance and interoperability. In addition, physical elements, such as broadband networks, analytics and mobile platforms, need to be in place.

The second key domain is the upskilling of the healthcare workforce to ensure that staff have adequate digital competence to optimise the usage of digital health products and enhance the appropriate fusing of traditional healthcare with new technologies. Institutions should implement fundamental organisational changes that promote the incorporation of digital health technologies. In addition, different frameworks exist to provide guidance on improving staff digital competency. One of these frameworks is the 'Health and Care Digital Capabilities Framework' which is used to evaluate an individual's digital competence level and identify specific digital skills that need to be strengthened (National Health Service, 2018; Figure 7)[18].

The last key domain is improving the digital literacy of the general public, and digital health solutions should align with the public's digital skills. In order to effectively roll out digital health technologies and maximise the benefit of these products, patients, family members and other types of caregivers need to be aware of digital health systems and possess relevant digital skills. Therefore, governments need to carry out public awareness campaigns and implement digital competence programmes for citizens to increase this baseline. Countries in the Asia-Pacific region can also follow specific frameworks to enhance the public's digital competence, such as the model developed by the European Commission (International Telecommunication Union, 2018; Figure 8)[19].

[18] Detailed information regarding the 'Health and Care Digital Capabilities Framework' can be accessed via the following link: https://www.hee.nhs.uk/sites/default/files/documents/Digital%20Literacy%20Capability%20Framework%202018.pdf

[19] Detailed information regarding the 'Digital Competence Framework for Citizens' can be accessed via the following link: https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf

Figure 7. Health and Care Digital Capabilities Framework developed by NHS.

