Building Resilient Health Systems in a Digital Era:

Cybersecurity in Remote Care Management

OCTOBER 2023

LEK™ APACMed
The voice of MedTech

Table of Contents

00.Foreword

Remote Care Management (RCM) has been a huge area of growth within healthcare systems globally and in APAC, both super-charged by the necessities of COVID but also in the post-pandemic era. In the future, RCM will become a mainstay in the healthcare system due to its significant benefits to patients (improving accessibility and affordability of healthcare), healthcare providers (i.e., enables providers to overcome manpower and infrastructure shortages to serve more patients) and payors (i.e., enables payors to reimburse health services at lower cost per patient).

As RCM is integrated into more healthcare settings and scenarios, there is a deluge of data now being collected, stored and analyzed via a wide diversity of platforms.

The explosion in the quantity and quality of private health data increases the appeal and hence the risk associated with inadvertent exposure and malign actors, from inappropriate access to sophisticated cybercrimes conducted by organized syndicate-organised cyber-threats.

In APAC, the escalating risk of data breach incidents has prompted regulatory entities and stakeholders to explore the establishment of cybersecurity regulation that applies specifically to RCM. New regulation also comes with significant risk to achieving the benefits that RCM promises to patients, clinicians, institutions and payors.

The objective of this paper is to illustrate the cybersecurity challenges faced as RCM grows in the market, highlight aspects of globally-established cybersecurity framework that can be relevant for RCM in APAC, and provide recommendations for effective measures addressing RCM cybersecurity challenges within the Asia-Pacific region.

01. Executive Summary

While RCM has already brought significant benefits such as increased accessibility and affordability to the Asia-Pacific (APAC) ecosystem, RCM innovation is expected to further revolutionize healthcare delivery and advance healthcare coverage in APAC.

To realize the benefits of RCM while maintaining cybersecurity efficiently, healthcare ecosystems and their stakeholders (i.e., policymakers, medical device manufacturers, healthcare providers) have to collaborate to enact effective and industry-relevant regional cybersecurity policies.

Therefore, in 2023 APACMed and L.E.K. Consulting conducted primary research through interviews with regional and international experts, including policy makers and industry experts. Incorporating the discussions from these interactions and drawing from global best-practices, recommendations for RCM cybersecurity policy standards were formed.

These recommendations include:

1
Governments and policymakers should tailor existing cybersecurity frameworks into an APAC-recognized cybersecurity regulatory framework that are consistent with globally approved standards. Further, government and policymakers should ensure that the frameworks are recognized across APAC countries jurisdictions and translate the cybersecurity regulatory framework into clear technical requirements for stakeholders. In the long term, as cybersecurity threats constantly evolve, policymakers should actively engage with other nations' policymakers as well as industry experts to refine RCM cybersecurity frameworks against latest cybersecurity developments.

2
With RCM-specific frameworks established, medical device manufacturers should aim to implement technical measures following the cybersecurity framework, such as classifying data collected and ensuring they are processed and stored compliant to national guidelines. Further, medical device manufacturers should collaborate with clients (i.e., hospital providers) and external vendors to ensure confidential information is secured. In the long term, as cybersecurity grows in importance, medical device manufacturers should invest in AI-powered cybersecurity to increase product competitiveness.

3
Healthcare providers' IT departments have to maintain a secure architecture, ensure the safe integration of hospital infrastructure with medical devices and organize internal data security training for healthcare staff and patients to follow cybersecurity protocol and their role to minimize the risk of cyber threats.

With the collaboration of healthcare ecosystem participants, all markets in APAC should be able to feasibly implement the recommendations across short and long-term horizons.
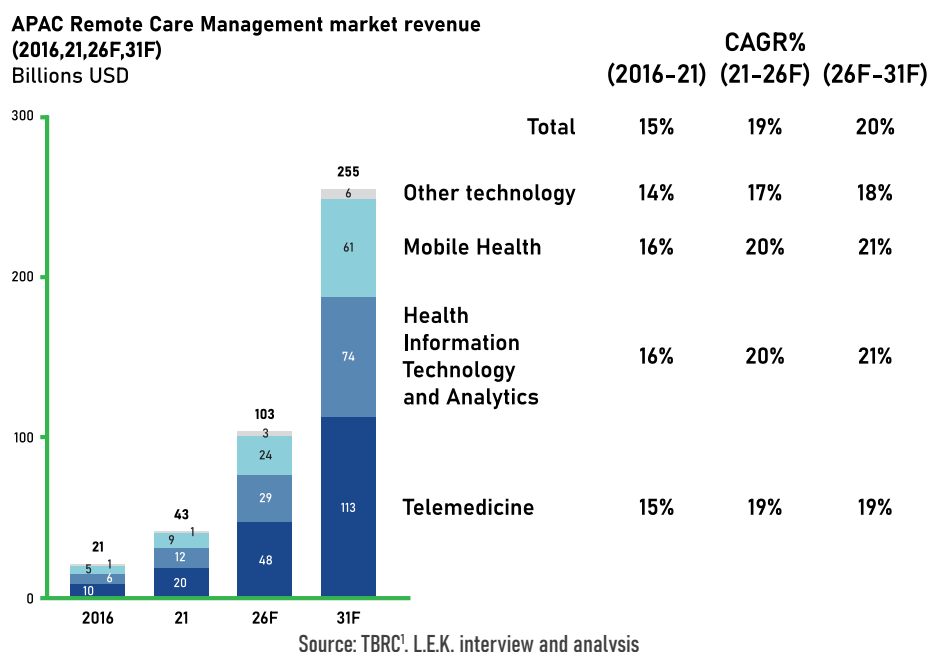
02. Evolution of Remote Care Management

2.1 RCM Market Overview

Remote care management (RCM) has emerged as a transformative force revolutionizing healthcare delivery in the digital era. RCM solutions enable patients to receive treatment beyond conventional clinical settings and enable data–driven, personalized care by leveraging information and communication technologies at scale.

Going forward, RCM will be broadly and permanently integrated into the healthcare system due to its significant benefits to patients (i.e., improving accessibility and affordability of healthcare), healthcare providers (i.e., enabling providers to overcome manpower and infrastructure shortages to serve more patients) and payors (i.e., enabling better outcomes at lower cost per patient/ episode).

Recognising these benefits of RCM to stakeholders across the healthcare ecosystem, the RCM market has seen growth of 15% annual growth in APAC and is projected to accelerate further to approximately 20% annual growth until 2031. (see Figure 1.)

Figure 1. APAC RCM Market Size, 2016–31

APAC Remote Care Management market revenue
(2016,21,26F,31F)
Billions USD

	CAGR% (2016–21)	(21–26F)	(26F–31F)
Total	15%	19%	20%
Other technology	14%	17%	18%
Mobile Health	16%	20%	21%
Health Information Technology and Analytics	16%	20%	21%
Telemedicine	15%	19%	19%

Chart data:
- 2016: Total 21 (10, 6, 1, 5)
- 21: Total 43 (20, 12, 1, 9)
- 26F: Total 103 (48, 29, 24, 1, 3)
- 31F: Total 255 (113, 74, 61, 6)

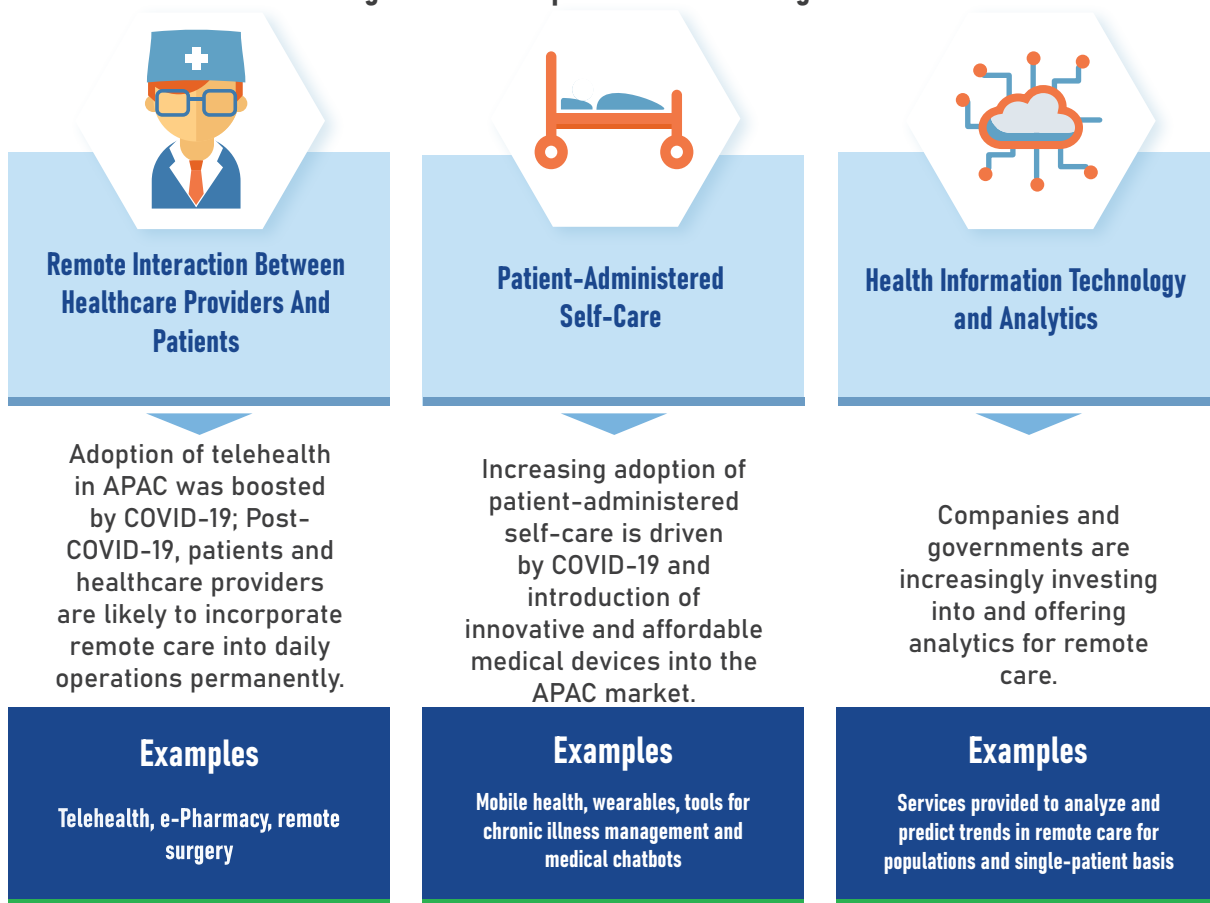Source: TBRC[1], L.E.K. interview and analysis

2.2 RCM Segments

The rapid development of RCM solutions has transformed the healthcare system, with a profound and enduring impact on all sub-segments (refer to Figure 2). This includes:

1. Remote interactions between healthcare providers and patients – Telemedicine
2. Patient-administered self-care – Mobile health
3. Health information technology and analytics

Figure 2. RCM Capabilities Across Segments

Remote Interaction Between Healthcare Providers And Patients

Adoption of telehealth in APAC was boosted by COVID-19; Post-COVID-19, patients and healthcare providers are likely to incorporate remote care into daily operations permanently.

