TECHNICAL REPORT

Exploring Digital Health and Telemedicine Practices: A Study Visit to Singapore

Prepared by: Health Intervention and Technology Assessment Program (HITAP)

06 October 2023

Contents

List of Figures

Acknowledgement

This report provides an overview of the study visit to Singapore from Thailand that was aimed at exploring digital health and telemedicine practices in Singapore. Supported by the Health Systems Research Institute (HSRI), the event took place from August 2nd to 4th, 2023, and was organised by the Health Intervention and Technology Assessment Program (HITAP) in collaboration with the National University of Singapore (NUS).

This report has been prepared by Ms. Jirathorn Sutawong, Mr. Thanayut Saeraneesophon, Ms. Papada Ranron, Mr. Thanakit Athibodee, and Ms. Annapoorna Prakash, with the support of and review by Ms. Nitichen Kittiratchakool and Assoc. Prof. Dr. Wanrudee Isaranuwatchai.

We are grateful to Dr. Sopon Mekthon, Dr. Pongsathon Pokpermdee, Dr. Piya Hanvoravongchai, Dr. Withita Jangiam, Dr. Supharerk Thawillarp, and Ms. Aree Moungsookjareoun for their active participation throughout this 3-day event.

We extend our sincere appreciation to Professor Yik-Ying Teo and Asst. Prof. Dr. Mornin Feng from the National University of Singapore for organising this event and for their hospitality.

We are grateful to Dr. Yot Teerawattananon from HITAP for his support and guidance throughout this initiative. We also acknowledge other HITAP staff whose work on telemedicine aided in the preparation for the event.

We would also like to extend our thanks to the organising staff at the venue for their assistance in ensuring a smooth and well-coordinated event.

The findings, interpretations, and conclusions presented in this report do not necessarily reflect the views of the funding or participating agencies.

List of Acronyms

APEC	Asia-Pacific Economic Cooperation
CCS	Country Cooperation Strategy
CDG	Cyber Defense Group
CERT	Computer Emergency Response Team
CQC	Care Quality Commission
CSA	Cybersecurity Agency of Singapore
DAC	Data Access Committee
DHI	Digital Health Interventions
EPSO	European Partnership for Supervisory Organisations
HCSA	Healthcare Services Act
HCSE	Healthcare Cybersecurity Essentials
HIB	Health Information Bill
HIS	Health Information Systems
HITAP	Health Intervention and Technology Assessment Program
HITMAP	Health IT Master Plan
HITSPS	Healthcare IT Security Policy and Standards
HPB	Health Promotion Board
HRG	Health Regulation Group
HSA	Health Sciences Authority
HSRI	Health Systems Research Institute
ICT	Information and Communication Technology
IT	Information technology
MOH	Ministry of Health
MOPH	Ministry of Public Health
MOSD	Modes of Service Delivery
NEHR	National Electronic Health Record
NHG	National Healthcare Group
NHS	National Health Services
NUHCS	National University Heart Centre, Singapore
NUHS	National University Health System
PHMCA	Private Hospitals and Medical Clinics Act
PDPA	Personal Data Protection Act
SPD	Strategy and Planning Division
TRUST	Trusted Research and Real World-Data Utilization and Sharing Tech
TTX	TableTop Exercise
WHO	World Health Organization

Introduction

Thailand is in the process of adopting technologies appropriate for its context to provide telemedicine on a national scale. However, there are some gaps that make achieving universal telemedicine in Thailand challenging on certain areas. Technological factors and the lack of a uniform information system is a problem, e.g., administrators select their own information systems which are incompatible with regards to future use, data items, and versions. Additionally, the poor performance of internet connection made patient identification, automatic data recording, and record pulling processes sometimes quite slow.

To ensure successful implementation, it is imperative to strategically plan the next steps. Drawing insights from practical telemedicine experiences from other settings can be pivotal to avoiding repeating past errors. Therefore, a study visit to a country line Singapore, which has made strides in implementing telemedicine, was deemed essential to grasp their digital health service provisions and foster dialogue between Thai and Singaporean stakeholders.