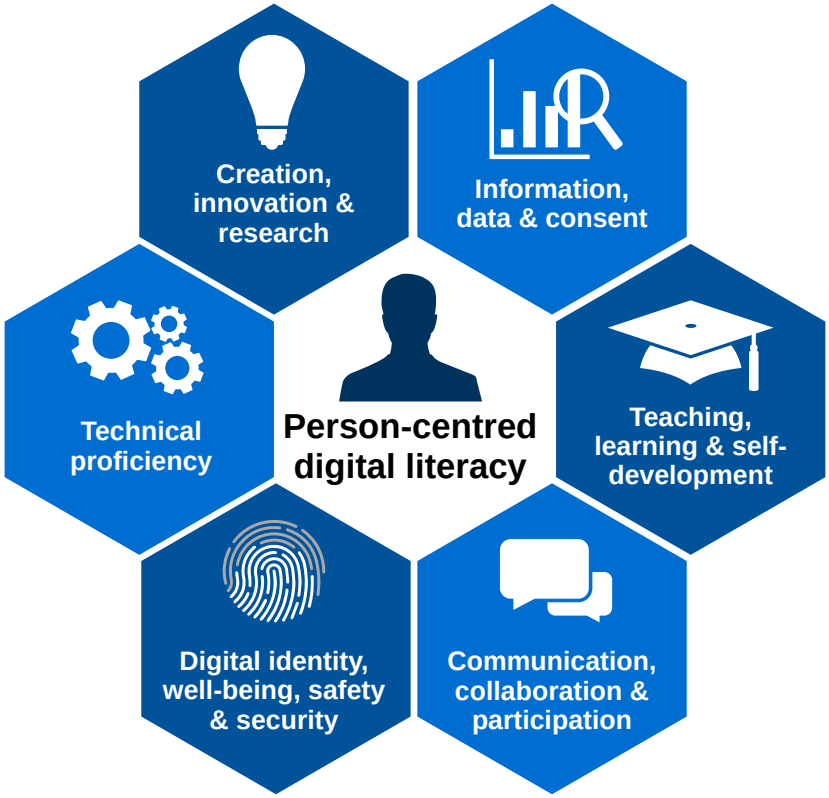
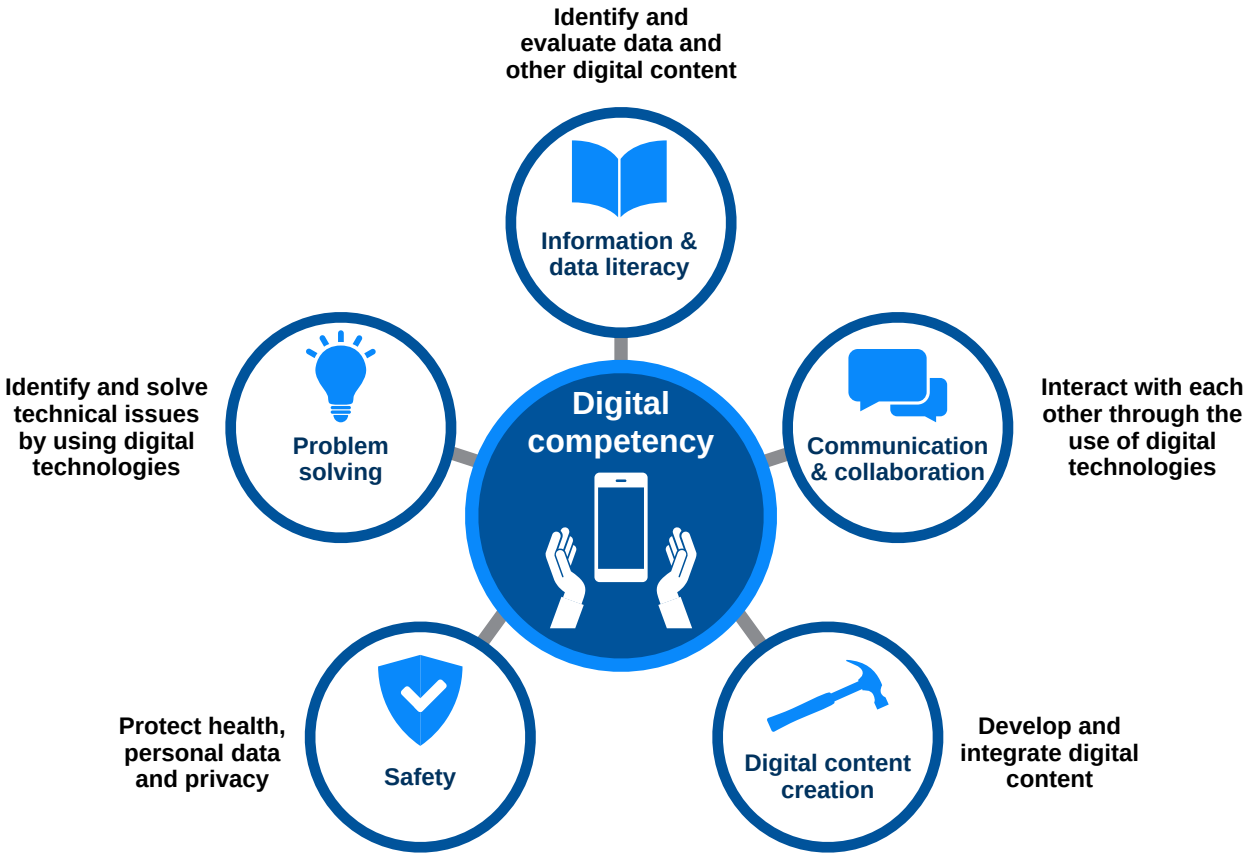


Figure 8. Digital Competence Framework for Citizens developed by the European Commission.



R12. Leverage CoRE as a neutral and academic platform

During the Roundtable breakout sessions, participants discussed the need for a neutral platform to move discussions on digital health regulatory issues forward. They suggested that CoRE could provide this platform, where the various stakeholders, including regulatory authorities, academia, NGOs and industry, could come together to share ideas concerning best practices, learn from each other, and openly engage in discussions on pressing digital health matters. Other regional and multilateral platforms such as the Asia eHealth Information Network (AeHIN) should also be leveraged to increase dialogue among stakeholders.