Examples

Telehealth, e-Pharmacy, remote surgery

Patient-Administered Self-Care

Increasing adoption of patient-administered self-care is driven by COVID-19 and introduction of innovative and affordable medical devices into the APAC market.

Examples

Mobile health, wearables, tools for chronic illness management and medical chatbots

Health Information Technology and Analytics

Companies and governments are increasingly investing into and offering analytics for remote care.

Examples

Services provided to analyze and predict trends in remote care for populations and single-patient basis

Source: L.E.K. interview and analysis

Remote Interaction Between Healthcare Providers and Patients

The COVID-19 pandemic has served as a catalyst for the widespread adoption of RCM. For example, RCM effectively alleviated strain on highly constrained, physical in-hospital capacity, enabling healthcare providers to prioritize more severe cases and those requiring a physical intervention. Additionally, telehealth has proven invaluable in enabling patients to access care regardless of their location. Across Southeast Asia countries, the rural population with limited access to healthcare services forms a significant percentage of the total population (i.e., 50% for Thailand and Philippines, 70% for Cambodia[2]).

However, with relatively high internet penetration (i.e., >70% in 2023), patients will be able to access healthcare services more efficiently through RCM[3]. The realization of the significant benefits offered by RCM is poised to drive a substantial and permanent integration of RCM into daily operations post-COVID-19 (See Figure 3).

Figure 3. APAC Telehealth Usage Indexed to Current Utilization

APAC telehealth usage indexed to current utilization
(Nov. 11–Dec. 2, 2020 COVID-19 Hospital Survey)
Percentage (current usage = 100%)
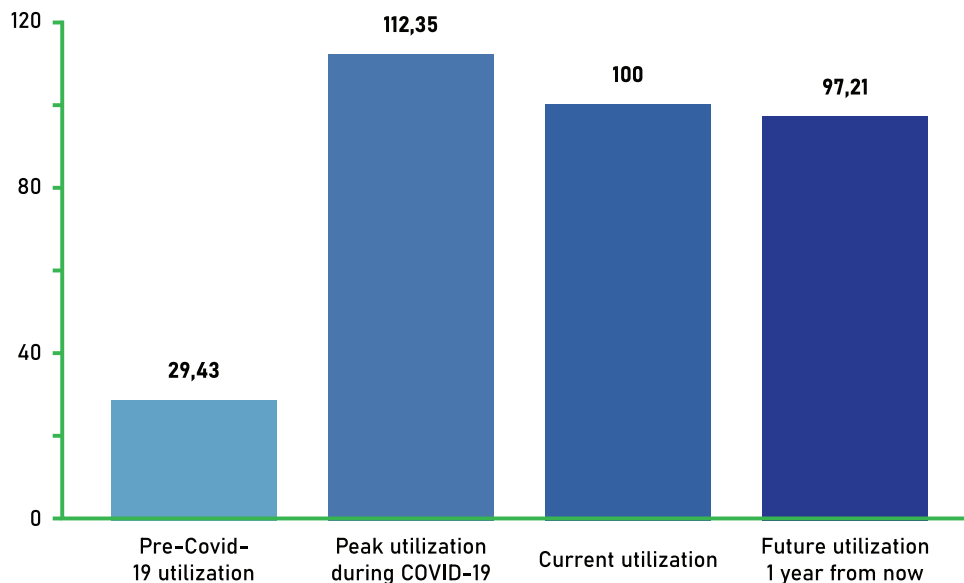
Source: L.E.K. Hospital Survey 2023

Patient-Administered Self-Care

The rising adoption of patient-administered self-care in APAC is propelled by a combination of factors: the impact of COVID-19 and the launch of innovative and cost-effective medical devices. The pandemic has underscored the significance of personal health maintenance, prompting individuals to prioritize self-care practices. Concurrently, manufacturers are responding to this growing demand by launching new consumerized medical devices at affordable price points, enabling wider adoption among consumers.

Health Information Technology and Analytics

Since COVID-19, both the private sector and governments are ramping up their investments in the provision of remote care analytics. (See Figure 4) These analytics are instrumental in informing efficiency of care spend during times of constrained resources.

Looking beyond the pandemic, remote care analytics also hold immense potential in population and individual patient analytics, further enhancing healthcare outcomes and enabling proactive care management.

Figure 4. Company and Government Investment Activities on Remote care

Nervotec (Singapore)

Nervotec employs machine learning and deep learning to transform smartphones with a camera into a triaging and vital signs monitoring gadget.

In 2022, Nervotec partnered with Prudential to develop Pulse, an AI-powered mobile app to help Prudential's customers track their vital signs (i.e., heart rate, oxygen saturation levels) by scanning their face.

JD.COM (China)

PharmCOO is a platform developed by JD.com where doctors' prescriptions will be reviewed and circulated to offline pharmacies.

In 2020, JD.com received an investment of more than $830 million from Hillhouse Capital to develop its digital health products/services, including PharmCOO.

Dr.Answer (South Korea)

Government-sponsored consortium including 25 medical institutions and 21 AI developers

Dr Answer analyzes medical data from patients to diagnose and remotely advises doctors on treatment plans.

Total of $40 million has been invested towards the development of Dr. Answer thus far since 2018.

Source: Company websites, L.E.K. interview and analysis

03. Growth of RCM in APAC

3.1 Key Drivers of RCM in APAC

While RCM in APAC countries is relatively nascent compared to other countries (i.e., penetration in APAC countries such as Thailand is less than 20%[4] compared to 40%[5] in the United States), adoption is expected to accelerate reflecting positive drivers across various stakeholders:

Medical Device Manufacturers and Other Industry (e.g., Telecommunication) Players

Broadband network coverage

With the widespread deployment of 5G networks in APAC (i.e., APAC will have over 1.4 billion 5G connections by the year 2030[6]) existing and future RCM solutions will be increasingly enabled and cost effective.

RCM developers expanding use cases

Companies are investing in expanding the use cases of remote care, with use cases spanning prevention through post-acute management in an ever-increasing range of disease areas.

Patients

Growing awareness among patients

With stronger marketing and word-of-mouth, as well as increased availability and support of clinicians, patients are becoming aware of the benefits, and open to adopting RCM solutions.

Increasing affordability of RCM

By 2035, APAC will have 210m more middle-income families[7] (disposable income between USD 20-70k/year) than in 2020 (~5% YoY growth across 2020-2035), increasing the affordability for remote care. Many countries including Australia, South Korea, Japan, China (People's Republic of China) , Singapore, Thailand and Vietnam have also introduced government reimbursement for telemedicine; further APAC countries are in discussion to establish telemedicine reimbursement.

"By 2035, APAC will have 210m more middle-income families (disposable income between USD 20-70k/ year) than in 2020 (~5% YoY growth across 2020-2035), increasing the affordability for remote care."
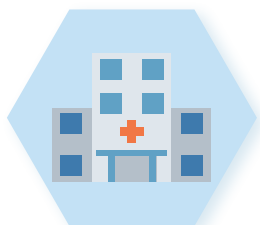
Healthcare Providers

Care institutions and payors supporting new models of care

APAC countries are adopting new models of care delivery to increase access to healthcare, particularly in LMICs (e.g., Telemedicine companies such as MSI international and MeetDocter entering into Cambodia)..
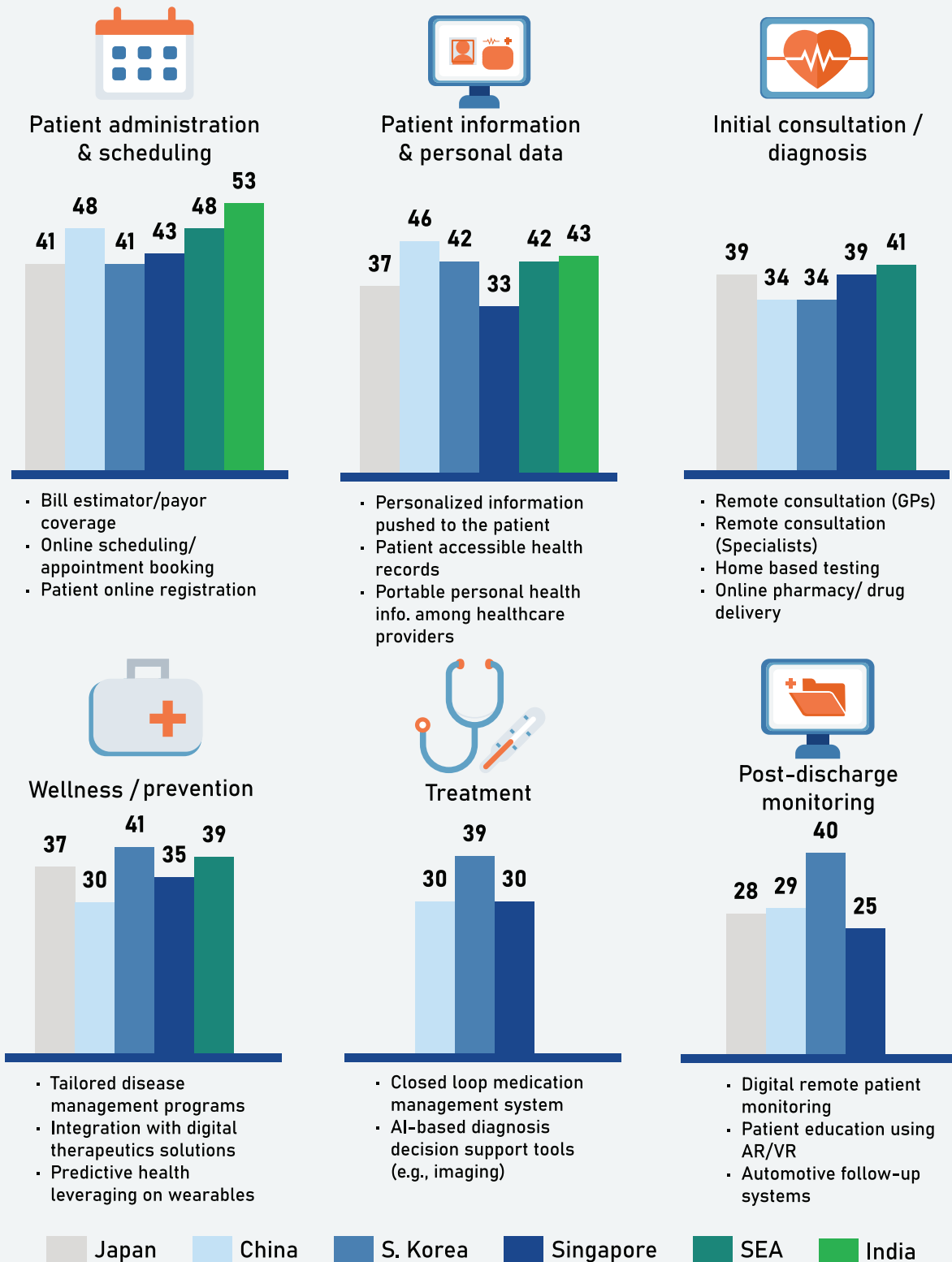
Increased adoption among healthcare providers

Hospitals in the APAC region are also actively driving the development of RCM solutions. L.E.K.'s 2023 APAC Hospital Survey[8] of 530 hospital executives across public and private hospitals in countries across the APAC region recorded that digital solutions have gained significant traction in the APAC region. Close to half of participating hospitals embrace implementation of digital solutions with a high adoption rate (See Figure 5). Key RCM solutions that are currently adopted include remote consultation, predictive health programs and digital-enabled remote patient monitoring.