This study visit is supported by the Health Systems Research Institute (HSRI) which supports a study titled "Recommendations to support the development of operation and M&E process for telemedicine programme based on lessons learned from Thailand and the world". This study is part of the World Health Organization's Country Cooperation Strategy (WHO-CCS) on digital health, which is supported by WHO, the Thai Health Promotion Foundation (ThaiHealth), with the Strategy and Planning Division (SPD) of the Ministry of Public Health (MoPH) and the Health Intervention and Technology Assessment Program (HITAP) serving as the Secretariat.

This report summarises the sites visited during the study visit from 2nd to 4th August 2023, providing an overview of each site, key discussion points, and crucial insights relevant to Thailand's context. The sites visited during this study visit include:

1. TRUST platform
2. Synapxe
3. Health Promotion Board
4. Health Regulation Group
5. National University Heart Centre, Singapore

The primary audience of this report is Thai policymakers, from the Ministry of Public Health and the Ministry of Digital Economy and Society including stakeholders who are keen on advancing the nation's digital health landscape. Additionally, this report also targets funding agencies such as the WHO and HSRI, who play a crucial role in advancing the research supporting digital health through adequate funding support.

Background to telemedicine in Singapore

The Republic of Singapore is an island nation situated in Southeast Asia with the population of nearly 6 million. The country's healthcare system, guided by the principles of Universal Health Coverage (UHC), is designed to ensure equitable access to different levels of healthcare in a timely and cost-effective manner [1].

Much like its rapidly growing economy and social progress, the healthcare system in Singapore is also advanced and fast evolving in response to the changing world [2]. Keeping themselves adept to the rapidly changing world, Singapore is a forerunner in digital health innovation and implementation [3]. COVID-19 pandemic played a crucial role in further cementing this shift toward digital health. Their strong information technology (IT) infrastructure along with the conducive legal and regulatory framework are the common positive determinant enabling this digital transformation.

In 2013, Singapore launched its Smart Nation Initiative, aiming to use IT to create a digital-first country [4]. As a part of this programme, Smart Health Initiatives were launched to introduce digital health to the healthcare system. Concurrently, the Health IT Master Plan (HITMAP) was developed in 2013 to incorporate advancement in digital health into Singapore's healthcare system. The three objectives of HITMAP are often described as the "3 Beyonds". These include:

- **Beyond hospital to community** referring to the extension of hospital services into homes, enhancing healthcare accessibility and lessening frequent hospitalisations to alleviate the burden on medical facilities;
- **Beyond quality to value** refers to efficient resource allocation to deliver value and sustainability; and
- **Beyond healthcare to health** promotes a comprehensive strategy for well-being, emphasising mental and physical health, preventive care, and more.

Figure 1: Objectives of HITMAP. Adapted from Synapxe website.

In order to achieve these three strategic objectives, seven programmes revolving around big data and healthcare digitalisation have been developed and deployed [5]. **Figure 1** demonstrates the key objectives and the seven programmes that were developed.

Additionally, in 2015 Singapore laid down the Health Products Act and the Health Products (Medical Devices) Regulations 2015 that serves as the foundation for the Digital Health Interventions (DHIs) regulatory landscape for the country [6]. These regulations require medical devices to be registered with Heath Sciences Authority (HSA) before placing them on the Singapore market unless they are exempted. Furthermore, in 2017 the HSA guidelines on telehealth were developed to determine if a telehealth intervention is a regulated medical device under HSA and to understand the relevant regulatory requirements [6].

In conclusion, Singapore has developed an innovative and agile digital health ecosystem from which some key lessons can be drawn. Learning such lessons can play a crucial role in helping Thailand take that extra mile in effective planning and implementation of its telemedicine services.

TRUST Platform

Overview

The commitment to establish the health-related real-world data for research led to the development of Singapore's national data sharing platform, Trusted Research and Real World-Data Utilization and Sharing Tech, popularly known as TRUST. Specifically, the TRUST Platform is a comprehensive digital security platform of Singapore that focuses on building trust, confidence, and security in the digital space. They provide cutting-edge services to safeguard data and ensure privacy for both businesses and individuals. The platform is especially prominent in the realm of digital health and medical information, where data security is of utmost importance.