The Centre has a unique value proposition in enhancing regulatory capability and scientific excellence for health products and systems in the Asia-Pacific through its education programmes and think tank initiatives, and Digital Health is identified as a focus area to amalgamate efforts. Participants were therefore of the view that CoRE is well positioned to draw on its global network of experts and connectivity with the region's stakeholders to play an active role in strengthening capacity, fostering dialogue, facilitating collaboration, and supporting development and implementation of regionally relevant solutions.

3.5. Conclusion

The first two decades of the 21st century have already been associated with tremendous discoveries and rapid innovation in the health industry. It has also been an era with seismic new global health challenges, including the SARS, Zika and Ebola outbreaks, and the current COVID-19 pandemic. New digital health technologies that have been rapidly developing and evolving offer huge potential for addressing a wide range of health and medical challenges, playing an important role in combatting diseases, and improving the health and well-being of the world population in both developing and developed countries. Amongst the various issues that need to be resolved to realise the full future potential of digital health, the need for clear and robust regulatory frameworks and policies stands out as a critical area to ensure safe and effective application of digital health solutions.

CoRE's 2020 Digital Health Roundtable aimed to help ASEAN and Asia-Pacific regional efforts by fostering dialogue among stakeholders to define the pressing issues and identify potential solutions. Three key issues of concern were highlighted: healthcare data policies, data security and cybersecurity, and digital health regulation. Countries in the Asia-Pacific region will benefit from agile regulatory frameworks that can cope with the rapid changing environment for digital health products and technologies as well as the implementation of reliance and recognition mechanisms. Governments and other institutions need proper data-sharing policies and regulations, together with strong data security and cybersecurity measures to protect sensitive and personal information, in order to improve local and cross-border data exchange. Moreover, a multistakeholder approach is needed to create greater convergence and harmonisation of digital health policies, regulations, and overall governance.

Ongoing engagement among local and regional stakeholders to clarify and coordinate regulatory frameworks is essential to realise the full potential of digital health in the Asia-Pacific. CoRE will continue to provide the neutral academic platform to strengthen capacity, facilitate discussions, build collaborations and follow through. Building on the CoRE 2020 Digital Health Roundtable and this White Paper discussing digital health issues at a broader level, CoRE will collaborate with its stakeholders to identify critical areas for subsequent more in-depth follow up.

Authors

Mr Allard W de Smalen

Dr Nokuthula Kitikiti

Mr Ananda P Muthalagu

Mr Cherng Yeu Neo

Adj Asst Prof Hishamuddin Badaruddin

Assoc Prof Silke Vogel

Prof John CW Lim

Centre of Regulatory Excellence (CoRE), Duke-NUS Medical School, Singapore

Acknowledgements

The organising committee would like to thank all speakers and participants for making this virtual Roundtable engaging and impactful. We also thank Roche for supporting the Roundtable.

CoRE CN: 2021_WP001_Enabling Digital Health Adoption in the Asia-Pacific

Contact us

Browse us
www.duke-nus.edu.sg/core

Email us
core@duke-nus.edu.sg

Follow us

https://www.linkedin.com/company/centre-of-regulatory-excellence/

@CoREdukeNUS

@CoREdukeNUS

Scan us

References

Accumulus Synergy. (2021, May). *Welcome to Accumulus Synergy*. https://www.accumulus.org/

American Academy of Family Physicians. (2021, May). *What's the difference between telemedicine and telehealth?* https://www.aafp.org/news/media-center/kits/telemedicine-and-telehealth.html

Australian Digital Health Agency. (2021, May). *Information for Everyone*. https://www.digitalhealth.gov.au/

Carrington, N., Hathi, M., Sarno, R., Su, J., Thornback, J., & Veigas, V. (2021, February). Digital health regulation in Asia-Pacific: overview and best practices. DIA Global Forum. https://globalforum.diaglobal.org/issue/february-2021/digital-health-regulation-in-asia-pacific-overview-and-best-practices/

Chong, S. S. F., Kim, M., Limoli, M., Obscherning, E., Wu, P., Feisee, L., Nakashima, N., & Lim, J. C. (2021). Measuring progress of regulatory convergence and cooperation among Asia–Pacific Economic Cooperation (APEC) member economies in the context of the COVID-19 pandemic. *Therapeutic Innovation & Regulatory Science*, 1-13.

