APACMed
The voice of MedTech

MEDTECH'S DATA AGE

EMBRACING OPEN DATA FLOWS FOR INNOVATION AND PATIENT CARE IN APAC

HEALTH DATA

KNOWLEDGE PARTNER

Access Partnership

Access Partnership

Access Partnership works with businesses, governments, and multilateral institutions to unlock new markets, drive commercial success, and create solutions that advance humanity. Our multidisciplinary team includes geopolitical analysts, regulatory specialists, and communications strategists, as well as economists, engineers, physicians, and scientists. We help ambitious organisations turn ideas into real-world outcomes quickly and decisively. Whether you're expanding into new markets, launching new solutions, or tackling global challenges, we combine commercial insight, public-policy and regulatory analysis, and deep networks to help you move with confidence and clarity. Find out more at accesspartnership.com.

CONTENTS

EXECUTIVE SUMMARY

Today's healthcare landscape is shaped by an unprecedented surge in data generation across various jurisdictions, with MedTech innovations driving better patient care and medical science. Cross-border data flows are crucial for innovation, research, and public health, as demonstrated during the COVID-19 pandemic. The management of cross-border data is a crucial aspect of economic development, contributing to progress towards the United Nations (UN) Sustainable Development Goals (SDGs).

However, sector-specific data localisation and cross-border data transfer regulations create complexities for the MedTech industry. Governments have updated their data protection frameworks to protect personal information and facilitate regulatory oversight over critical data, mandating local storage and restricting transfers in some instances. These regulations can complicate healthcare provision for patients who access services across multiple jurisdictions, hinder vital cross-border medical research, and increase capital costs for companies. They also limit the utility of advanced cloud-based and Artificial Intelligence (AI) services, which often rely on data transfer for training and processing.

This white paper captures the evolving regulatory landscape and its impacts on MedTech industry players, synthesising findings from the global literature and interviews with multidisciplinary public and private sector stakeholders. Asia-Pacific (APAC) countries exhibit a diverse array of regulatory approaches, with MedTech industry players facing a combination of general data protection regulations, health and medical device data regulations, and, increasingly, regulations on the use of AI. The research suggests that shifting away from restrictive data policies would enhance patient access, unleash innovation, and improve operational efficiencies.

The MedTech industry aims to create a policy environment that promotes secure and governed cross-border data flows and establishes robust mechanisms for the safe and effective use of health and medical device data. This is founded on three key recommendations:

- **Designing fit-for-purpose data regulations**
  We must adopt a risk-based approach to regulation and prioritise robust technical and contractual safeguards to achieve privacy and security, rather than relying on strict data localisation mandates. Regulations should be transparent, non-discriminatory, no more restrictive than necessary, aligned with international best practices, and flexible enough to accommodate future technological advancements.

- **Increasing engagement and collaboration**
  We recommend establishing regular channels for dialogue between data regulators, healthcare agencies, and the MedTech industry to ensure that data regulations account for sector-specific needs. Collaboration should focus on developing and adopting secure mechanisms and common frameworks to enable trusted and seamless cross-border data transfers. Examples include the European Health Data Space (EHDS) and Fast Healthcare Interoperability Resources (FHIR) standards.

- **Promoting best practices in technology and data governance**
  Policymakers should signal acceptance of privacy-enhancing technologies (PETs) to support business adoption. PETs such as anonymisation and pseudonymisation can reduce data sensitivity, enabling broader utility for research and innovation while upholding privacy. A cloud-first approach to healthcare also holds potential to enhance security, reduce costs, and improve data interoperability within the MedTech ecosystem.

Ultimately, health and medical device data should be seen as a strategic regional and global asset that, when shared responsibly, can improve public health and drive economic growth. Although domestic considerations have historically dominated healthcare data governance, the increasing cross-border nature of health and medical device data necessitates a fundamental shift in mindset to view healthcare and MedTech as a global collaborative effort. We invite continued dialogue among industry, technology providers, and governments to navigate this transformative journey.

1 THE EVOLVING LANDSCAPE OF DATA REGULATION IN MEDTECH

The MedTech industry is awash in a data explosion. The healthcare sector now generates 30 per cent of the world's entire data volume[1], much of it attributable to medical technology (MedTech)[2], such as medical devices, equipment, and in vitro diagnostics. MedTech innovations are present throughout the entire lifecycle, across prevention, diagnosis, treatment, and management[3], and are powerful data engines, especially as software is increasingly embedded in these technologies. They continuously generate diverse types of information vital for patient care, operational efficiency, and innovation. The World Health Organization (WHO) estimates that about 2 million types of medical devices are available globally, each generating data through interactions with healthcare facilities and digital applications.[4]

Healthcare data can be categorised into four groups based on how they are collected: device-generated data, medical records, administrative data (primary care, hospital, ancillary, and pharmacy records), and survey and registry data.[5] Besides generating data through medical devices, the MedTech industry, including medical device manufacturers, digital health start-ups, and healthcare information system providers, also accesses, processes, and exchanges data from the other three sources as part of the normal course of operations.[6]

Therefore, this whitepaper will use the term "health and medical device data" to refer to all data relevant to the MedTech industry. It also recognises that this definition does not preclude other classifications of healthcare data – for instance, demographic, medical, consumer-generated, financial, environmental, and research data.[7]

1. RBC Capital Markets (n.d.), "The healthcare data explosion". Available at: https://www.rbccm.com/en/gib/healthcare/episode/the_healthcare_data_explosion#content-panel
2. Medical technologies can be defined as the technologies that diagnose, treat and/or improve a person's health and wellbeing. Examples of medical technologies are wide ranging and very diverse: from contact lenses to rubber gloves, syringes, and needles. From pacemakers, CT's and MRI's, surgical robots and laboratory analysers to artificial hip and knee implants. And from insulin pumps and dialysis machines to pregnancy tests, catheters and wheelchairs. APACMed (2020), MedTech in APAC: Improving Health, Transforming Lives. Available at: https://apacmed.org/wp-content/uploads/2020/12/MedTech-in-APAC-Improving-Health-Transforming-Lives.pdf
3. APACMed (2020), MedTech in APAC: Improving Health, Transforming Lives. Available at: https://apacmed.org/wp-content/uploads/2020/12/MedTech-in-APAC-Improving-Health-Transforming-Lives.pdf
4. MedTech Europe (2022), "The journey of health data in medical technologies". Available at: https://www.medtecheurope.org/resource-library/the-journey-of-health-data-in-medical-technologies/
5. Ghoneimy et al (2019), "A Framework for Social Network-Based Dynamic Modeling and Prediction of Communicable Diseases". Available at: https://www.researchgate.net/publication/332965162_A_Framework_for_Social_Network-Based_Dynamic_Modeling_and_Prediction_of_Communicable_Diseases#pf3
6. Datasets from these sources may be leveraged for patient-level purposes (e.g., disease prediction, comorbidity analysis), provider-level purposes (e.g., physician collaboration, hospital coordination) and policy-level purposes (e.g., cost reduction, performance monitoring).
7. NUS Saw Swee Hock School of Public Health and Precision Public Health Asia Society (2022), White Paper: Responsible Data Sharing in Health and Healthcare. Available at: https://cens.-cl/wp-content/uploads/2022/08/pub-responsible-data-sharing-in-health-and-healthcare.pdf