The main objective of the TRUST platform is to create a secure digital space that integrates the diverse and complex health-related data into the large-scale datasets for the academic community to utilise and synthesise those available data for research purposes, thereby driving novel and data-driven research. The suppliers and users of data for this platform include:

- Data contributors who allow their anonymised data to be accessed via TRUST. These contributors include public health institutions, research institutions, and public agencies.
- Data requesters who use the data which is available in the platform for research. These requestors can vary from healthcare professionals to researchers to academics.

Figure 2 demonstrates the procedure of deriving data from contributors.

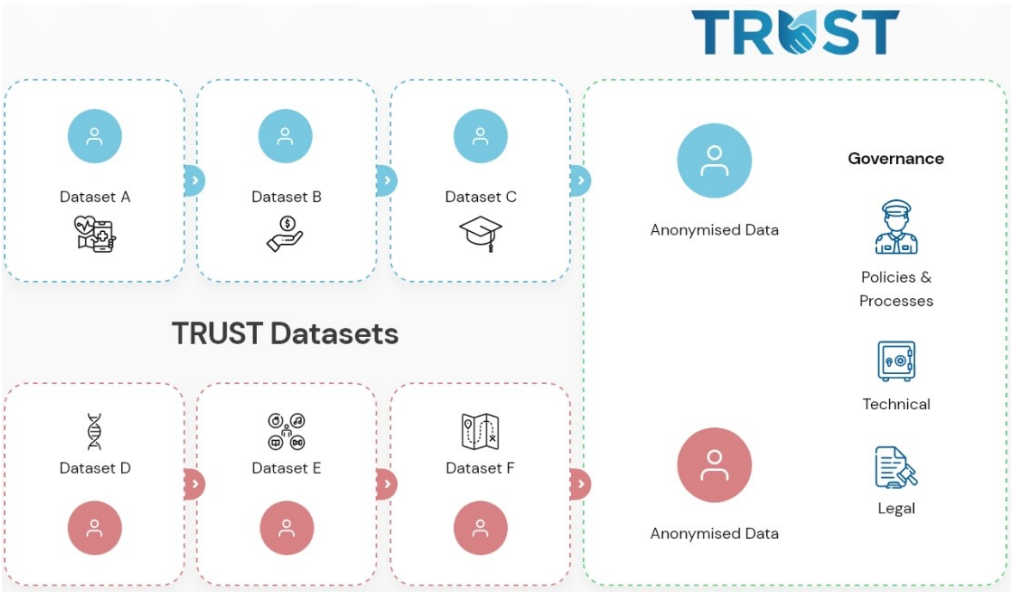

Figure 2:Schematic representation of deriving data from contributors. Adapted from TRUST website.

Notably, the data requestors can only access the data upon approval by the Data Access Committee (DAC). The DAC currently has 13 members with a variety of specialisations and backgrounds. The committee has representatives from the Ministry of Health, National Heart Centre Singapore, National Council of Social Service, and The Smart Nation and Digital Government Office. The DAC evaluates the purpose and outcomes of the data requested for approval.

Stakeholder engagement activities

The meeting followed a concise format, beginning with a brief 15-minute presentation by the TRUST representative, followed by an interactive open question and answer (Q&A) session. The meeting was primarily led by Ms. Koh Mingshi, Director of the Chief Health Scientist Office (CHSO), Ministry of Health (MOH).

The presentation by the representatives from the TRUST platform can be accessed here.

Key discussion points

This section of the report sheds light on the key discussion points that emerged during the visits to the site.

Five Pillars of Safety

During the presentation, it was highlighted that the cooperation, led by the MOH, GovTech, Synapxe, and Smart Nation of Digital Government Office, had proceeded to develop this digital platform under the objective of building non-border space for health-related research since 2020. Although the development process had been affected by the COVID-19 outbreak, the platform was successfully operationalised in 2022 with data protection and cybersecurity at the core of it. According to the presentation, the "Five Safe Pillars" which form the cornerstone of the platform were also highlighted. These five pillars are:

1. **Safe Purpose:** The scientific, clinical, and health values of the research request must be reviewed by The TRUST DAC before allowing access to the data. During this review process, the committee will determine if the research benefits the public and generates social benefits.
2. **Safe People:** Within a pre-defined timeframe, TRUST requires every individual to have the credible credentials and approval of research to be eligible for accessing TRUST, hence ensuring that data will not be disclosed to any unauthorised individuals.
3. **Safe Settings:** TRUST employs standard government security measures in both physical and technical implementation to prevent unauthorised data disclosure. Besides, all steps of every activity will be stored on TRUST and monitored to ensure proper usage.
4. **Safe Data:** The utilisation of data on TRUST is upon authorised access and involves anonymisation measures to lower the potential for re-identification. This process implies that the data extracted with TRUST does not include any personal identification details, such as National Registration Identify Card (NRIC) numbers and names, making it improbable to pinpoint specific individuals within the research data. Additionally, various legal and technical precautions are in place to mitigate the possibility of re-identifying individuals.
5. **Safe Output:** Any output that the data requester intends to publish must first be offered in drafting form to TRUST for assessment and for verification of any potential re-identification issues.

The procedure of deriving data and the implementation of five safe pillars is demonstrated in **Figure 3.**

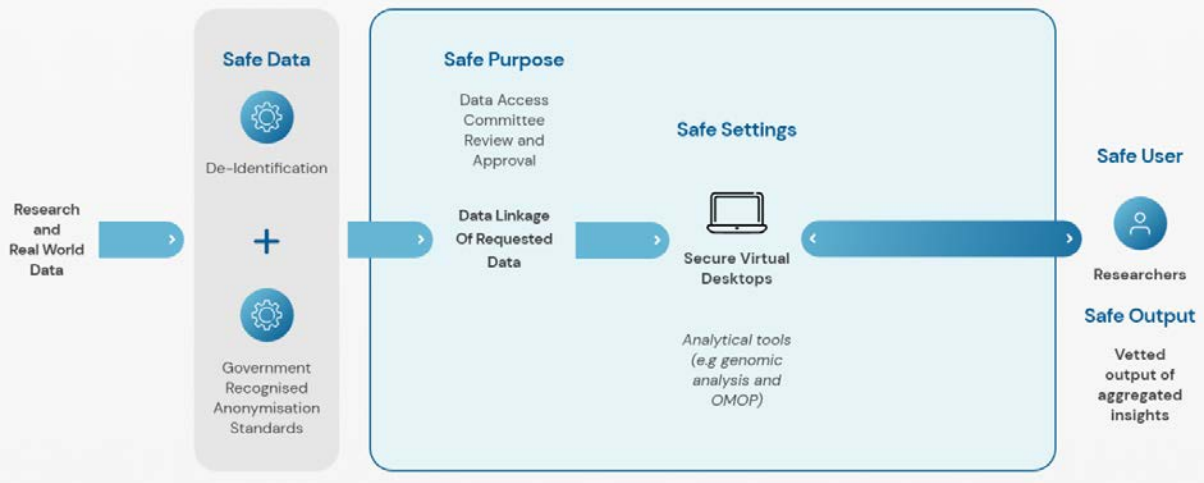

Figure 3:Implementation of 5 safe pillars. Adapted from TRUST website [7].

Example of TRUST platform driven research

There are seven projects so far that employed integrated health data from the TRUST platform for real-world analysis. For instance, research to "determine how lifestyle choices affect the likelihood of chronic disease based on a person's genetic information (Polygenic Risk Score or PRS)" attempted to comprehend the effects of lifestyle on the development of chronic disease based on the genetic information of an individual used genetic information made available through the TRUST platform. The study concluded that people who have an active lifestyle are less likely to be at genetic risk of obesity.

Facilitators for the development of a national health platform

There are many hurdles in developing a national health platform like TRUST. However, identifying the factors that can enable the creation of such platform is crucial in a country's digital health advancements. As highlighted by representatives from TRUST, some of the significant enablers are:

- political buy-in;
- identifying and collaborating with suitable partners;
- improving digital infrastructure and technical development;
- conducive policies and laws; and
- engagement of relevant communities and public sphere.

Lessons for Thailand

This section of the report aims to draw insights from the study visit to TRUST and identify valuable lessons that can be applied to the context of Thailand.