Coravos, A., Khozin, S., & Mandl, K. D. (2019). Developing and adopting safe and effective digital biomarkers to improve patient outcomes. *NPJ digital medicine*, *2*(1), 1-5.

DIA Europe (2021) Transformative Disruption to Regulatory Submissions and Approvals: Accumulus Synergy. March 15, 2021.

European Medicines Agency. (2020). *Questions and Answers: Qualification of digital technology-based methodologies to support approval of medicinal products*. https://www.ema.europa.eu/en/documents/other/questions-answers-qualification-digital-technology-based-methodologies-support-approval-medicinal_en.pdf

Gill, H. (2020). Regulatory Reliance. APACMed. http://www.imdrf.org/docs/imdrf/final/meetings/imdrf-meet-200921-singapore-webconference-26.pdf

Global Digital Health Index. (2021, May). *World map*. http://index.digitalhealthindex.org/map

Goel, A., Haddow, J., & Kumar, A. (2018). *Managing cybersecurity risk in government: an implementation model*. IBM Center for The Business of Government. http://www.businessofgovernment.org/sites/default/files/Managing%20Cybersecurity%20Risk%20in%20Government.pdf

IBM Security. (2017). Six steps for building a robust incident response function. https://www.ibm.com/downloads/cas/QEBYPND1

IBM Security. (2019). *Cost of a data breach report*. https://www.ibm.com/downloads/cas/RDEQK07R

IBM Security. (2020). *Strategies for managing cybersecurity risk: assess and advance your security and compliance posture*. https://www.ibm.com/security/digital-assets/strategy-risk-management-ebook/pdfs/Strategy_Risk_Management_EB.pdf

Infocomm Media Development Authority of Singapore and Personal Data Protection Commission. (2019). *Trusted data sharing framework*. https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

International Medical Device Regulators Forum. (2014). *"Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations*. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf

International Medical Device Regulators Forum. (2021). *"Artificial Intelligence Medical Device (AIMD) Working Group Update*." http://www.imdrf.org/docs/imdrf/final/meetings/imdrf-meet-210316-korea-webconference-aimd.pdf

International Telecommunication Union. (2018). *Digital skills toolkit*. https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/ITU%20Digital%20Skills%20Toolkit.pdf

Kozlakidis, Z., Abduljawad, J., Al Khathaami, A. M., Schaper, L., & Stelling, J. (2020). Global health and data-driven policies for emergency responses to infectious disease outbreaks. *The Lancet Global Health*, *8*(11), e1361-e1363.

Leong, M. H. J., Vogel, S., Kitikiti, N., & Muthalagu, A. P. (2020). *Artificial intelligence in healthcare: landscape, policies and regulations in Asia-Pacific*. Duke-NUS Medical School Centre of Regulatory Excellence. https://www.duke-nus.edu.sg/docs/librariesprovider5/default-document-library/niha_white-paper_ai-in-healthcare_vfinal-23102020.pdf?sfvrsn=1c5e2636_0

Leptak, C. (2020). *Regulatory Guidance and Evidentiary Criteria for Drug Development Tools*. Food and Drug Administration. https://fnih.org/sites/default/files/pdf/2%20-%20Leptak_Reg%20Guidance%20DDT.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. *Bmj*, *358*.

Ministry of Health Singapore. (2021, May). *Licensing Experimentation and Adaptation Programme (LEAP) - A MOH Regulatory Sandbox.* https://www.moh.gov.sg/home/our-healthcare-system/licensing-experimentation-and-adaptation-programme-(leap)---a-moh-regulatory-sandbox

National Health Service. (2018). *A health and care digital capabilities framework.* https://www.hee.nhs.uk/sites/default/files/documents/Digital%20Literacy%20Capability%20Framework%202018.pdf

National Health Service. (2019). *Universal personalised care: implementing the comprehensive model.* https://www.england.nhs.uk/wp-content/uploads/2019/01/universal-personalised-care.pdf