The MedTech industry generates and uses data with varying sensitivity (Figure 1). Suppliers, manufacturers, and users of medical technologies generate machine and operational data on products, treatments, and procedures. This data is generally less sensitive but offers valuable insights into health and commercial aspects, ranging from understanding treatment efficacy across populations to quantifying market shifts that inform research and product development.[8] Personally identifiable health data comes from a variety of sources. Software as medical devices (SaMDs)[9], such as apps that monitor heart conditions or support dosing decisions, generate patient data in home-use settings.[10] Diagnostic imaging devices, such as MRI machines, produce patient-level data that feed into electronic health records (EHRs)[11] and disease or device registries. Clinical trials are another source of personally identifiable health data. Specific categories – such as genetic data, biometric data, body images, and sensitive diagnoses – are considered highly sensitive due to their risk of re-identification and the high impact of loss.[12]

FIGURE 1 DATA SENSITIVITY CLASSIFICATION AND EXAMPLES

DATA SENSITIVITY CLASSIFICATION	HEALTH AND MEDICAL DEVICE DATA EXAMPLES (NON-EXHAUSTIVE)
LOW SENSITIVITY	• Data not related to any human being • Recordings of human/machine interaction • Anonymised or pseudonymised data
MEDIUM SENSITIVITY	• Individual identifiers and reference data – purchasing habits, income, social class, address, opinions, facial images, sex, age, race, ethnic group, occupation, wellness, and lifestyle data
HIGH SENSITIVITY	• Clinical trials, medical and lab reports, discharge summaries, billing and reimbursement claims • Body images, biometrics, genetic and genomic data • Highly sensitive diagnoses (e.g., pregnancy, HIV, mental disorders). • Device security parameters (e.g., cryptographic keys, digital certificates, access control lists, authentication tokens, login credentials, etc.)

Adapted from Ministry of Health, Singapore (2023)[13], Global Digital Health Partnership (2024)[14], Rumbold (2018)[15]

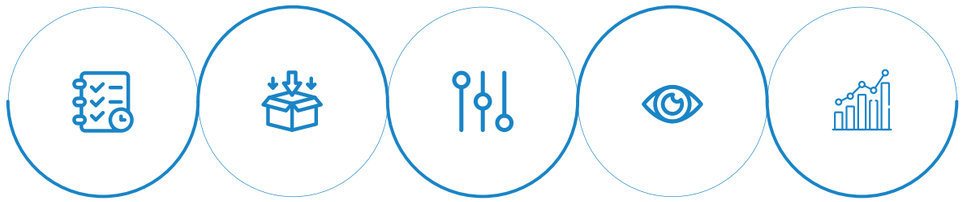
Various techniques, such as anonymisation and pseudonymisation, reduce data sensitivity by lowering the re-identification risk and the impact of data loss. Beyond primary uses such as direct patient care, health and medical device data can also support research, education, and public health, often requiring sharing with universities, pharmaceutical companies, insurers, and other stakeholders.[16] Anonymisation and pseudonymisation are two commonly used privacy-enhancing technologies that reduce the sensitivity of data and facilitate such transfers.

8. IQVIA (2022), "Demystifying data in the MedTech industry". Available at: https://www.iqvia.com/locations/united-states/blogs/2022/02/demystifying-data-in-the-medtech-industry
9. Software designed for one or more medical purposes that performs said functions without being part of a hardware medical device
10. U.S. Food and Drug Administration (FDA) (2021), Clinical Decision Support Software. Available at: https://www.fda.gov/media/152503/download
11. Including different types of patient-level variables: demographics, vital signs, patient history, laboratory results, diagnoses, treatments, therapies. Kim et al. (2019), "Data Management in Healthcare". Available at: https://www.ncbi.nlm.nih.gov/books/NBK551878/
12. There is no globally accepted classification of healthcare data sensitivity levels, however, there have been attempts to do so. See Rumbold (2018), "What Are Data? A Categorization of the Data Sensitivity Spectrum". Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214579617302010
13. Ministry of Health (2023), Cyber and data security guidelines for healthcare providers. Available at: https://www.healthinfo.gov.sg/files/MOH_Cir_No_85_2023_04-Dec2023_Cyber_and_Data_Security_Guidelines_for_Healthcare_Providers_Annex_A.pdf
14. Global Digital Health Partnership (2024), Guidance for Medical Device Cybersecurity (GMDC). Available at: https://gdhp.health/wp-content/uploads/2024/10/GDHP-Guidance-for-Medical-Device-Cybersecurity_final.pdf
15. Rumbold (2018), "What Are Data? A Categorization of the Data Sensitivity Spectrum". Available at: https://www.sciencedirect.com/science/article/abs/pii/S2214579617302010
16. Chang, T. and Chen, P. (2024), "Data Governance Framework for Healthcare Data: A Systematic Review". Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC10963197/

1.1
Considerations for data localisation and cross-border transfer restrictions for MedTech

As data is generated, localisation and cross-border transfer restrictions affect the five stages of data lifecycle management (Figure 2), especially collection, processing, and sharing.

FIGURE 2 DATA LIFECYCLE MANAGEMENT



PLANNING	COLLECTION	PROCESSING	SHARING	ANALYSIS
SETTING THE MISSION, AGENDA, AND STAKEHOLDER ANALYSIS OF DATA USE AND REUSE FOR AN INITIATIVE	GATHERING AND STORING DATA FROM RELEVANT SOURCES, SUCH AS HEALTH RECORDS, REGISTRIES, MACHINES, BUSINESS OPERATIONS	REMOVING IRRELEVANT AND INACCURATE INFORMATION, STANDARDISING CONTENTS FOR SOFTWARE, DE-SENSITISING DATA	PROVIDING ACCESS TO DATA WITH RELEVANT COLLABORATORS FOR INSIGHTS, INCLUDING CROSS-BORDER TRANSFERS	ASSESSING DATA TO EXTRACT INSIGHTS AND RE-SHARE PROCESSED DATA AND INSIGHTS AMONG PARTIES

Adapted from TheGovLab [17]

As more data crosses international borders, concerns have amplified across three main areas: privacy and security, digital sovereignty, and national interest. These concerns have driven regulations that restrict or prohibit cross-border data transfers ("flow restrictions") and localisation measures that require domestic storage or processing ("data localisation").