Figure 5. Adoption of Digital Solutions by APAC Hospitals

Adoption of digital solution*

Percentage of respondents 'currently using' digital solutions

Patient administration & scheduling
- Bill estimator/payor coverage
- Online scheduling/ appointment booking
- Patient online registration

Patient information & personal data
- Personalized information pushed to the patient
- Patient accessible health records
- Portable personal health info. among healthcare providers

Initial consultation / diagnosis
- Remote consultation (GPs)
- Remote consultation (Specialists)
- Home based testing
- Online pharmacy/ drug delivery

Wellness / prevention
- Tailored disease management programs
- Integration with digital therapeutics solutions
- Predictive health leveraging on wearables

Treatment
- Closed loop medication management system
- AI-based diagnosis decision support tools (e.g., imaging)

Post-discharge monitoring
- Digital remote patient monitoring
- Patient education using AR/VR
- Automotive follow-up systems

Legend: Japan | China | S. Korea | Singapore | SEA | India
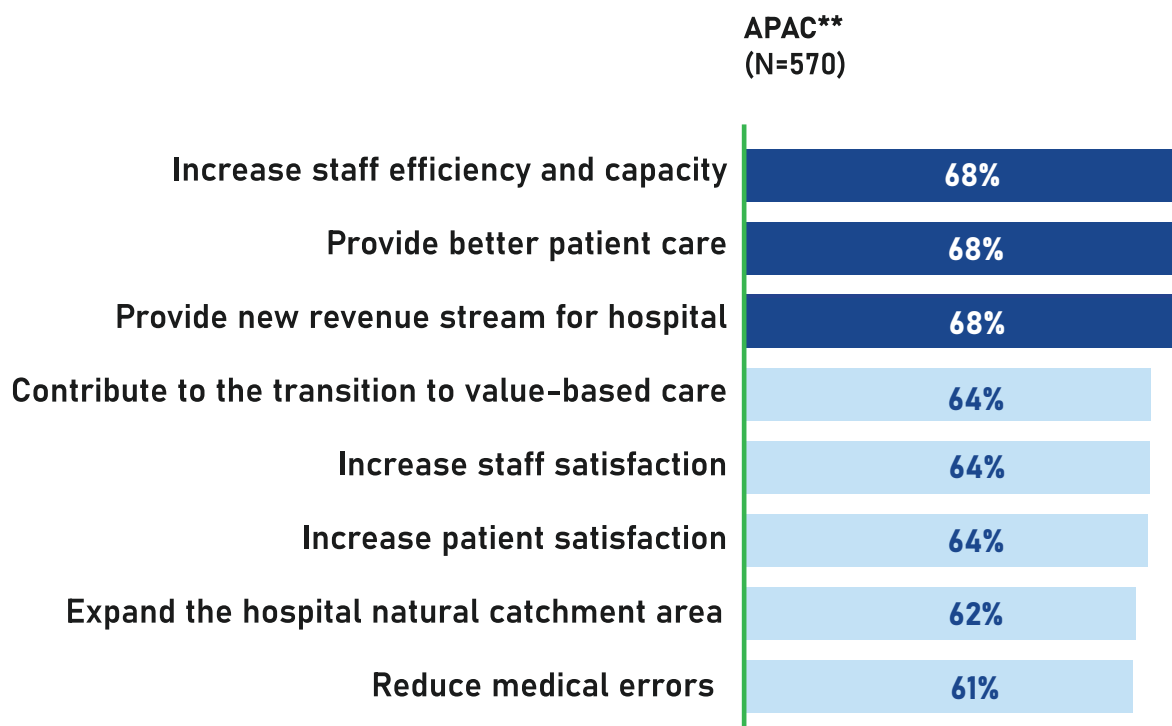
Source: L.E.K. Hospital Survey 2023

Survey question: 'Digitalization of hospitals is gaining traction in many countries. What digital health solutions have you adopted/would you like to adopt?' Respondents who answered that the hospital is 'currently using' each digital solution.

There is growing priority placed on RCM across APAC because healthcare providers increasingly recognize the potential for digital solutions to transform and enhance healthcare delivery (See Figure 6). By embracing digital health, organizations can optimize operations (i.e., capacity and cost benefits), enhance patient outcomes, and unlock new opportunities for growth in the healthcare sector.

Figure 6. Value from Digital Health Solution Adoption by APAC Hospitals

Value from digital health solution adoption*
Percentage of respondents that chose 6 and 7 (1-7 scale, 1 — least, 7 — most)

APAC**
(N=570)

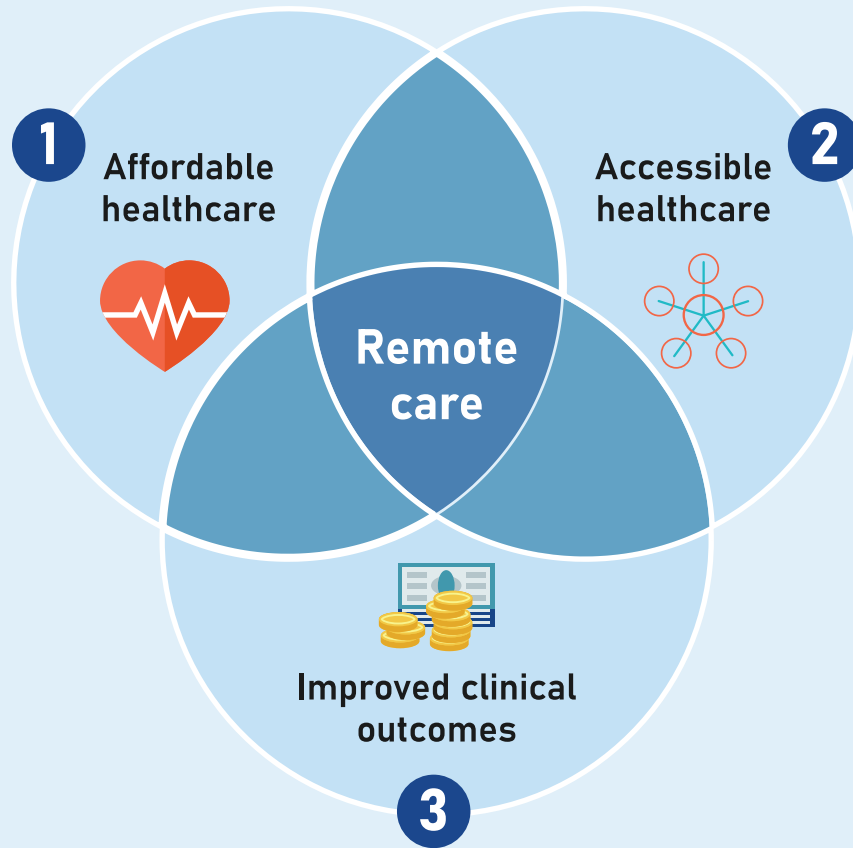|	
Increase staff efficiency and capacity	68%
Provide better patient care	68%
Provide new revenue stream for hospital	68%
Contribute to the transition to value–based care	64%
Increase staff satisfaction	64%
Increase patient satisfaction	64%
Expand the hospital natural catchment area	62%
Reduce medical errors	61%

Source: L.E.K. Hospital Survey 2023

Survey question: 'What value do you think digital health solutions will likely bring about for your hospital? ("1"=not likely, "7"=very likely)

Going forward, RCM is expected to become an essential component of the healthcare ecosystem as it offers access, cost efficiency and improved patient outcomes (See Figure 7).
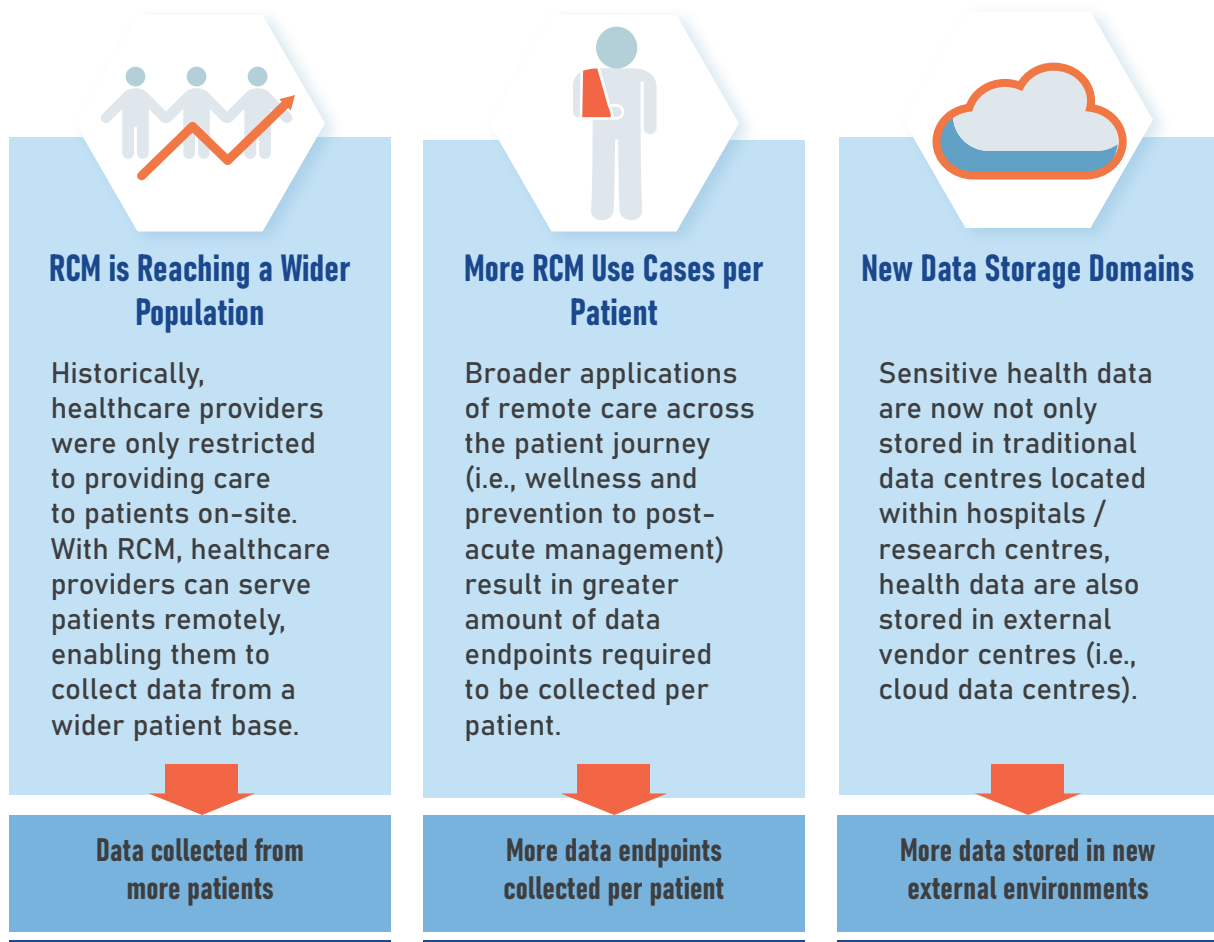
Figure 7. RCM Roles in Healthcare System