National Institute for Health and Care Excellence. (2019). *Evidence standards framework for digital health technologies*. https://www.nice.org.uk/Media/Default/About/what-we-do/our-programmes/evidence-standards-framework/digital-evidence-standards-framework.pdf

National University of Singapore Yong Loo Lin School of Medicine. (2019, October). *#EthicallySpeaking: Ethics framework for big data in health and research*. https://medicine.nus.edu.sg/ethicallyspeaking-delivering-a-practical-framework-for-ethical-decision-making-involving-big-data-in-health-research/

Organization for Economic Co-operation and Development. (2015). *Health data governance: privacy, monitoring and research – policy brief*. https://www.oecd.org/health/health-systems/Health-Data-Governance-Policy-Brief.pdf

Pan, C., Latimer, J., & Gaebler, J. A. (2020). Transforming the regulatory landscape for digital health technologies in drug development. Biogen – Health Advances. https://www.biogen.com/content/dam/corporate/en_us/pdfs/all-PDFs/Biogen-Regulatory-Policy-White-Paper_Transforming-the-Regulatory-Landscape-for-Digital-Health-Technologies-in-Drug-Developmen.pdf

Robertson, A. S., Malone, H., Bisordi, F., Fitton, H., Garner, C., Holdsworth, S., ... & Wegner, M. (2020). Cloud-based data systems in drug regulation: an industry perspective. *Nature Reviews Drug Discovery*, *19*(6), 365-366.

Roche. (2020). *Roche personalised healthcare: small differences, big effects*. https://www.roche.com/dam/jcr:f63fdbe0-0c97-428d-9f36-819b723e9780/en/phc_brochure.pdf

Scott, B. K., Miller, G. T., Fonda, S. J., Yeaw, R. E., Gaudaen, J. C., Pavliscsak, H. H., ... & Pamplin, J. C. (2020). Advanced digital health technologies for COVID-19 and future emergencies. *Telemedicine and e-Health*, *26*(10), 1226-1233.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare 8*(2), 133.

Standards and Interoperability Lab – Asia. (2021, May). *Home*. http://sil-asia.org/

Stewart, J., Honig, P., AlJuburi, L., Autor, D., Berger, S., Brady, P., ... & Wegner, M. (2020). COVID-19: A Catalyst to Accelerate Global Regulatory Transformation. *Clinical Pharmacology and Therapeutics*. Systems Solution Inc, 2021

Sust, P. P., Solans, O., Fajardo, J. C., Peralta, M. M., Rodenas, P., Gabaldà, J., Garcia Eroles, L., Comella, A., Munoz, C. V., Sallent Ribes, J., Monfa, R. R., & Piera-Jimenez, J. (2020). Turning the crisis into an opportunity: digital health strategies deployed during the COVID-19 outbreak. *JMIR public health and surveillance*, *6*(2), e19106.

United States Food and Drug Administration. (2020). What is Digital Health? https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health

United States Food and Drug Administration. (2021, April). *Clinical Outcome Assessment (COA) Qualification Program*. https://www.fda.gov/drugs/drug-development-tool-ddt-qualification-programs/clinical-outcome-assessment-coa-qualification-program

United States Food and Drug Administration. (2021, May). *Digital Health Software Precertification (Pre-Cert) Program*. https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-program

Vayena, E., Dzenowagis, J., Brownstein, J. S., & Sheikh, A. (2018). Policy implications of big data in the health sector. *Bulletin of the World Health Organization*, *96*(1), 66.

Weeramanthri, T. S., Dawkins, H. J., Baynam, G., Bellgard, M., Gudes, O., & Semmens, J. B. (2018). Precision public health. *Frontiers in Public Health*, *6*, 121.