17. United Nations System Chief Executives Board for Coordination (2023), Annex 1 - Mapping and Comparing Data Governance Frameworks. Available at: https://unsceb.org/sites/default/files/2023-05/Annex%201%20-%20Mapping%20and%20Comparing%20Data%20Governance%20Frameworks.pdf

First, given the variance in regulatory regimes around the world, regulators are concerned that data stored abroad may not receive adequate privacy and security protection. Personally identifiable information is a key focus due to its sensitivity and the rising risk of cyberattacks and biowarfare. Second, localisation and transfer restrictions may also aim to secure access for regulatory oversight or preserve policy powers. In this regard, some regulations also attempt to exert an extra-territorial reach beyond a country's borders. Third, governments may use data as a form of digital industrial policy to build domestic capacity in digitally intensive sectors, treating it as a resource to be prioritised for domestic firms.

However, evidence shows that security and privacy in healthcare systems are best achieved through robust technical safeguards, not physical location requirements. Modern cloud architectures enhance security through distributed systems that ensure continuous operations even during regional disruptions. Leading healthcare organisations report incident recovery times under 30 seconds while maintaining complete control of patient data through sophisticated encryption and access controls.

FIGURE 3 DATA RESIDENCY, DATA SOVEREIGNTY, AND DATA LOCALISATION

Data residency, data sovereignty, and data localisation hold different meanings but are often intermingled.[18]

Data residency refers to the physical location where data is stored. Data sovereignty concerns apply local legal rights and protections to data storage and processing. Data localisation requires that some or all data be stored and processed within the country or region where it was collected.

While data localisation can be an extreme form of data sovereignty, it is not synonymous with it.

18. Forcepoint (n.d.), Guide to Data Sovereignty and Localization in the Cloud. Available at: https://www.forcepoint.com/sites/default/files/resources/brochures/guide-data-sovereignty-and-localization-in-the-cloud-en_0.pdf; Scale Computing (n.d.), Data Sovereignty. Available at: https://www.scalecomputing.com/documents/Data-Sheets/SC_Data-Sovereignty_7-23.pdf

1.2
Landscape of data localisation regulations

There are three main categories of data-related regulations that are pertinent to MedTech. The first category includes general data regulations. The second category sets additional expectations for health and medical data, a subset of personal data. The third, an emerging category, regulates the use of AI.

1.2.1
Category 1
General data localisation and transfer regulations

Data localisation requirements are often paired with processing and/or flow restrictions. For instance, some approaches may require that genetic data be stored and processed locally, permitting cross-border transfers only under specific conditions. Thus far, many APAC governments have been content to allow health and medical device data to fall under broader data protection laws, with relatively few specific rules targeting its storage and flow. As mentioned in Figure 1, laws governing personally identifiable information are directly relevant to electronic medical records. Data localisation requirements may also extend to less well-defined data categories such as "important" or "critical" data, and to operators like "critical information infrastructure" or "network" operators.

Countries can be grouped into four broad categories based on requirements for data localisation ("local storage") and cross-border data transfers ("flow restrictions"), as demonstrated in Figure 4. The Excel sheet accompanying this whitepaper contains a more detailed breakdown of each country's policies.

FIGURE 4 RESTRICTIVENESS OF GENERAL DATA LOCALISATION AND TRANSFER REGULATIONS

	Progressive	Mostly Progressive	Partially restrictive	Restrictive
Local storage required?	No	No	Yes For very specific types of data	Yes For a wider range of data
Cross-border data transfers allowed?	Yes	Yes, but limited More stringent requirements	Yes Based on clearly defined conditions	No Ability to restrict transfers
Countries	Philippines Thailand	Australia India Japan	Indonesia Korea Malaysia Singapore	China Vietnam

Source: Access Partnership analysis, literature review

At one end, China has one of the world's most comprehensive data localisation regimes, including the Cybersecurity Law (CSL), Personal Information Protection Law (PIPL), and Data Security Law (DSL). Under the PIPL, health-related personal data is categorised as "sensitive personal information" and is subject to stricter requirements than other data types. That said, recently, regulators have eased cross-border transfer rules by increasing the threshold for the number of data subjects whose non-sensitive personal information is transferred outbound, above which the data will require security evaluation when being transferred out of the country.[19] Vietnam is also closely monitoring and updating its data regulations to be more stringent. Health data is classified as sensitive under Decree 13/2023/ND-CP on personal data protection and must be periodically assessed. Under current law, sensitive data involving 10,000 or more Vietnamese citizens is considered core data, requiring prior filing or approval from the Ministry of Public Security (MPS) before any cross-border transfer. This means new data assets – such as digital apps collecting sensitive user data – must be flagged, as they add to the total volume processed. In June 2025, Vietnam issued the Personal Data Protection Law (PDPL), effective January 2026, which may replace Decree 13. At the other end, the Philippines takes a more progressive approach. The Data Privacy Act of 2012 also classifies health information as sensitive and requires explicit consent except under specific exceptions, but it does not mandate localisation.

1.2.2
Category 2
Health and medical device data regulations

Medical device and health data restrictions have been adopted to a smaller extent in APAC (Figure 5).

FIGURE 5 EXAMPLES OF HEALTH AND MEDICAL DEVICE DATA LOCALISATION REQUIREMENTS AND CROSS-BORDER DATA RESTRICTIONS IN APAC

2012
The Electronic Health Records Act in Australia (2012) requires My Health Record system data to be stored domestically but allows overseas access for data subjects and registered healthcare providers overseas.

2017
Korea's Medical Service Act of 2017 (amended in 2023) created a localisation requirement for the back-up storage of electronic medical records (EMR).[20] China's Population Health Information Measures (2017), which governs health data including basic population information and health service information, stipulates that population health information be stored or hosted in China, with graded safeguards based on sensitivity.

2018
China's Health Care Big Data Measures (2018) mandates that healthcare big data (disease prevention, treatment, and health management data) be stored on servers within the country.