	Patients	Healthcare Providers	Payors
1 Affordability	Remote care such as self-care and telehealth reduces consultation and treatment costs for patients	Remote care enables providers to offer more affordable business models, expanding their patient base	Remote care enables payors to reimburse for patient health at a lower cost per patient
2 Accessbility	Remote care enables patients to overcome geographical barriers and receive treatment	Remote care enables providers to overcome manpower and infrastructure shortages to serve more patients	Remote care enables public payors to ensure larger population receive healthcare access and insurance firms to provide more attractive healthcare coverage for customers
3 Improved Clinical Outcomes	With more consistent monitoring of patients and advanced analytics, remote care increases quality of care provision to patients and reduces financial burden on payors		

Source: L.E.K. interview and analysis

3.2 Generation of Large Quantities of High-Quality Data Attracts Risk of Cyberthreats

As APAC healthcare stakeholders recognize the benefits of RCM and implementing it into their ecosystem, 3 key dynamics relating to data and cybersecurity are particularly relevant (See Figure 8).

Figure 8. Key Trends of RCM in APAC

RCM is Reaching a Wider Population	More RCM Use Cases per Patient	New Data Storage Domains
Historically, healthcare providers were only restricted to providing care to patients on-site. With RCM, healthcare providers can serve patients remotely, enabling them to collect data from a wider patient base.	Broader applications of remote care across the patient journey (i.e., wellness and prevention to post-acute management) result in greater amount of data endpoints required to be collected per patient.	Sensitive health data are now not only stored in traditional data centres located within hospitals / research centres, health data are also stored in external vendor centres (i.e., cloud data centres).
Data collected from more patients	More data endpoints collected per patient	More data stored in new external environments

Source: L.E.K. interview and analysis

RCM is Reaching a Wider Population

Traditionally, healthcare was mainly delivered within the confines of the hospital, restricting the amount of patients healthcare providers can serve and the agglomeration of data. Interlinked care networks expanded the pools of data. With RCM, however, healthcare providers are able to serve patients remotely (i.e., telehealth), enabling them to engage on an ongoing basis with a much wider population. For example, Halodoc (Indonesia telemedicine company) serves significant more patients (~7 million patients a month[9]) compared to one the largest Indonesia private hospitals RS Pantiwilasa dr Cipto (~20k patients a month[10])

More RCM Use Cases Per Patient

A typical patient journey spans wellness and prevention, early-stage identification, diagnosis and treatment, chronic disease management, and post-acute management; this journey is now experiencing a broader integration of RCM.

As the use cases of RCM continue to expand across the entire patient journey, more data types and endpoints about each person will be collected, and typically with much greater frequency than traditional care models would capture (i.e., Holter monitor is limited to data storage of internal chip, but biotelemetry can collect significantly large amounts of data that will be uploaded to the cloud)

New Data Storage Domains

Historically, health data were localized to hospitals or medical research centres, either in paper records or on-premise / premise-specific data storage solutions. However, with the generation of an exponential of new amount of data, and the emergence of IaaS services (e.g., private cloud / public cloud storage solutions) health professionals are now drawing on sensitive health data that is distributed in increasingly differentiated environments.

For example, many health records are now not only stored in traditional data centres located within hospitals, but many of these records are now also stored in external v endor data centres (i.e., cloud data centres) and some patient data types (e.g., blood glucose measurements) may be stored in proprietary vendor systems.

The sprawl of medical data across geographically distanced data centres and users increases the number of potential points of data egress and hence the cyber risk profile.

As a result of above dynamics, multiple cybersecurity risks across the patient journey have been created. For example, data generated from wearables may put the patient's location safety at risk if compromised. Further, incidents of cybercrime and data breaches have been on the rise in the APAC region recently (i.e., Ministry of Health Singapore database exposure[11], 39 million patient records stolen from Thailand's Siriraj Hospital[12])

Traditional care providers, as they step into this new operating model, also voice reasonable concerns about patient privacy for digital health, and such concerns regarding the handling of private data are the top concern for hospitals in the L.E.K. hospital survey (See Figure 9).

Figure 9. Digital Health Adoption Concerns

Digital health adoption concerns*
Percentage of respondents

Digital health adoption concerns*
Percentage of respondents
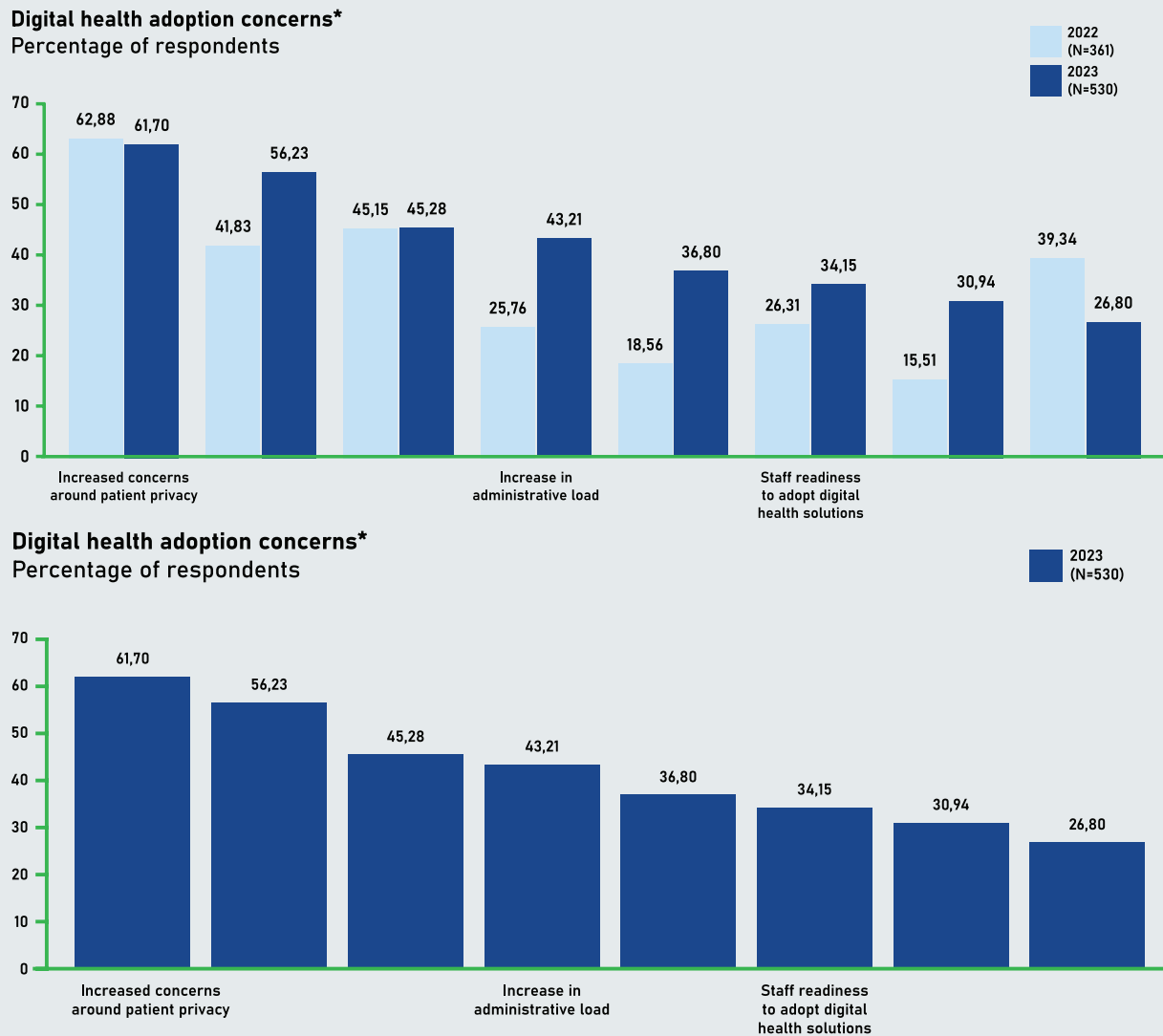
Source: L.E.K. Hospital Survey 2023

Survey question: 'What are your concerns for digital health adoption?'

So, while RCM brings significant and unique advantages for APAC's healthcare systems, the growth of RCM also brings inherent cyber risk. The progress of RCM, and delivery of its inherent benefits, requires broad stakeholder confidence that these benefits can be reaped safely; regulatory safeguards have to be established and consistently enforced across RCM device manufacturers and healthcare providers.

04. Cybersecurity Challenges of RCM

4.1 Key Challenges of RCM in APAC

There are significant cybersecurity challenges that currently exist for different stakeholders in APAC's RCM landscape (See Figure 10).

Figure 10. Cybersecurity Challenges of RCM in APAC

Government and Policymakers
Cybersecurity frameworks.

Medical Device Manufacturers
Regulatory and technical guidance for medical device manufacturers are not adapted for remote care devices.