Turning conventional data into a unified digital format is a complicated endeavour. Nevertheless, Thailand acknowledges the necessity of this evolution, as emphasised by Thai stakeholders during the study visit. The visit to TRUST underscored the critical importance of standardising health records to enable the digital evolution of healthcare. Despite the challenges and the substantial resources required for implementing this digital unification, the outcomes of such an initiative can play a pivotal role in enabling practical health research. This achievement has the potential to effectively guide the

trajectory of Thailand's healthcare system in a positive direction including to support health services and policy research which can ultimately be used to further assist policy-making process.

Synapxe

Overview

Integrated Health Information System (IHiS), now known as Synapxe established in 2008 is the Ministry of Health's HealthTech agency to advance healthcare Information Technology (IT) in Singapore [5]. Synapxe is the implementor of IT systems into the public healthcare infrastructure of Singapore. They maintain and manage around 800 IT systems including electronic medical records, medical imaging, laboratory test records, medication dispensing, patent registration and billing, financial aid, community care, telehealth and more.

In terms of impact, Synapxe has supported all major public healthcare institutions in Singapore in achieving either HIMSS EMRAM1 stage 6 or 7, which is the international benchmark for advanced technology used in patient care. Moreover, IT systems developed by them are reported to have benefited more than 12 million visits annually in Singapore.

Additionally, Synapxe has a dedicated Cybersecurity & Information Security team tasked with the protection of Singapore's public health system, networks and devices. The key activities of the team include:

- Protection against cyberattacks;
- Protection against accidental data leakage; and
- Protection against intentional data theft.

In addition to pioneering IT techniques to combat cyberattacks, Synapxe is effectively engaging and training healthcare staff to improve their awareness and vigilance on cyber security. Lastly, in supporting the building of technology to combat cyberattack and increasing awareness about cyber security, Synapxe has also developed additional strengthening measures like:

- Strengthening of the organisational and governance structure in Synapxe to better manage cybersecurity risks;
- Strengthening operating processes for quicker responses to cybersecurity events;
- Building capabilities through training, reviews, and assessments; and
- Reviewing IT systems, particularly Critical Information Infrastructure (CII), to better defend and respond to advanced threats.

In conclusion, the multi-pronged approach adopted by Synapxe in tackling potential cyberattack is commendable. Getting a better understanding of the operation of these strategies can add critical insights that can be helpful in Thailand's digital health journey.

Stakeholder engagement activities

The meeting started with a brief 15-minute presentation by the Synapxe representative, followed by an interactive open Q&A session. The meeting was led by Mr. Frankie Phee, Deputy Director of Synapxe.

Key discussion points

This section of the report sheds light on the key discussion points that emerged during the visits to the site.

After the presentation from the Synapxe representatives, the stakeholders from Thailand showed particular interest in understanding the initiation and operational aspects of Synapse. The discussion topics ranged from budget allocation for Synapxe to cyber security.

Financial allocation and the human resources

Synapxe representative confirmed that they are allocated a budget ranging from 500 to 700 million Singapore dollars for their IT project. This budget also supports a workforce of over 200 professionals who exclusively focus on cyber security aspects. Additionally, the representative highlighted the significance of tailoring the cyber security budget based on the digital maturity of the country. Furthermore, it was underscored that an established international practice involves allocating 15% of the initial IT budget to cyber security during the initial stages of a project. As the project matures, this proportion is adjusted to 7% to sustain robust cyber security measures.

Fortification of cyber defence

Some of the strategies employed by Synapxe for the fortification of Singapore's cyber defence are:

- Advanced Threat Protection (ATP),
- Restriction of privileges access to dedicated local workstations,
- Database Activity Monitoring,
- Ongoing pilot on Virtual Browser solution to minimise risks of downloading and executing malicious files from internet.

Cybersecurity Awareness and Proactive Defense

There was a dynamic exchange of dialogue centered around cybersecurity and the pivotal role played by Synapxe in ensuring cyber security. Delving into the imperative aspect of raising awareness amongst the general healthcare staff concerning cybersecurity, Synapxe highlighted their multi-faceted strategies meticulously designed to engage the public proactively. Among these strategies, the adoption of a dual-pronged "carrot and stick" approach was highlighted. This approach entails the utilisation of both incentives and consequences to foster a heightened sense of responsibility regarding cybersecurity practices among the healthcare work force. While incentives act as motivational guides, prompting individuals to proactively engage in upholding digital environments, the enforcement of consequences, such as influencing performance evaluations or the possibility of termination, functions as a discouragement against potential disregard for sound cybersecurity protocols.