2023
Indonesia's Law No. 17 of 2023 on Health (the Health Law) requires the processing of health data and information to be conducted primarily in Indonesia, with offshore transfers subject to Ministry of Health and presidential approval.

2025
Vietnam's Decree No. 102/2025/ND-CP ("Decree 102") regulates digital medical data, imposing strict consent requirements, extraterritorial scope, and provisions on cross-border transfers and risk assessments.

19. China Law Translate (2024), "Provisions on Promoting and Regulating the Cross-Border Flow of Data". Available at: https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/
20. It states that if electronic medical records (EMR) are managed and stored outside hospitals, the physical location of the EMR system and its backup equipment must be within Korea.

There has also been a trend towards encouraging data sharing at the national level led by governments. Japan enacted the "Next-Generation Medical Infrastructure Law" ("NGMIL") under the Act on the Protection of Personal Information (APPI) to enable anonymised and pseudonymised medical data to be accessed for research, supporting advances in treatment and drug development. Separately, policymakers are also expanding national EHR systems to build healthcare resilience and promote digital health innovation.[21] In India, the government is implementing the Ayushman Bharat Digital Mission to enable interoperability by linking health data systems across public and private providers in both urban and rural areas.[22]

Cross-border data sharing remains limited outside of public health emergencies, though several drivers signal future potential. During COVID-19, governments broadly agreed on cross-border health data sharing, revealing that public health emergencies are a legitimate and sufficiently strong motivator. In the post-pandemic era, demand for remote care management has also encouraged more open flows of cross-border health data.[23] Separately, momentum is growing for anonymisation and encryption through federated data networks. At the same time, harmonised standards, such as Health Level 7 (HL7) and Fast Healthcare Interoperability Resources (FHIR), provide a common language and expectations for interoperability, reducing friction and fostering consensus on health data sharing.

> Data pseudonymisation and anonymisation is crucial for transferring sensitive data outside the country, as it helps with compliance with privacy and cybersecurity regulations.
>
> APAC Privacy Lead for a leading MedTech company

1.2.3
Category 3
Regulations on the use of AI

The growing use of AI in MedTech is exposing tensions between the optimal development of AI and restrictive data regulations. As AI systems scale, they increasingly depend on large cross-border datasets to train models, extract insights, and support decision-making. Global data access is also crucial in reducing bias that can occur when models are trained on limited regional data, as well as to train and adapt models for local populations and needs. Yet, this reliance raises significant concerns regarding data privacy, particularly with respect to personal, sensitive, and proprietary information. From a data governance perspective, patient consent is another hurdle: health data is typically collected for care or research, not AI training, and re-obtaining explicit consent from large patient groups would require disproportionate effort.[24] Addressing these challenges will be essential for regulators to unlock AI's potential in MedTech.

21. Asia House (2023), Asia's Digital Health Innovations. Available at: https://www.asiahouse.org/files/documents/10.11.23_AH_Asias-digital-health-innovations_AW_2.pdf
22. Ibid.
23. APACMed (2023), Cybersecurity White Paper. Available at: https://apacmed.org/wp-content/uploads/2023/10/DIGI-2023_10-RCM-Cybersecurity-White-Paper-2.pdf
24. Sun et al. (2022), "Data Governance for Genomic Data Sharing: A Review". Available at: https://www.frontiersin.org/journals/genetics/articles/10.3389/fgene.2022.929453/full

Furthermore, clear regulatory guidance and support would help MedTech providers and institutions balance innovation with compliance with existing privacy and consent laws relevant to AI. The current focus is on broad privacy laws and AI governance principles, such as transparency, explainability, and auditability; fairness, non-discrimination, and justice; reliability, security, and robustness; and safety.[25] However, more sector-specific considerations are important. For instance, policies around medical device data should be more nuanced, considering technology such as AI and ML are increasingly a part of these medical devices' capabilities. These devices would require cross-border software infrastructure, and further calibration and improvements would require cross border data transfers for localisation and optimisation for local populations. As such, more specific guidance is needed on managing data from Software as a Medical Device (SaMD), Software in a Medical Device (SiMD), and AI as a Medical Device (AIaMD),[26] ensuring flexibility while safeguarding patients. This could take the form of a living one-stop toolkit for navigating AIaMD regulations, harmonisation efforts, and regulatory sandboxes for real-world testing.[27] Governments in APAC are beginning to act: Australia intends to roll out a principles- or list-based approach to define "high-risk AI", while Singapore's Artificial Intelligence in Healthcare Guidelines aim to codify good practice and support the safe growth of AI in healthcare, with clear guidance for developers and implementers.[28]

Healthcare AI development presents unique challenges under strict data localisation requirements. Effective clinical AI systems require access to diverse patient populations, rare disease cases, and global treatment outcomes to ensure accuracy and prevent bias. Recent advances in privacy-preserving computation and federated learning now enable healthcare organisations to maintain complete control over sensitive clinical data while participating in global AI development. The ability of healthcare organisations to leverage global AI to improve patient care while preserving sovereign control over clinical operations suggests that policy frameworks should prioritise secure collaboration over geographic restrictions, which may ultimately compromise both innovation and patient outcomes.

25. Baker McKenzie (2025), AI Governance Principles and Regulatory Landscape. Available at: https://www.bakermckenzie.com/-/media/files/insight/publications/resources/ai-governance-principles-and-regulatory-landscape-june-2025.pdf
26. Synonymous with AI/ML-enabled devices
27. Path (2024), "Artificial intelligence as a medical device regulatory landscape: Current state, key challenges and guidance for partners". Available at: https://media.path.org/documents/AI_-regulatory_landscape_FINAL.pdf
28. Ropes & Gray (2025), "Regulatory Landscape for AI-enabled MedTech in APAC". Available at: https://www.ropesgray.com/en/insights/viewpoints/102k97d/regulatory-landscape-for-ai-enabled-medtech-in-apac