Healthcare Providers and Patients
User education and integration of medical devices into healthcare infrastructure.
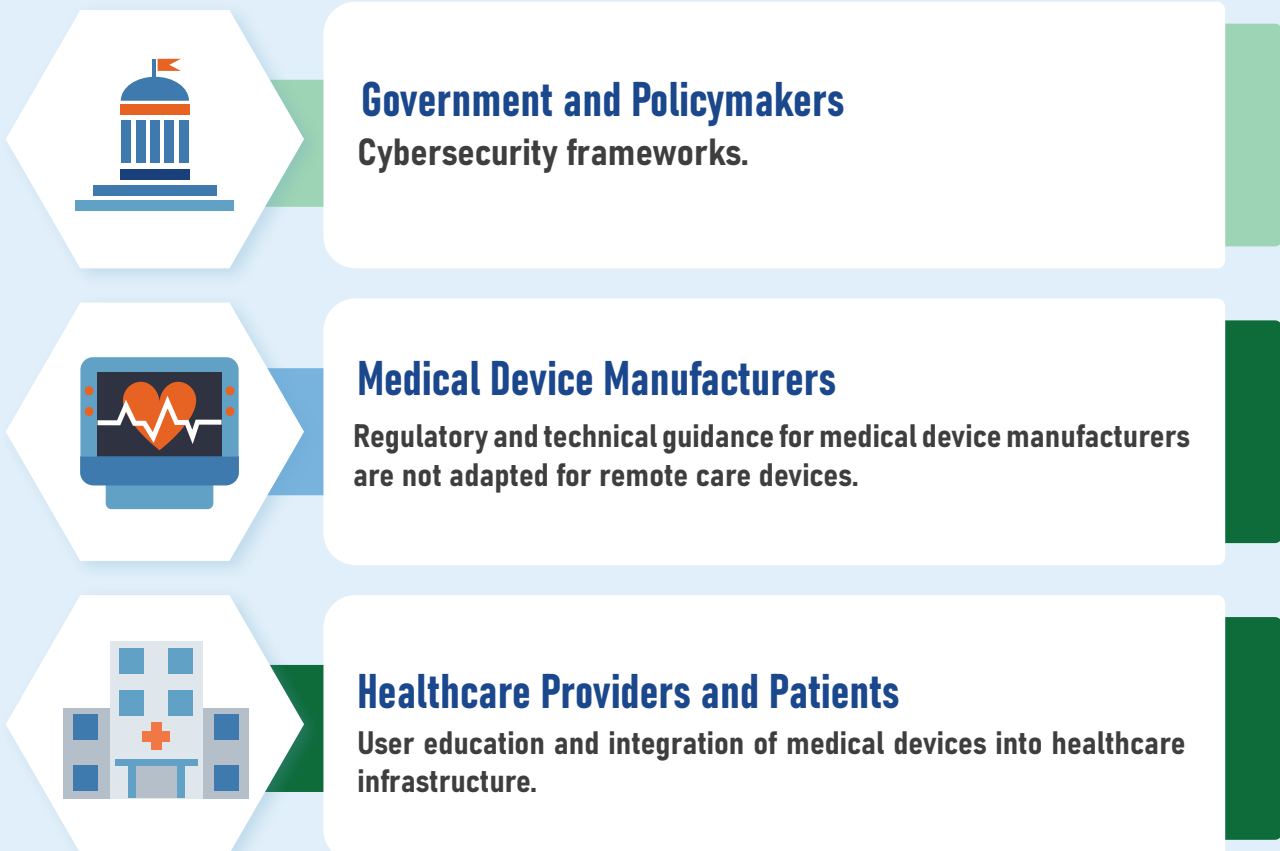
Source: L.E.K. interview and analysis

4.2 Challenges by Stakeholders

The lack of RCM-specific regulatory frameworks results in challenges for various stakeholders such as policymakers, medical device manufacturers and healthcare providers.

Government and Policymakers

First, existing cybersecurity frameworks across the APAC region are not fully adapted to various RCM solutions and lack harmonization (or cross-recognition) across jurisdictions. The data security protections are not well-established, and there are challenges with enforcement compared to more developed markets in Europe and America (See Figure 11).

Moreover, there is a pressing need for APAC to tailor existing healthcare and cybersecurity frameworks to support RCM.

Last, the regulation of remote and software medical devices is not as stringent as that of standard hardware medical devices, raising the potential risk of data breaches.

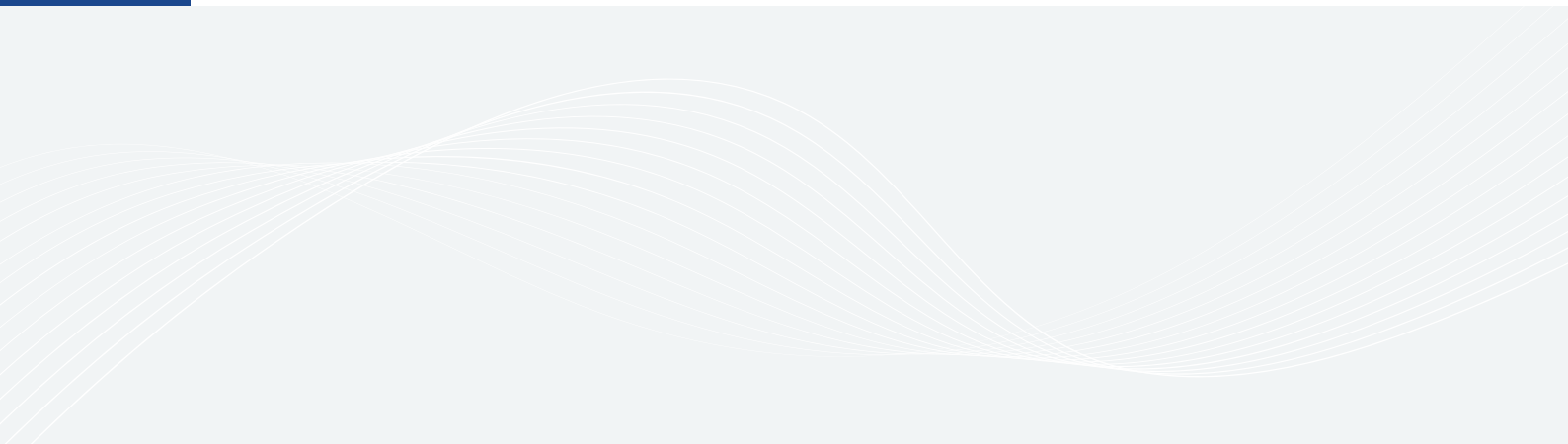**Figure 11. Existing CybersecurityFramework in Selected Countries**

	COUNTRY	CYBERSECURITY FRAMEWORK	GUIDELINES OF RCM	RULES/ REGULATION/ LAW OF RCM	RCM-CYBERSECURITY FRAMEWORK
Global Benchmark	**United States**	V	V	V	V
	Germany	V	V	V	V
APAC Countries	Japan	V	V	V	Not available yet, current general cybersecurity frameworks* apply
	China	V	V	V	
	South Korea	V	V	V	
	Singapore	V	V	Healthcare Services Act	
	Thailand	V	V	V	
	Malaysia	V	V	V	
	Vietnam	V	V	V	
	Indonesia	V	V	V	
	Philippines	V	V	V	
	India	V	V	not available yet	
	Australia	V	V		
	New Zealand	V	V		not available yet
	Cambodia	not available yet	not available yet		
	Myanmar				

Source: DLA Piper[13], L.E.K. interview and analysis

Across APAC, data transfer is generally allowed with consent and sufficient cybersecurity protection established while data storage is allowed beyond hospitals in most countries, although the China is a notable exception. A detailed reference on data transfer and storage is shown in Figure 12.

Figure 12. Existing Cybersecurity Framework in Selected Countries

EXAMPLE APAC COUNTRIES	KEY GOVERNING LAW	DATA COLLECTION AND PROCESSING	DATA TRANSFER (WITHIN COUNTRY, OVERSEAS)	DATA STORAGE (LOCALLY OR CLOUD)
Japan	Act on the Protection of Personal Information (APPI)	Voluntary, clear and prior consent of the individual concerned before processing collecting and processing medical data	**Within country:** Companies must obtain direct consent from the data subject and receiving entity must meet APPI **Overseas:** Additional consent is still required before overseas transmission of data, prior consent not required if the destination country (1) has data protection regime same equivalent to Japan or (2) data protection system meets standards in accordance to APPI (i.e., Europe)	**Location of storage:** No specific laws, but Guidelines for Safety Management of Medical Information by Providers of Information Systems and Services Handling Medical Information state that medical data should be stored within Japan **Cloud storage:** Data can be stored externally (beyond hospital) and in the cloud (i.e., Fujitsu)
China	Personal Information Protection Law (PIPL), Data Security Law (DSL), Cybersecurity Law (CSL)		**Within country:** The DSL regulates transfer of data depending on the data's classification level **Overseas:** Chapter 3 of PIPL requires to (1) inform users, (2) ensure that the foreign recipient of the data has in place data protection requirements that are no less stringent than PIPL, (3) recipient to be reviewed by Cyberspace Administration of China	**Location of storage:** DSL state that medical data should be stored within China **Cloud storage:** Can only be stored in the hospital's own private cloud at present
South Korea	Personal Information Protection Act (PIPA)		**Within country:** Consent is required from subject and receiving entity must meet PIPA **Overseas:** Permitted with (1) the consent of the data subject, (2) international agreements or overseas recipient to whom the data is transferred has obtained a data protection certification by the PIPC	**Location of storage:** Medical data should be stored within Korea **Cloud storage:** South Korean government allows digital hospital records to be stored externally in offsite cloud data centres (i.e., Amazon Web Services)
Australia	Privacy Act and Australian Privacy Principles (APP)		**Within country:** Companies must obtain direct consent from the data subject and receiving entity must meet APP **Overseas:** Companies are not prohibited by the Privacy Act from transmitting, keeping, or processing personal information outside of Australia. However, if a corporation does so, it must guarantee that the subject consents and that the receiver does not violate the APPs in respect to the information, unless an exemption exists, according to APP 8.1	**Location of storage:** Health records regulations prohibit publication of health records outside of the relevant State/Territory in various States/Territories (e.g., NSW and Vic). Further, original "My Health Records" and copies of them are not permitted to leave Australia. **Cloud storage:** Data can be stored externally (beyond hospital) and in the cloud (i.e., Intergrid)
Singapore	Personal Data Protection Act (PDPA)		**Within country:** Companies must obtain direct consent from the data subject and receiving entity must meet PDPA **Overseas:** Except in line with the conditions provided by the PDPA, organizations must not transmit any personal data to a country or territory other than Singapore	**Location of storage:** Medical data should be stored within Singapore **Cloud storage:** Data can be stored externally (beyond hospital) and in the cloud (i.e., H-Cloud)
India	Digital Information Security in Healthcare Act (DISHA)		**Within country:** Companies must obtain direct consent from the data subject and receiving entity must meet DISHA **Overseas:** Under a contract or intra-group plan authorised by the Data Protection Authority ("DPA"), medical data can be moved outside of India if sufficient protection measures are in place	**Location of storage:** Medical data should be stored within India **Cloud storage:** Data can be stored externally (beyond hospital) and in the cloud (i.e., Google Cloud)

Source: Government websites: Japan[14 15 16], China[17 18], South Korea[19 20 21], Australia[22], Singapore[23], India[24 25], L.E.K. interview and analysis

In comparison to other regions, APAC markets are generally still in the early stages of developing RCM-specific cybersecurity frameworks (See Figure 13). The maturity level of these frameworks remains relatively nascent, highlighting the need for continued efforts to establish robust regulatory measures and comprehensive cybersecurity frameworks that are tailored specifically to the unique challenges of RCM in the APAC region.