An interesting facet of their approach is the incorporation of regular phishing exercises. By subjecting employees to simulated phishing scenarios, Synapxe cultivates a heightened sense of vigilance and awareness, actively preparing them to identify and thwart genuine threats.

Steps after a cyberattack

When asked about the initial steps undertaken in response to a potential cyberattack, Synapxe's representative elaborated on procedure. Firstly, the forensic team is tasked with discerning the extent

and nature of the attack. This phase is pivotal in comprehending the breach's scope, enabling the organisation to strategise effectively. Subsequently, the focus shifts towards containment and resolution, wherein immediate steps are taken to patch vulnerabilities and isolate the threat.

Lessons for Thailand

This section aims to draw insights from the study visit to Synapxe and identify valuable lessons that can be applied to the context of Thailand.

Prioritise Data Hygiene and Proactive Measure: Embarking on a cyber security journey entails starting with a strong focus on maintaining good data hygiene. This foundational step involves ensuring the integrity and cleanliness of data. Following this first step, proactive measures such as timely patching of vulnerabilities and robust defense against phishing attacks become imperative. Furthermore, it is crucial to phase out outdated and obsolete technology that might pose security risks.

Reconsidering Personal Data Protection Act: Contrary to assumptions, the Personal Data Protection Act (PDPA) might not necessarily impede effective cybersecurity practices. In some instances, maintaining strong cybersecurity does not require unrestricted data access. Additionally, Synapxe's practices demonstrate that they engage in rigorous data cleaning procedure, which allows them to work within PDPA regulations while ensuring robust security measures.

Shift to Unified Health Records: Transitioning from a "one patient one record" approach to a "one citizen one health record" strategy can bring about significant advantages. This shift unifies health information across different interactions and healthcare providers, enabling a more holistic view of an individual's health journey. This streamlined approach can lead to better care coordination and enhanced data security.

Cybersecurity as an Enabler: Instead of considering cybersecurity as solely a defensive measure, it should also be seen as an enabler in the digital health journey of a country. Effective cybersecurity practices can facilitate innovation and the integration of advanced technologies in the healthcare sector. By establishing robust safeguards, stakeholders can confidently explore new opportunities without compromising data integrity and patient privacy.

Health Promotion Board

Overview

The Health Promotion Board (HPB) was established as a statutory board under the MOH in 2001 with the vision of building “A Nation of Healthy People”. HPB aims to empower Singaporeans to attain optimal health, increase the quality and years of healthy life and prevent illness, disability, and premature death. As the key agency overseeing national health promotion and disease prevention programmes, HPB spearheads health education, promotion and prevention programmes as well as creates a health-supportive environment in Singapore. The organisation develops and organises health promotion and disease prevention programmes, reaching out to the healthy, the at-risk and the unhealthy at all stages of life – children, youths, adults, and older Singapore residents. Its health promotion initiatives cover nutrition, physical activity, mental well-being, health screening, tobacco control and communicable disease education [8].

Stakeholder engagement activities

The meeting, beginning with a brief 15-minute presentation by the HPB representatives, followed by an interactive open Q&A session. The meeting, primarily led by Mr. Tay Choon Hong, Chief Executive Officer of the Health Promotion Board.

Key discussion points

After the presentation, there were discussions between the delegation from Thailand's Ministry of Public Health and the HPB management team on various issues, such as how Singapore promotes digital literacy among its citizens and about the public-private partnership to foster creativity and innovation while guaranteeing long-term commercial cooperations. Some of the key discussion points were as follows:

Digital health promotion initiatives

HPB has organised many health promotion programs since its inception. Most of them employ digital technologies such that it brings participation at their fingertips. For example, the National Step Challenge encourages everyone to get more physically active by walking. People can get points for every step they take and subsequently the points can be redeemed to buy healthy products at convenience stores nationwide. It is a successful project that has been running for over five years, with the number of participants growing steadily yearly.