2 THE VALUE OF CROSS-BORDER DATA ACCESS IN MEDTECH

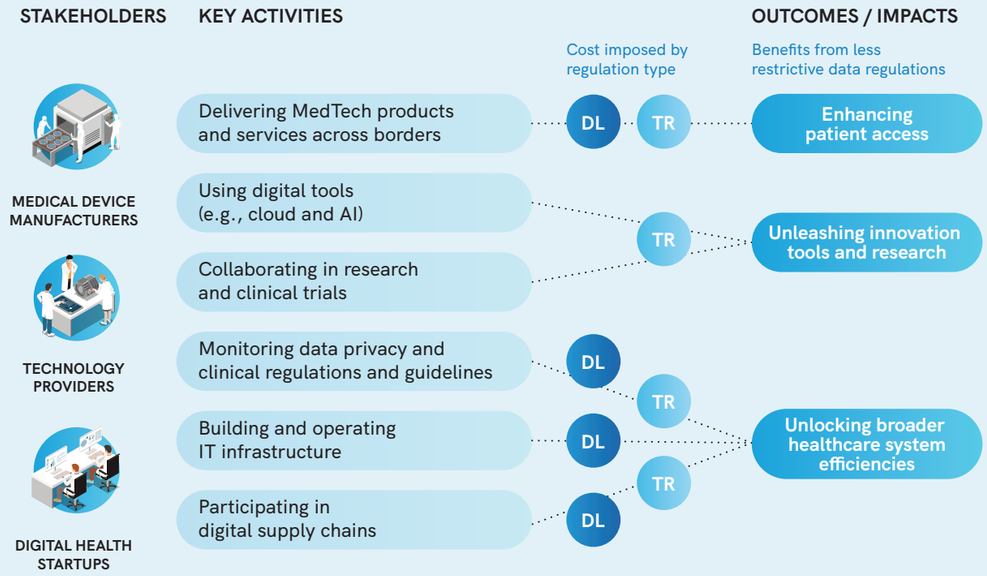
2.1 How open data flows create value

There are significant economic and societal benefits from sharing and reusing data. A recent European Union (EU) study estimated that patient data sharing created USD 11.5 billion[29] in value by enabling 14 per cent more clinical trials and supporting new treatments, lower clinical trial costs, additional research, greater patient access to personal medicine, and higher productivity through efficiency gains and better supply chain coordination.[30] The study further added that removing current barriers to data sharing between the EU and non-EU locations could create an additional USD 5.8 billion annually across the EU27.[31]

MedTech players, including medical device manufacturers, digital health start-ups, and healthcare information system providers, are essential to the integrated healthcare ecosystem, which increasingly relies on the agile and secure flow of data. While data localisation and cross-border transfer restrictions are often well-intentioned, limiting their non-essential use could unlock profound benefits for patient access, innovation, and efficiency. Consultations with industry stakeholders have highlighted three key areas of value if such restrictions are eased (Figure 6): enhancing patient access, unleashing innovative tools and research, and unlocking broader efficiencies within the healthcare system.

29. Converted using the historical exchange rate of EUR to USD of 1.082245 as of December 31, 2023. Available at: https://www.ofx.com/en-sg/forex-news/historical-exchange-rates/yearly-average-rates/
30. Frontier Economics (2023), "Understanding the value of international healthcare data sharing for the EU". Available at: https://www.frontier-economics.com/uk/en/news-and-insights/news/news-article-i20346-understanding-the-value-of-international-healthcare-data-sharing-for-the-eu/
31. Ibid.

FIGURE 6 BENEFITS UNLOCKED THROUGH LESS RESTRICTIVE DATA LOCALISATION AND CROSS-BORDER DATA TRANSFER RESTRICTIONS, BY CHANNEL OF IMPACT



2.1.1 Benefit 1 Enhancing patient access

A light-touch approach to restrictive data policies paves the way for delivering seamless, personalised healthcare – especially for individuals who travel across borders, ensuring access to their medical histories.[32] Digital health services, which accelerated during COVID-19 for remote interactions, self-care, and health analytics, also depend on robust cross-border data flows.[33] Policy frameworks that actively encourage these services will lead to the widespread availability and sophistication of these services. Removing data localisation and transfer restrictions further enables pooled patient insights and interoperability, both crucial for integrated care and stronger population health management.[34]

Furthermore, an accommodative data regime helps companies deliver innovative solutions to patients in various markets. Anecdotal evidence shows that jurisdictions imposing stringent data localisation requirements risk being overlooked by MedTech firms. High costs and added complexity associated with privacy and technical constraints – through certification processes, local storage mandates, or reliance on local vendors – often deter organisations from selecting these countries for Proof-of-Concept studies or product launches. These issues are compounded if legislation is unclear or enacted rapidly without explicit guidelines or enforcement, further delaying market entry.

32. Amazon Web Services (AWS) (2024), "Data governance policies for Asia Pacific cloud adoption in healthcare". Available at: https://aws.amazon.com/blogs/publicsector/data-governance-policies-for-asia-pacific-cloud-adoption-in-healthcare/
33. APACMed (2023), Cybersecurity White Paper. Available at: https://apacmed.org/wp-content/uploads/2023/10/DIGI-2023_10-RCM-Cybersecurity-White-Paper-2.pdf; HIMSS (2023), Cross-border Health Data Flows Global Report. Available at: https://www.himss.org/sites/hde/files/media/file/2023/08/17/cross-border-health-data-flows-global-report_roche-himss.pdf
34. APACMed (2023), The Power and Promise of Health Data Value. Available at: https://apacmed.org/wp-content/uploads/2023/08/APACMed-Power-Promise-of-Health-Data-Value_August-2023-2.pdf

2.1.2
Benefit 2
Unleashing innovative tools and research

Moving away from data localisation and cross-border transfer restrictions would enable the MedTech industry to fully leverage technologies like cloud computing and AI for global healthcare innovation. Cloud-based solutions dismantle geographical barriers, supporting capabilities like telehealth and remote care through real-time data access.[35] They also shift health-IT budgets towards a flexible pay-as-you-go model, reducing infrastructure costs. Beyond savings, the cloud underpins data-powered decision-making and automation, while offering enhanced resilience, scalability, and availability. Where policy supports open data sharing and interoperability, providers can unlock these advantages.[36]

AI has the potential to realise next-generation, intelligent healthcare but could be hindered by restrictive data regulations. In MedTech, AI can enhance operational efficiency, improve diagnostic accuracy and treatment speed, and enable sophisticated remote health monitoring.[37] Applications range from revolutionising good materiovigilance practice (GVP) to refining surgical techniques.[38] With the advent of Generative AI, large language and multimodal models (LLMMs) are emerging as powerful tools for clinical practice and research, capable of processing complex concepts and responding to diverse prompts.[39] However, training LLMMs demands massive resource consumption and long training times, often requiring out-of-country development for commercial viability.[40] In this way, it may be significantly facilitated by unfettered access to and flows of data.