Therefore, addressing these gaps through targeted remote healthcare–specific cybersecurity laws is essential to safeguard patient data and mitigate cybersecurity risks in the APAC region.

Figure 13. Regulatories and Frameworks in Selected Countries

| COUNTRY	RCM REGULATIONS	RCM-CYBERSECURITY FRAMEWORKS
Germany	In Germany, remote care standards are governed by a patchwork of numerous laws, rules, and directives. Remote care is regulated by **the German Patients Data Protection Act ("PDSG"), the German Social Code Book V ("SGB V"), the German Federal Framework Agreement for Physicians ("BMV-Ä"), the German Drug Act ("AMG"), the German Act on Drug Advertising ("HWG"), the Model Professional Code for Physicians in Germany ("MBO-Ä") and the Model Professional Code for Psychological Psychotherapists and Child and Youth Psychotherapists ("MBO-P").**	Personal data processing for remote care services is largely controlled by the **General Data Protection Regulation (EU) 2016/679 ("GDPR"),** as well as the **German Federal Data Protection Act ("BDSG").**
US	The practice of remote care is **governed at the state level or professional standards set by state professional licensing authorities** such as the Board of Medicine. According to the New York State Education Law, every telehealth provider in New York must be registered or certified and have a valid registration.	The current federal legislation controlling the use of personal health information is the **Health Insurance Portability and Accountability Act of 1996 ("HIPAA").** HIPAA, on the other hand, only applies to persons and businesses that fulfil the criteria of a "covered entity" or a "business associate" of a covered entity, **leaving a significant quantity of personal health information unprotected.**
Singapore	RCM devices are subjected to the **pre-market regulations by HSA;** Post-market approval, RCM devices will also be then subjected to **each hospital's medical device operational policy.**	The **Personal Data Protection Act 2012 (No. 26 of 2012) ("PDPA")** protects personal data. From 2025, the full Cybersecurity Labelling Scheme for medical devices, CLS(MD), is expected to be mainstreamed, which aims to enable healthcare purchasers to make informed decisions towards buying more secure devices; thus, elevating the usage of cyber secure medical devices.
Japan	**The Medical Practitioners' Act (the "Act")** and several recommendations issued by the Minister of Health, Labour, and Welfare (the "MHLW") and other government authorities control remote care in general. Medical device manufacturers in Japan largely adhere to the 3G / 3M culture to ensure high standards are met during medical device development and production.	Data privacy regulations available but not specific to telehealth. In Japan, **the Act on the Protection of Personal Information ("APPI")** governs the provision of remote care .
China	Remote care is governed by a set of **administrative rules promulgated by the PRC National Health Commission and National Administration.**	Data privacy regulations available but not specific to telehealth. Administrative Measures for Internet Diagnosis and Treatment requires medical institutions **to follow all applicable laws and regulations on healthcare data information security,** including the Cyber Security Law.

Source: DLA Piper[13], L.E.K. interview and analysis

Regulatory Strength

Nascent   **Advanced**
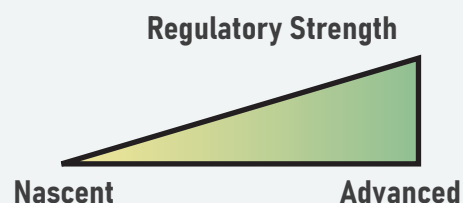
Medical Device Manufacturers

Current frameworks governing cybersecurity in APAC are not specific to remote care management solutions, leading to complex regulatory processes to certify new remote care management solutions. As a result, although there is demand for remote care solutions due to their significant incremental cost-savings and quality of care benefits, there is friction medical device manufacturers to bring to market new remote care management solutions.
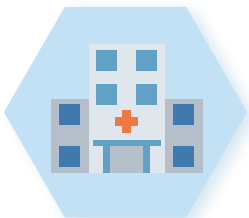
Healthcare Provider and Patients

The limited integration of cybersecurity measures into current healthcare operations is predominantly attributed to the substantial costs involved and the operational challenges that arise due to limited RCM-specific frameworks available.

In terms of architecture integration, as there is insufficient regulatory guidance for healthcare providers, most RCM systems are either built independently or lack proper integration with existing healthcare infrastructure and electronic health records. Additionally, due to inconsistent cybersecurity standards, manufacturers and third-party software providers still face challenges in ensuring interoperability between their remote care medical devices and hospital systems.
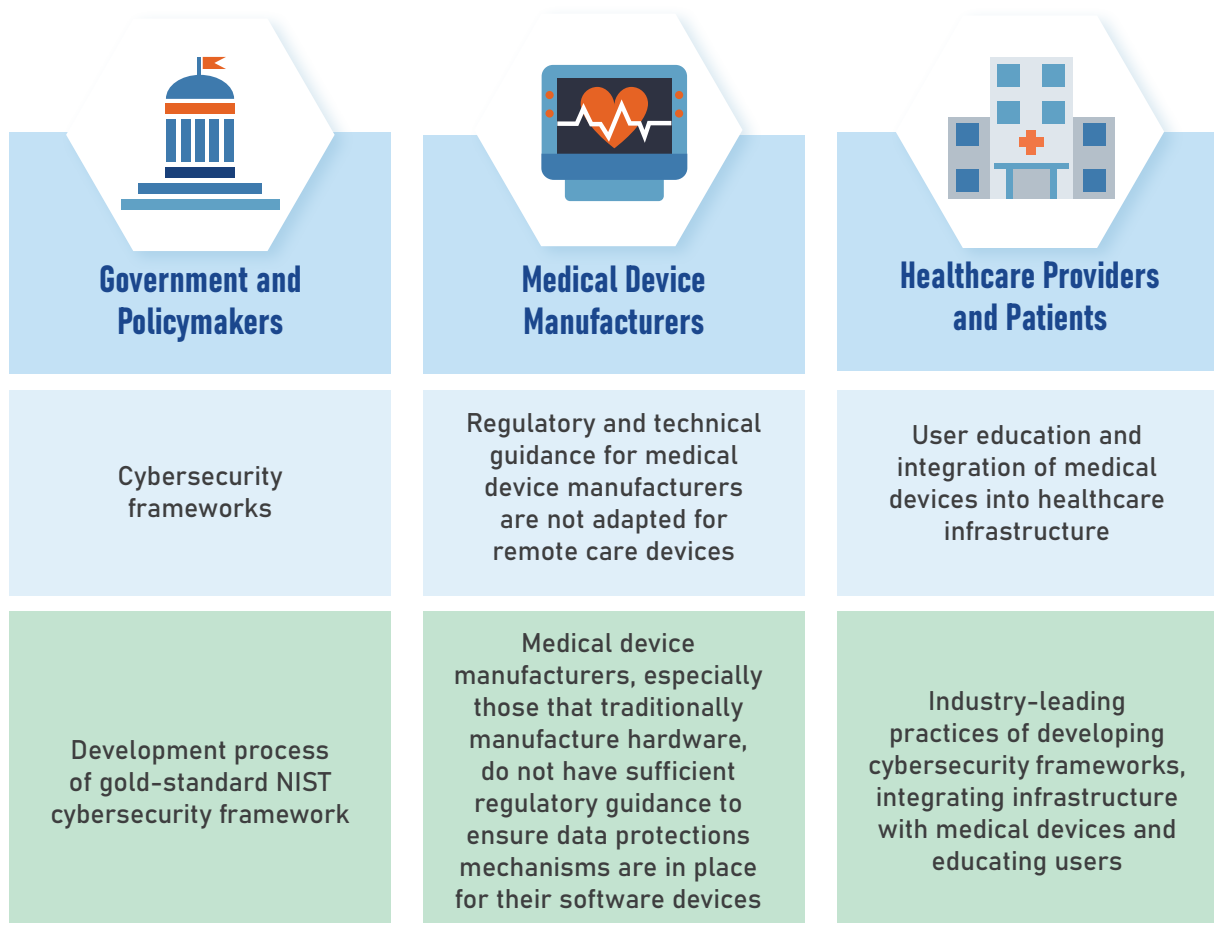
On the user education and compliance front, due to limited framework guidance, healthcare providers are yet to adopt comprehensive processes and training to ensure secure data handling during the provision of remote care services. Furthermore, patients are not fully informed and aware of the significance of patient privacy. These factors collectively highlight the need for enhanced efforts to address these challenges and prioritize cybersecurity within the healthcare sector.

05. Learning from Global Good Practices

5.1 Key Global Countries Benchmarking

Given the challenges discussed above, it is crucial to explore solutions and learn from approaches adopted in other regions to address these issues effectively. In response to the diverse stakeholders involved, we observe the following good practices (See Figure 14).

Figure 14. RCM Best Practices from Key Global Countries

Government and Policymakers	Medical Device Manufacturers	Healthcare Providers and Patients
Cybersecurity frameworks	Regulatory and technical guidance for medical device manufacturers are not adapted for remote care devices	User education and integration of medical devices into healthcare infrastructure
Development process of gold-standard NIST cybersecurity framework	Medical device manufacturers, especially those that traditionally manufacture hardware, do not have sufficient regulatory guidance to ensure data protections mechanisms are in place for their software devices	Industry-leading practices of developing cybersecurity frameworks, integrating infrastructure with medical devices and educating users

Source: L.E.K. interview and analysis

5.2 Best Practices by Stakeholders

Government and Policymakers

The NIST Cybersecurity Framework (NIST CSF, outlined in Figure 15) is widely regarded as the industry gold standard for developing robust cybersecurity programs and serves as the pioneering regulation for data cybersecurity. Its framework encompasses a comprehensive set of measures and protocols that address the collection, processing, and management of health data, as well as data governance across critical assets.