World Health Organization. (2021). WHO Expert Committee on Specifications for Pharmaceutical Preparations: Fifty-fifth report (WHO Technical Report Series, No. 1033) https://apps.who.int/iris/bitstream/handle/10665/340323/9789240020900-eng.pdf

Annex A

Programme and speakers

Day 1: 18 November 2020 | 5 pm to 8 pm (Singapore time)

Time	Topic	Speaker/Facilitator
5.00pm	**Welcome and opening remarks**	**Prof John Lim** Executive Director Centre of Regulatory Excellence (CoRE) Duke-NUS Medical School
5.10pm	**Keynote** Opening presentation by WHO	**Mr Bernardo Mariano Jr** Chief Information Officer & Director Digital Health Innovation World Health Organization (WHO)
5.25pm	**Healthcare data policies** • Policy for healthcare data governance • Considerations in protecting patients privacy	**Mr Colin Lim** Chief Information Officer & Group Director InfoComm Technology and Data Ministry of Health Singapore
5.40pm	**Data security** • Health data cybersecurity management and best practices in risk mitigation • Cloud-based data storage and data residency	**Mr Ralph K Ramsey** Global Associate Partner Healthcare and Life Sciences Leader IBM Security Services
5.55pm	**Preparing health systems for integrated and personalised care** • Integrating advancement in medicines, diagnostics and digital health technologies • Identifying essential elements of health systems to implement personalised care	**Dr Nick Guldemond** Senior Researcher Leiden University Medical Center Visiting Professor IM Sechenov First Moscow State Medical University
6.05pm	**Digital health in APAC: An industry perspective*** * Views of companies are listed in Annex B	**Dr Daniel Thurley** General Manager Roche, Hong Kong
6.15pm	**Q&A**	**Prof John Lim** CoRE
6.25pm	**Break**	
6.35pm	**Breakout session** • Group 1: Healthcare data policies • Group 2: Health systems for integrated and personalised care	Facilitated breakout sessions with participants
7.10pm	**Group sharing and discussions** (Up to 5 minutes sharing per group)	**Prof John Lim** CoRE
7.50pm	**Summary and closing remarks**	**Prof John Lim** CoRE
8.00pm	**End of Day 1**	

Day 2: 19 November 2020 | 5 pm to 8 pm (Singapore time)

Time	Topic	Speaker/Facilitator
5.00pm	**Opening remarks and recap of Day 1**	**Adj Asst Prof Hishamuddin Badaruddin** Adjunct Assistant Professor CoRE
5.10pm	**Digital health products regulations** • Creating a balance between innovation and regulation • Regulatory paradigm shift	**Mr Sukhjit Singh** Senior Manager Community Engagement and Strategic Partnerships, APAC Healthcare Information and Management Information and Management Systems Society **Dr Sethuraman Rama** Director Medical Devices Branch Health Sciences Authority, Singapore
5.25pm	**Capacity building** • Creating awareness on digital health technologies among public and healthcare stakeholders • Regulatory training on digital health products	**Asst Prof James Leong** Head of Pharmaceutical Regulatory Science Programme CoRE, Duke-NUS Medical School
5.40pm	**Q&A**	
5.50pm	**Break**	
6.00pm	**Breakout session** • Group 1 & 2: Digital health products regulations • Group 3 & 4: Capacity building	Facilitated breakout sessions with participants
6.45pm	**Group Sharing and Discussions** (Up to 5 minutes sharing per group)	**Adj Asst Prof Hishamuddin Badaruddin** CoRE
7.30pm	**Prioritising digital health focus areas: Next steps**	**Adj Asst Prof Hishamuddin Badaruddin** CoRE
7.45pm	**Summary and concluding remarks**	**Prof John Lim** CoRE
8.00pm	**End of Day 2**	

Annex B

Roundtable participants

Regulatory Authorities and other Government Agencies	Academia/NGO	Industry
Brunei Darussalam (3) China (1) Hong Kong (3) Indonesia (1) Malaysia (3) Singapore (3) Thailand (1)	World Health Organization, South-East Asia Regional Office (1) Queensland University of Technology, Australia (1) Diagnostics Development Hub, Singapore (1) Leiden University Medical Center, The Netherlands (1) National Taiwan University, Chinese Taipei (2)	Amazon Web Services (1) IBM Security Services (1) Johnson & Johnson (2) Merck Sharp & Dohme (2) Roche (6) Sanofi (2) Ubie (1)
15	**6**	**15**


DukeNUS
Medical School


Centre of
Regulatory Excellence