> AI plays a critical role in diagnostics, with its ability to summarise large amounts of information, supporting patient engagement, as well as research and drug development. Cross-border data sharing is essential to leverage these benefits fully and to ensure that AI systems are fine-tuned to specific population data. Therefore, it is important for regulators to have a balanced approach to data regulations, to allow access to new technologies and not limit innovation.
>
> Head of Digital Transformation for a major MedTech company

35. Amazon Web Services (AWS) (2023), Cloud for Healthcare Overview. Available at: https://d1.awsstatic.com/institute/Cloud%20for%20Healthcare_Overview.pdf
36. Amazon Web Services (AWS) (2024), "Data governance policies for Asia Pacific cloud adoption in healthcare". Available at: https://aws.amazon.com/blogs/publicsector/data-governance-policies-for-asia-pacific-cloud-adoption-in-healthcare/
37. KPMG (2024), Realizing the Value of AI in MedTech within Asia Pacific. Available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/09/realizing-the-value-of-ai-in-medtech-within-asia-pacific.pdf
38. Mishra et al. (2025), "Leveraging artificial intelligence to revolutionize medical device safety". Available at: https://accscience.com/journal/ITPS/articles/online_first/4458
39. In patient care, LLMMs can prove invaluable by providing rapid and accurate translations across multiple languages, including rendering complex medical information into plain, everyday language. Furthermore, LLMMs can streamline documentation and administrative requirements, such as generating standardised reports, converting unstructured notes into structured formats, and automating dictation and chart reviews. Within medical research, LLMMs are poised to assist researchers in staying current with the latest developments by summarising existing evidence with increasing factuality and supporting essential computer programming tasks, such as code debugging, simplification, and data visualisation. Mei et al. (2023), "Large language models in medicine: Current applications and future directions". Available at: https://www.nature.com/articles/s43856-023-00370-1
40. Lee et al. (2024), "Ethical and legal considerations for the use of large language models in healthcare". Available at: https://link.springer.com/article/10.1007/s10462-024-10921-0

Removing these barriers to innovation would create broad benefits for the healthcare ecosystem. Small and medium-sized firms – previously inhibited by limited access to training data – could scale AI-driven services more effectively. Advanced AI services, which require significant resources often unavailable locally, would also benefit from the removal of local storage and data transfer restrictions.

> MedTech is particularly affected by data localisation. It often requires the processing of large amounts of data, which is more efficiently done in centralised, offshore facilities. Data localisation can impede the delivery of innovative healthcare solutions and negatively impact patient outcomes.
>
> Policy Manager for a global software industry association

Data localisation and transfer restrictions limit MedTech companies' ability to conduct broad, diverse studies, slowing collaboration. The Cato Institute observed that in the two years after GDPR's passage, clinical trials in the United States funded by the National Institutes of Health (NIH) rose significantly (20.7 per cent) compared to the prior three years, while NIH collaboration with EU4 countries dropped 47.5 per cent during the same period. This suggests that GDPR constraints significantly reduced cross-border data collaborations and research.[41]

> What we're seeing is that there is growing interest in cross-border data sharing for purposes such as clinical trials and research.
>
> Business Development Lead for a healthcare information systems provider

National and global initiatives like the China Real-World Healthcare Data Collaboration (CRHEDO) project and Observational Health Data Sciences and Informatics (OHDSI) initiative highlight how data sharing drives research collaboration. CRHEDO convenes industry, regulators, trade associations, and other stakeholders to use databases from major tertiary hospitals serving more than 18 million patients.[42] At the global level, OHDSI brings together volunteers and collaborators from around the world to establish shared, standardised data ecosystems by using common, interoperable data models and open-source analytical tools.[43]

41. Cato Institute (2024), "How Data Localization Restrictions Hurt Health Care". Available at: https://www.cato.org/regulation/winter-2024-2025/how-data-localization-restrictions-hurt-health-care
42. APACMed (2022), Advancing Real-World Evidence in APAC. Available at: https://apacmed.org/wp-content/uploads/2022/03/Advancing-Real-World-Evidence-in-APAC.pdf
43. OHDSI (n.d.). Home. Available at: https://www.ohdsi.org/

2.1.3
Benefit 3
Unlocking broader healthcare system efficiencies

Rethinking data localisation and cross-border data restrictions could unlock efficiencies in the MedTech and healthcare system.

Data localisation requirements currently impose significant costs. First, monitoring fragmented regulations creates complexity. Divergent regimes across APAC impose substantial compliance burdens on digital health start-ups, device manufacturers, and technology firms. This demands continuous, resource-intensive tracking of often conflicting data privacy laws across multiple jurisdictions.

Second, mandates for multiple local servers require significant capital and operational spending. Healthcare organisations must choose between maintaining redundant infrastructure and investing in patient care innovation. Data localisation can increase data hosting costs by an estimated 30-60 percent.[44] Beyond hardware and software setup, ongoing expenses include personnel for monitoring, patching, and upgrades. In contrast, cloud can reduce operating costs by using on-demand data storage – a 2023 Amazon Web Services study estimated that USD 21.5 billion in cost savings could be realised over five years if all hospitals across the nine studied countries transitioned to the cloud.[45] Dispersed data storage policies also weaken interoperability and increase cyber risks by multiplying data exit points.[46]

> Maintaining multiple servers across regions increases infrastructure costs for us. Additionally, on-premises installations are more expensive and less flexible than cloud, which offers greater flexibility, and often provides better security protocols, reducing the risk of data breaches and unauthorised access.
>
> Founder of a digital health start-up

Finally, MedTech's digital supply chains are inherently cross-border in nature, relying on unrestricted data flows. Outsourcing models such as information technology outsourcing (ITO), business process outsourcing (BPO), and knowledge process outsourcing (KPO) are increasingly data-intensive. Similarly, stringent regulations may push digital health start-ups, often built on global service models, towards B2B rather than B2C offerings, or away from consumer-focused remote healthcare, limiting the scope of innovation.[47]

If data localisation and cross-border data transfer restrictions are eased, MedTech players could reduce compliance and IT costs, restructure their supply chains and operations more efficiently, and pass the savings on to the broader healthcare system, governments, and payers as cost savings.