Figure 15. NIST Framework and Key Contents

1	**Executive Order 13636, Feb 2013**	**Key activities:** The Executive Order established initiatives to share cyberthreat information and to develop a framework of existing and proven ways for lowering cyberthreats to critical infrastructure **Impact:** NIST was tasked with developing a "Cybersecurity Framework" as a result of this Presidential Order
2	**RFI, Feb 2013**	**Key activities:** The primary objectives for the initial RFI was to collect lessons learned from industry by understanding which standards were being used, and how effective these standards were in improving cybersecurity across industries **Impact:** NIST collected approximately 270 RFI answers and reviewed them to create the agenda for the 2nd Cybersecurity Framework session
3	**1st–5th Cybersecurity Framework Workshop, Apr-Nov 2013**	**Key activities:** The goals of these seminars were to generate industry interest, create knowledge of the framework project and give insight into the collaborative Framework development process **Impact:** NIST reviewed the material given and created summary papers explaining their workshop takeaways. The summaries were then sent to industry and used to construct the Provisional Cybersecurity Framework
4	**Preliminary drafts, Feb-Aug 2013**	**Key activities:** The Preliminary drafts incorporated feedback from the initial RFI and earlier workshops **Impact:** These remarks had a significant impact on the release of the Framework version 1.0
5	**Framework 1.0 Publication, Feb 2014**	**Key activities:** The Framework for Enhancing Critical Infrastructure Cybersecurity, version 1.0, was issued by NIST. The Framework contains feedback from over 3,000 workshop participants as well as 15,000 comments received throughout its development **Impact:** While the introduction of Framework v1.0 was an important milestone, NIST did not cease collaborating with industry afterward. In the United States, NIST compliance is enforced under the Federal Information Security Management Act (FISMA)

Source: NIST[26] [27], L.E.K. interview and analysis

Key Contents of
NIST CSF

Measures and Protocols

1. **Program for Integrated Risk Management**

2. **Protocol for incident reaction and mitigating measures**

3. **Cybersecurity regulations for suppliers and enforcement measures**

4. **Solutions for cyber security and their applicability**

5. **Encourages competitiveness and innovation**

Framework Coverage
1. Protocols for collecting, processing, and managing health data
2. Data governance across critical assets

Beyond NIST, policymakers, industry players and healthcare providers can reference a myriad of other security frameworks (See Figure 16) including FDA premarket guidance, NIS2, GDPR, HITRUST CSF, ISO27001 and HIPAA. Firms globally value the NIST and HITRUST Cybersecurity Frameworks most highly[28]; convergence on these frameworks by APAC regulators would facilitate rapid adoption and scaling of RCM solutions.

Figure 16. Other Security Frameworks and Corresponding Details

NAME	COUNTRY COVERAGE	LAUNCH DATE	DETAILS	COMPLIANCE MECHANISMS/ PENALTIES	EVOLUTION RELATED TO REMOTE CARE
NIS2	European Union	2023	Addresses the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements	Administrative fines for certain breaches of up to EUR 10M or 2% of total worldwide turnover (whichever is higher)	NIS2 caters to broader healthcare entities including MedTech manufacturers of wearable devices, telehealth solutions, in silico medicine, etc. NIS2 requests organizations to execute and oversee the implementation of the risk management measures
FDA Premarket Submissions Guidance	United States	2022	Emphasizes the importance of ensuring that devices are designed securely and enables emerging cybersecurity risks to be mitigated throughout the Total Product Life Cycle	A penalty not to exceed $15,000 for each such violation, and not to exceed $1,000,000 for all such violations adjudicated in a single proceeding	FDA requests manufacturers to: · Demonstrate they have a cybersecurity plan · Execute vulnerability scanning on a regular basis · Submit a Software Bill of Materials (SBOM) accounting for SOUP (Software of Unknown Provenance) and other third-party software
General Data Protection Regulation (GDPR)	Imposes requirements on organizations worldwide if they gather data on European citizens	2016	GDPR was created to harmonise data privacy legislation across all of Europe's member nations and to highlight the Europe's strong position on data privacy and security	There are two levels of sanctions, with a maximum fine of €20 million or 4% of worldwide turnover (whichever is greater), and data subjects have the right to seek compensation for damages	Given the exponential data collected due to remote care, GDPR is expected to launch new codes of conduct for sensitive categories of data (health and scientific research)
HITRUST Common Security Framework (CSF)	Internationally certified program that can be tailored to various companies	2009	Support healthcare businesses and their cloud service providers in showing their cybersecurity protections and compliance	Not mandatory for organizations; However, every entity that creates, and accesses personal health information should achieve HITRUST compliance in order to explicitly show compliance with industry requirements such as HIPAA	HITRUST accreditation can be leveraged to confirm that the organizations' administrative, operational, and technological safeguards for telemedicine cybersecurity have been applied
Health Insurance Portability and Accountability Act (HIPAA)	United States	1996	Aims to identify and limit the conditions under which covered entities may use or disclose an individual's healthcare information	Penalties range from USD $100 to $50,000+ per violation, with a Calendar Year Cap of USD $1,500,000	According to telemedicine guidelines within HIPAA: · only authorized individuals should have access to ePHI · to ensure the integrity of ePHI, a secure communication mechanism should be created · to avoid breaches, an ePHI-containing system should be built

Source: NIS2[29 30 31], FDA[32 33 34], GDPR[35], CSF[36], HIPAA[37], L.E.K. interview and analysis
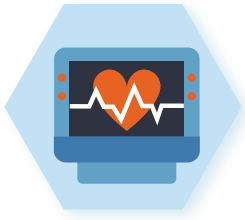
Medical Device Manufacturers

Under the scopes of the frameworks, there have already been cases of healthcare companies effectively addressing the security and compliance of hardware, software and employee touchpoints. For instance, within the scope of HIPAA regulations, medical device manufacturers are required to incorporate safeguards for sensitive information across their hardware (i.e., classify sensitive data based on data protection legislation such as GDPR and HIPAA and use Data Loss Prevention technologies to protect sensitive data from being shared or kept locally on work PCs), software (i.e., ensure operating software is updated and seek cross–platform cyber solutions for multi–operating software environments) and organization (i.e., cybersecurity training for employees).

Healthcare providers must establish protocols to safeguard patient information, restrict access to health data, and assume responsibility for data protection and enforcement of security standards. These measures ensure the integrity and privacy of healthcare data throughout the ecosystem.
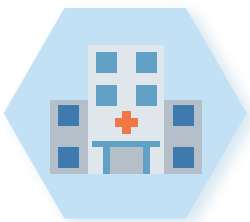
Healthcare Providers and Patients

Queensland Health and Mayo Clinic are recognized as frontrunners in developing industry–leading practices for developing robust cybersecurity frameworks, infrastructure integration and user education.

Queensland Health mandates that all external connections must be configured to the network through their designated vendor Virtual Private Network (VPN) services gateway. Additionally, a named account is required to be tagged for each external party to facilitate tracking and monitoring. Additional security setup is available for staff to securely work remotely with their own devices via their own health digital platform. Compulsory security training are given to all the health staff to prevent data leakage.

Mayo Clinic has continuously invested in research and development (R&D), by researching the potential of Quantum Computing for cybersecurity. For example, a medical device cybersecurity audit process was established as a part of infrastructure integration, which require medical devices to comply and integrate to Mayo Clinic's security criteria and infrastructure along with security issues tracking and sanitization.

06. Recommendations and Initiatives for RCM Cybersecurity

This paper provides recommendations that are based on 3 general aspects across key stakeholders, (1) Governments and policymakers forming a APAC-recognized cybersecurity regulatory framework, (2) Medical device manufacturers ensure RCM devices meet cybersecurity standards established by policymakers, and (3) Healthcare providers ensuring secure operation and control infrastructures in medical institutions.

6.1 Near Term Recommendations

Government and Policymakers

1

RCM cybersecurity policies should ensure approved RCM medical devices are secure in terms of data protection and privacy. Regulators should ensure that RCM cybersecurity policies promote a sufficiently diverse and innovative portfolio of RCM solutions in the market. To achieve that, RCM cybersecurity policies should be developed based on the following guiding principles:

Policymakers should enhance existing cybersecurity frameworks to support RCM solutions by **localizing existing local and global frameworks** based on existing national remote care environments. Further, new frameworks should not deviate significantly from current industry standards followed such as NIST Cybersecurity framework, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA).

This will ensure that new RCM cybersecurity policies proposed are consistent with globally approved standards that have been adopted across the medical device industry. This supports rapid availability of global solutions that can deliver value in local markets, as well as offering local developers the opportunity to scale rapidly outside their home markets.

Potential regulatory enhancements include introducing an integrated risk management program, incidence response protocol and mitigation measures, supplier cybersecurity requirements and enforcement measures to promote device security and competition.

2 Policymakers should ensure that the frameworks are recognized across APAC jurisdictions and translate the cybersecurity regulatory framework into **clear technical requirements** for stakeholders (i.e., manufacturers and healthcare providers) and establish consistent, transparent compliance and enforcement mechanisms. These technical requirements can be iteratively updated as policymakers collaborate with associations that bridge medical device manufacturers / healthcare providers and policymakers to incorporate the latest global developments of RCM cybersecurity management from manufacturers and healthcare providers.

3 Policymakers should ensure assessment for each RCM medical device is customized based on their individual risk level (i.e., rather than applying a blanket assessment process). Hence, for each RCM medical device, policymakers should identify data collected, classify types of data collected (e.g., based on HIPAA classification) and develop customized risk management strategies (i.e., incidence response protocol) for each type of health data. For example, RCM medical devices connected to a network are at higher risk of data leakage compared to medical devices that are not connected to a network. Hence, for medical devices with lower risk levels, less stringent assessment processes can be applied to ensure sufficient innovation and competition in the RCM medical device market.

Medical Device Manufacturers

With RCM-specific frameworks established, medical device manufacturers should aim to implement technical measures following the cybersecurity framework, ensuring their RCM solutions attain regulatory approval and enter markets efficiently.

1 Medical device manufacturers need to ensure their RCM solutions meet regulatory guidance for RCM hardware protection such as classifying data collected and ensuring they are processed and stored compliant to national guidelines. Further, medical device manufacturers have to ensure their RCM solutions' software is sufficiently guarded against cyber threats such as checking if the RCM solutions' operating system for medical devices is consistently updated and protected by cybersecurity software.

2

Medical device manufacturers can also establish specific accountabilities to manage breach incidents and reduce future risks. There should be proactive collaboration with clients (i.e., hospital providers) and external vendors to ensure confidential information is secured. For example, medical device manufacturers can conduct regular audits to ensure the applicability and enforcement of frameworks.

3

Medical device manufacturers should also educate employees to build an organizational culture to ensure cybersecurity. For example, medical device manufacturers can schedule routine training on updated measures as a result of software / technology evolution.
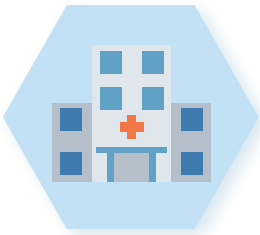
Healthcare Providers and Patients

Once more RCM-specific regulatory guidance is provided and as more RCM solutions are connected through the hospitals' hardware and software environment, healthcare providers' IT departments have to maintain a secure architecture. For example, the information technology (IT) departments can establish a systematic security operation system, including the ability to identify, detect, and recover from cyberthreats.

Further, as most RCM solutions' software are linked to external vendors, healthcare providers have to ensure the safe integration of hospital infrastructure with medical devices. For example, healthcare providers can convince medical device manufacturers and 3rd party software providers of financial and social benefits to ensure safe integration into hospital system when launching remote care solutions.

Last, healthcare providers can organize internal data security training for healthcare staff and patients to follow cybersecurity protocol and their role to minimize the risk of cyberthreat.

# 6.2 Longer-Term Recommendations
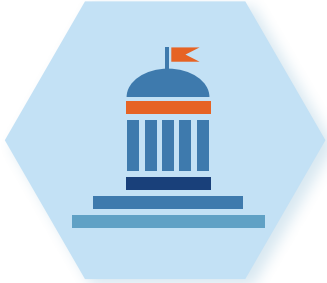
Government and Policymakers

As cybersecurity threats constantly evolve, policymakers should actively engage with other nations' policymakers as well as industry experts to refine RCM cybersecurity frameworks against latest cybersecurity developments.Governments should actively fund partnerships across healthcare providers and manufacturers (e.g., Funding support by Cyber Security Agency (SG) to develop cybersecurity health strategy).

Medical Device Manufacturers

As cyber threat increases for remote care, data security is growing in importance for product differentiation and customer acquisition. Hence, medical device manufacturers can consider investing in smart technologies such as for hardware protection (i.e., AI-powered network firewall to detect and prevent threats actively) and software protection (i.e., secure software architecture, storage of sensitive data following secure coding guidelines, property management of 3rd party libraries, secure default settings and anti-malware endpoint protection).
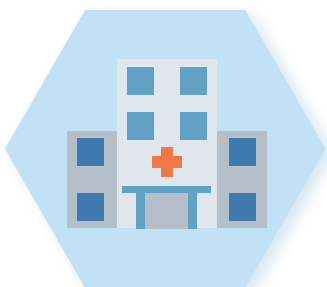
Healthcare Providers and Patients

As patients are increasingly seeking remote care, healthcare providers can differentiate themselves by offering RCM solutions (i.e., remote surgery, telehealth) that are secure and cost-efficient. For example, hospitals can invest into machine identity management where each connected device is tagged with a unique identity and hospitals can validate the integrity of each device.

07. Conclusion

Across APAC, the healthcare ecosystem is already seeing the significant benefits of RCM and is integrating this into a wider range of healthcare delivery settings and care pathways. Looking ahead, to safeguard the healthcare system and the wider population, appropriate cybersecurity measures are needed that enable trust from all participants in the healthcare ecosystem, while enabling widespread delivery of RCM and its benefits.

The recommendations proposed here are a stepping stone towards appropriate RCM cybersecurity in the APAC region. Given the dynamism of RCM innovation, these RCM cybersecurity policies will need to be updated based on new market innovations and patient needs.
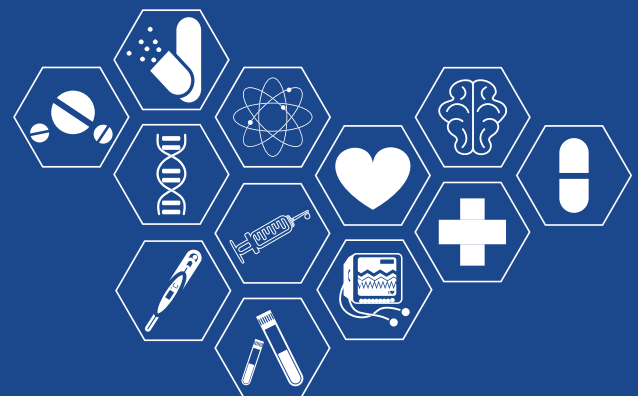
08. References

[1] TBRC. (2022). Asia-Pacific Digital Health Market Report 2022.

[2] The World Bank. (2023). Rural population.

[3] CNBC. (2023). Southeast Asia's digital economy may be set to hit $1 trillion, but roadblocks remain.

[4] Pioneer Consulting Asia Pacific (2022). Telemedicine industry forecasts for key Asian markets: Indonesia, Malaysia, Singapore & Thailand.

[5] Centers for Disease Control and Prevention. 2022. Telemedicine Use Among Adults: United States, 2021.

[6] GSMA. (2023). Mobile Economy APAC 2023 Report.

[7] Oxford Economics. (2021). Asia Pacific Cities and Regions Outlook.

[8] L.E.K. Consulting, (2023). L.E.K. Consulting 2023 APAC Hospital Survey.

[9] MobiHealthNews. (2019). Indonesia's healthcare superapp Alodokter raises $33M in Series C funding

[10] Jurnal Rekam Medis dan Informasi Kesehatan Indonesia. (2021). Analisis trend jumlah kunjungan pasien saat pandemi dengan metode trend kuadrat terkecil di Rumah Sakit Pantiwilasa dr.Cipto Semarang

[11] Ministry of Health Singapore. (2019). Unauthorised possession and disclosure of information from HIV registry.

[12] Bangkok Post. (2022). Claim on huge patient data leak.

[13] DLA Piper. (2023). Telehealth and cybersecurity regulations by country.

[14] Didomi. (2023). Japan data protection law (APPI).

[15] ICLG. (2023). Data Protection Laws and Regulations Japan 2023.

[16] Thomson Reuters. (2022). Data Localization Laws: Japan.

[17] InCountry. (2022). Data Protection Laws and Compliance in China for Healthcare Industry.

[18] Skadden. (2021). China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies.

[19] DataGuidance. (2023). South Korea - Data Protection Overview.

[20] Baker McKenzie. (2022). Global Data Privacy & Security Handbook South Korea.

[21] Chambers and Partners. (2023). Data Protection & Privacy 2023.

[22] Baker McKenzie. (2022). Global Data Privacy & Security Handbook Australia.

[23] PDPC. (2017). Advisory guidelines on key concepts in the PDPA.

[24] Mint. (2022). Cross-border transfers and data localization under the Data Protection Bill 2021.

[25] Economic Times. (2022). Manipal Hospitals partners with Google Cloud.

[26] NIST. (2023). Cybersecurity Framework.

[27] NIST. (2022). NIST Updates Guidance for Health Care Cybersecurity.

[28] Healthcare Finance. (2023). Almost 80% of healthcare organizations experienced cyber incidents in the past year.

[29] European Parliament. (2023). The NIS2 Directive: A high common level of cybersecurity in the EU.

[30] Mayer Brown. (2022). NIS2 Directive New Cybersecurity Rules Expected in the EU.

[31] FieldFisher. (2023). The NIS 2 Directive – implications for the healthcare sector and manufacturers of medical devices.

[32] US FDA. (2022). Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.

[33] Ankura Consulting Group. (2023). FDA Authorized to Establish New Cybersecurity Standards for Medical Devices: What it Means for Industry.

[34] MedCity. (2023). How Can Medtechs Prepare for the FDA's Shift Left Strategy on Cybersecurity.

[35] GDPR. (2023). What is GDPR, the EU's new data protection law?

[36] HITRUST. (2008). HITRUST Confirms Release Date for First-Ever Common Security Framework for Electronic Health Information.

[37] University of Northern Colorado. (2022). Summary of HIPAA Privacy Rule.

09. Acknowledgements

Experts Interviewed

Devan Tay, Assistant Director, Cyber Defence Group, **Synapxe Pte. Ltd.**

Shan Xu, Vice Chair, ITU & WHO AI for Health Focus Group; Head, WHO Collaborating Centre for Digital Health (CHN-147), **World Health Organization**

Authors and Contributors

APACMed Cybersecurity Working Group:

Jim Sarka, CIO & Vice President, Technology – Asia Pacific, **Johnson & Johnson MedTech.**

Paul Chua, Product Security Officer, Greater Asia, **BD**

Thomas Harding, Head of Public Affairs, Asia Pacific, Japan & India, **Varian**

Stefan Gentsch, Regional CISO and Cybersecurity Advisor, **Siemens Healthineers**

Neha Sethi Manchanda, Specialist, Regulatory Affairs, **ResMed**

Yeow Kee Tay, Director, Digital Customer Solution & Services, Asia Pacific, **B. Braun**

Stephen Sunderland, Head of APAC, **L.E.K Consulting**

Wonder Wang, Senior Consultant, **L.E.K Consulting**

Jocelyn Hiranyajinda, Associate, **L.E.K Consulting**

Anirudh Sen, Director, Digital Health, APAC, **APACMed**

Birgitta Riani, Assistant Manager, Digital Health, **APACMed**

The voice of MedTech

The Asia Pacific Medical Technology Association (APACMed) represents manufacturers and suppliers of medical equipment, devices and in vitro diagnostics, industry associations, and other key stakeholders associated with the medical technology industry in the Asia Pacific region. APACMed's mission is to improve the standards of care for patients through innovative collaborations among stakeholders to jointly shape the future of healthcare in Asia-Pacific. In 2020, APACMed established a Digital Health Committee to support its members in addressing regional challenges in digital health. For more information, visit: www.apacmed.org

"Asia Pacific" means the countries and/or economies in the Asia Pacific region, namely: Australia, Bangladesh, Bhutan, Cambodia, DPR Korea, Hong Kong (China), Independent State of Papua New Guinea, India, Indonesia, Japan, Lao People's Democratic Republic, Macau (China), Malaysia, Mongolia, Myanmar, Negara Brunei Darussalam, Nepal, New Zealand, Pacific Islands, Pakistan, People's Republic of China, Chinese Taipei, Philippines, Singapore, South Korea, Sri Lanka, Thailand, Timor Leste, Vietnam;

L.E.K. Consulting is a global management consulting firm that uses deep industry expertise and rigorous analysis to help business leaders achieve practical results with real impact. We are uncompromising in our approach to helping clients consistently make better decisions, deliver improved business performance and create greater shareholder returns. The firm advises and supports global companies that are leaders in their industries — including the largest private- and public sector organizations, private equity firms, and emerging entrepreneurial businesses. Founded in 1983, L.E.K. employs more than 1,600 professionals across the Americas, Asia-Pacific and Europe. For more information, go to www.lek.com