44. Belfer Center (2021), "Sovereignty and Data Localization". Available at: https://www.belfercenter.org/publication/sovereignty-and-data-localization
45. Amazon Web Services and Deloitte Access Economics (2023), Benefits of cloud-enabled healthcare in Asia Pacific edition. Available at: https://d1.awsstatic.com/institute/Deloitte-Access-Economics-AWSI-Benefits-of-cloud-enabled-healthcare-in-Asia-Pacific-2023.pdf
46. APACMed (2023), Cybersecurity White Paper. Available at: https://apacmed.org/wp-content/uploads/2023/10/DIGI-2023_10-RCM-Cybersecurity-White-Paper-2.pdf
47. Asia House (2023), Asia's Digital Health Innovations. Available at: https://www.asiahouse.org/files/documents/10.11.23_AH_Asias-digital-health-innovations_AW_2.pdf

3 POLICY RECOMMENDATIONS TO UNLOCK MEDTECH'S POTENTIAL

To fully harness the transformative power of health and medical device data, the MedTech industry requires a policy environment that not only facilitates secure data access and transfer but also actively enables innovation and enhances patient care outcomes. This section outlines a comprehensive framework of policy recommendations categorised into three interconnected areas (Figure 7).

FIGURE 7 RECOMMENDATIONS

DESIGNING FIT-FOR-PURPOSE DATA REGULATIONS

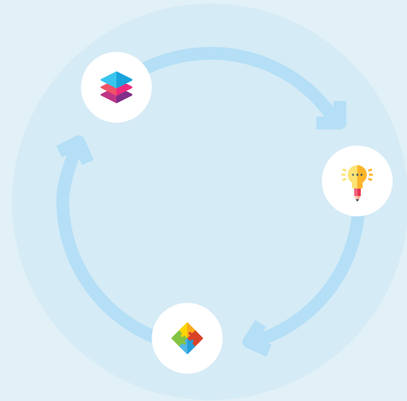
- Adopt risk-based and proportionate health and medical device regulations harmonised with global standards
- Prioritise robust security and privacy standards over strict data localisation

PROMOTING BEST PRACTICES IN TECHNOLOGY AND DATA GOVERNANCE

- Signal acceptance of privacy-enhancing technologies and and common standards.
- Support a cloud-first approach for healthcare

INCREASING ENGAGEMENT AND COLLABORATION

- Communicate closely with medical device regulators to reflect sector-specific needs
- Develop secure mechanisms and frameworks for cross-border data transfers
- Bridge interoperability gaps in cross-border sharing, especially for medical devices



LEGEND
- Actions for businesses
- Actions for government
- Actions for businesses and government

3.1
Recommendation 1:
Designing fit-for-purpose data regulations

We recommend adopting risk-based, fit-for-purpose health and medical device data regulations that are harmonised with global standards.

Prioritising robust technical and organisational security and privacy standards is more effective than strict localisation mandates. Centralised servers, for example, allow greater investment in security, whereas duplicating servers in every country can actually increase the risk of data breaches.[48]

> Data localisation tends to reduce access rather than improve security. Security and privacy are achieved separately, through proper architecture, encryption, and access controls, regardless of data location.
>
> APAC Healthcare Policy Lead for a global cloud service provider

This approach calls for updating privacy and consent protocols to align with international standards for cross-border data transfers. Regulations should be risk-proportionate and support harmonised, interoperable data classification and security measures, rather than country-specific classification rules that hinder cross-border flows. As good regulatory practice, cross-border rules should be transparent, non-discriminatory, and no more restrictive than necessary to achieve their objectives, including for national security. They must also align with international best practices and be flexible enough to accommodate future technological advancements.

48. Piersford (2024), APAC report: Cross-border health data flows. Available at: https://piersford.co.uk/wp-content/uploads/2024/05/APAC-report_Cross-border-health-data-flows_final.pdf

3.2
Recommendation 2:
Increasing engagement and collaboration

We recommend establishing regular engagement channels among data regulators, healthcare agencies, and the MedTech industry, as well as greater technical collaboration for cross-border data transfers.

Policymakers overseeing localisation and transfer rules should communicate closely with medical device regulators to reflect sector-specific needs. This inter-agency dialogue is critical, as general-purpose digital technologies, such as AI, increasingly converge with medical devices. Additionally, governments should foster open consultations with industry stakeholders to capture real-world use cases, from R&D to patient care, ensuring regulations are both effective and practical.

Secure mechanisms and frameworks are critical for trusted cross-border data transfers. Health Data Research UK and the National Research Foundation Singapore, for example, have launched a landmark partnership to advance trustworthy data use at an international scale.[49] Beyond APAC, the European Health Data Space (EHDS) presents a valuable model, as it establishes a unified EU framework for utilising and exchanging electronic health data, enhancing individual access and control over their data, and facilitating secondary use for policy support and scientific research. By 2029, priority health data categories will be exchanged across all EU Member States, and rules on secondary use will also apply more widely (e.g., for data from EHRs).[50] The EHDS aims to overcome one of the biggest hurdles – the fragmented implementation of GDPR – which has hindered cross-border research and secondary use.

Healthcare governance frameworks must recognise that sovereignty comes from sophisticated controls, not physical infrastructure. Evidence suggests that robust technical safeguards and clear governance standards are more effective in protecting patient interests while enabling essential innovation in healthcare delivery.

Emerging initiatives such as the Global Cross-Border Privacy Rules (CBPR) also present a path forward. In April 2022, seven countries signed a declaration to promote trusted cross-border data flows under the Global CBPR and Privacy Recognition for Processors (PRP) Systems. These systems aim to create international certifications ensuring member countries adhere to specific data protection and privacy standards, drawing from the Asia-Pacific Economic Cooperation (APEC) CBPR and PRP systems. However, the lack of sector-specific focus limits their direct relevance for health data. A regional patchwork of non-binding principles for sharing economic data will not suffice as a universal framework for health data.

Interoperability remains another gap, especially for medical devices. While EHR systems have advanced since the introduction of interoperability standards like FHIR in 2013,[51] medical device interoperability lags. Devices such as infusion pumps, ventilators, and patient monitors often operate in data silos, requiring manual transcription into IT systems. HL7 is addressing this through a new FHIR accelerator to help communities create and adopt implementation guides for device data exchange, including personal health and point-of-care devices.[52]

49. National Research Foundation Singapore (NRF) and Health Data Research UK (HDR UK) (2023), MOU NRF HDRUK for Media Dissemination. Available at: https://www.nrf.gov.sg/-files/MOU_NRF_HDRUK_for_media_dissemination.pdf
50. European Commission (n.d.), "European Health Data Space Regulation (EHDS)". Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en
51. MedTech Europe (2021), Interoperability standards in digital health. Available at: https://www.medtecheurope.org/wp-content/uploads/2021/10/mte_interoperability_digital_health_white-paper_06oct21.pdf
52. TechTarget (2025), "HL7 FHIR initiative targets medical device interoperability". Available at: https://www.techtarget.com/searchhealthit/feature/HL7-FHIR-initiative-targets-medical-device-interoperability

3.3
Recommendation 3: Promoting best practices in technology and data governance

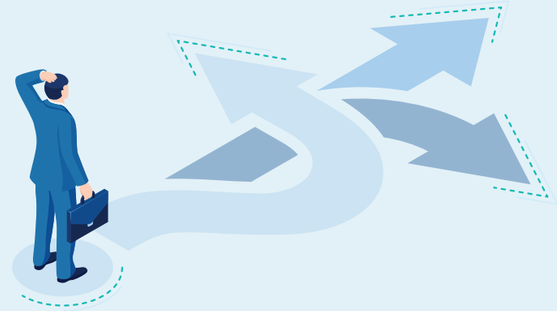
It is important for policymakers to signal acceptance of privacy-enhancing technologies (PETs) as part of stewardship and lifecycle management to support business adoption at scale. PETs such as anonymisation and pseudonymisation reduce data sensitivity, enabling broader use for research, public health, and innovation while upholding privacy and security principles. They enable secondary uses beyond direct patient care, generating insights without compromising individual patient identities. Importantly, safe data sharing and transfer can also be supported through governance and technology tools, including PETs, de-identification, and in-situ analytics platforms that extract insights without moving raw data[53] – avoiding one-size-fits-all regulation. Clear protocols for data archival and decommissioning further mitigate system risks and ensure the long-term integrity, accessibility, and security of data.

Additionally, healthcare policymakers should support a cloud-first approach. Cloud adoption can enhance security, reduce costs, and improve interoperability across the MedTech ecosystem. With healthcare investments lagging in many countries, cloud computing helps shift IT budgets to more efficient, variable-cost models. Rather than imposing new requirements, governments could encourage providers to rely on existing cloud certifications while ensuring services meet local needs. For instance, this could also leverage cloud mechanics such as temporary access mechanisms for specific data sharing needs and pre-built security certifications.

Modern healthcare clouds leverage sophisticated architectural approaches that prioritise patient safety through uninterrupted service. Leading healthcare organisations have moved beyond isolated infrastructure to embrace distributed clinical applications that maintain continuous operation even during regional disruptions. They add advanced automatic security monitoring that identifies and responds to potential threats in real time, updating systems without disrupting clinical care. This model provides far greater reliability than traditional localised systems while preserving complete sovereign control over clinical operations. This is especially valuable for organisations operating across diverse settings, from major hospitals to remote clinics.

> Only 20 per cent of hospitals are currently using cloud services; most of them have a preference to keep it on-premises rather than moving to the cloud.
>
> Solutions Architect for a leading health information systems provider

53. Amazon Web Services (2024), "Data governance policies for Asia Pacific cloud adoption in healthcare". Available at: https://aws.amazon.com/blogs/publicsector/data-governance-policies-for-asia-pacific-cloud-adoption-in-healthcare/



4 THE WAY FORWARD

The MedTech industry operates at the forefront of a data explosion, but its transformative potential is undermined by fragmented and often restrictive data localisation and cross-border transfer regulations across APAC. These rules limit patient access to innovation, hinder collaboration, and impose significant operational costs. Yet they remain central to regulation, reflecting legitimate concerns over privacy and cybersecurity. To earn stakeholder trust, it is essential to demonstrate how these objectives can be met while still enabling open, responsible data flows. Technological solutions, such as privacy-enhancing technologies and robust access controls, offer a critical path forward.

Taking a broader view, the data age of MedTech demands a recalibration of our collective philosophy regarding health and medical device data. Rather than a static asset confined by borders, data should be seen as a dynamic resource that generates exponential benefits through secure, ethical, and collaborative sharing. Its power lies in its ability to be reused and combined, creating a strategic regional asset. For governments, cross-border mobilisation of this data can enhance public health, stimulate economic growth, and improve citizen outcomes. For the industry, it is the key to accelerating the development of life-changing technologies.

Our approach to health and medical device data sharing must unequivocally reflect this global imperative. Healthcare is inherently collaborative, and data sharing should become the norm. While cross-border data sharing has been limited to date, today's digitalised healthcare offers new possibilities. Default restrictions on cross-border data flows frustrate the development of novel health innovations. The public and private sectors must avoid a default presumption that health-related data should not cross borders and instead remain open to the opportunities of such sharing. Although we acknowledge concerns about national interest and cybersecurity, governments must weigh these against the significant benefits that data sharing can deliver in addressing pressing healthcare challenges. Aligning policy with the inherent value and global nature of health and medical device data is therefore not aspirational – it is the vital pathway to a more innovative, efficient, and patient-centric healthcare future for the APAC region and beyond.

ACKNOWLEDGEMENTS

This whitepaper was jointly produced through a collaboration between the Asia Pacific Medical Technology Association (APACMed) and Access Partnership.

Access Partnership

Abhineet Kaul	Director
Daryl Teo	Manager, Economics Strategy
Megan Lim	Manager, Economics Strategy
Patricia Wu	Senior Vice President, Tech-Enabled Verticals

APACMed

Su Fen Ong	Lead, Health Data & AI
Devya Bharati	Associate, Health Data & AI

We would also like to thank the following contributors:

APACMed Health Data Committee

Andrew Wiltshire	Head, Healthcare Policy, Public Policy APJ | **Amazon Web Services**
Julian Petrescu	Senior Business Development Manager | **InterSystems Corp**
Shweta Bhardwaj	Director, Global R&D and Digital Policy | **Johnson and Johnson**
Laurence Laumonier	Senior Director, Global Privacy, APAC | **Johnson and Johnson**
Wanlin Wu	Senior Manager, Global Privacy, MedTech China | **Johnson and Johnson**
Hoang An Vu	Privacy Consultant | **Johnson and Johnson Vietnam**
Tian Xu	Senior Manager, Government Affairs | **Johnson & Johnson China**
Dr Suhina Singh	CEO and Founder | **Jonda Health**
Kuben Vather	COO | **Jonda Health**
Leon Jackson	APAC Digital Transformation Lead | **Roche Information Solutions**
Darwin Mariano	VP External Affairs - East Asia and Pacific | **UnitedHealth Group**
David Wearne	CEO Inventor | **Wearne Digital**

Industry Experts

Tham Shen Hong	Senior Manager, Policy, APAC | **Business Software Alliance**
Christy Tsang	Head of Secretariat | **Asia Cloud Computing Association**

APACMed
The voice of MedTech

About APACMed

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. For more information, visit **www.apacmed.org**