Gamification of health promotion initiatives

HPB representatives emphasised that the primary conceptual foundation for each wellness promotion program was inspired by Pokémon games. The concept revolves around merging enjoyment and accessibility, allowing anyone to participate with just a mobile phone while engaging in physical activities. Despite being a non-profit game, it remains highly popular. The feasibility of introducing such activities to the general public while also providing incentives was also discussed further.

Lessons for Thailand

The integration of technology in health promotion is widely seen in Singapore. Governments' commitment to fostering an environment conducive to innovative health promotion programs, such

as those gamifying healthy behaviors, sets an example. The innovative program that incentivises healthy behaviors through convenience store coupons serves not only as a health promotion tool but also as a means to enhance participation and stimulate both public and private sector economies.

Health Regulation Group

Overview

The MOH in Singapore has established the Health Regulation Group (HRG) with the purpose of overseeing the comprehensive regulation of healthcare services, premises (including hospitals, clinics, and nursing homes), and the digitalisation of health-related practices within Singapore's healthcare landscape. The central mission of the HRG revolves around ensuring public health, fostering healthcare innovations, and safeguarding patient safety. The approach is geared towards proactively assessing and adapting to new healthcare services to ensure they adhere to robust standards. As new services emerge, our readiness to effectively regulate them is a top priority.

HRG oversees the licensing of healthcare institutions under the Private Hospitals & Medical Clinics (PHMC) Act/Regulations, encompassing diverse healthcare facilities such as hospitals, medical centers, community health centers, nursing homes, clinics (including dental clinics), and clinical laboratories. Their role encompasses ensuring compliance with MOH regulations through rigorous audits and inspections. Additionally, HRG also assumes the responsibility of regulating healthcare professionals, verifying the qualifications and licenses of doctors, nurses, dentists, and allied health staff. This comprehensive approach guarantees the perpetual maintenance of elevated standards in patient care and safety.

Singapore's healthcare landscape is guided by the cornerstone initiative, Heathier SG, which emphasises preventive care and early intervention through secure health data sharing. This strategic approach underscores the necessity of consolidating patient information within robust government databases, building upon the National Electronic Health Record (NEHR) repository. The pivotal roles of entities like National Healthcare Group (NHG), National University Health System (NUHS), and SingHealth (SHS) enhance patient management.

A patient enrollment strategy, structured into geographic clusters, East, Central, and West, empowers local general practitioners to collaboratively enroll and oversee patients. This proactive approach includes health status monitoring and resource provisioning for holistic care. Simultaneously, Family doctors, Hospitals, Laboratories, and Nursing Homes contribute selected health data to NEHR, while residents access information through the HealthHub platform, fostering a comprehensive and accessible healthcare network.

Aligning with these efforts, stringent cybersecurity and data governance standards are pivotal. The Healthcare Cybersecurity Essentials (HCSE) ensures fundamental cybersecurity adherence, promoting the security, confidentiality, and integrity of health data. The Health Information Bill (HIB) enforces these standards uniformly, solidifying security across both public and private sectors. This harmonised approach culminates in a robust framework that optimises resource utilisation while ensuring comprehensive patient management.

Stakeholder engagement activities

The meeting began with a brief 15-minute presentation by the HPB representatives, followed by an interactive open Q&A session. The meeting, primarily led by Professor Raymond Chua, Deputy Director General of Health overseeing healthcare regulations, concurrently holds the role of Assistant Commissioner for Cybersecurity in the healthcare sector, designated by the Cybersecurity Agency of Singapore (CSA).

The presentation used by the HRB representatives can be found here.

Key discussion points

This section sheds light on the key discussion points that emerged during the visits to the site.

Coordinated approach to healthcare regulation

Professor Raymond Chua delineated a comprehensive and integrated strategy for healthcare regulation characterised by a multi-layered oversight approach **(Figure 4)** including:

- SG Wide Legislation (e.g., Penal Code, Personal Data Protection Act)
- Health Products & Devices (Health Products Act)
- Healthcare Professionals (various professional registration acts e.g., Medical Registration Act, Ethical Code and Ethical Guidelines)
- Healthcare Services (Private Hospitals and Medical Clinics Act, Healthcare Services Act)

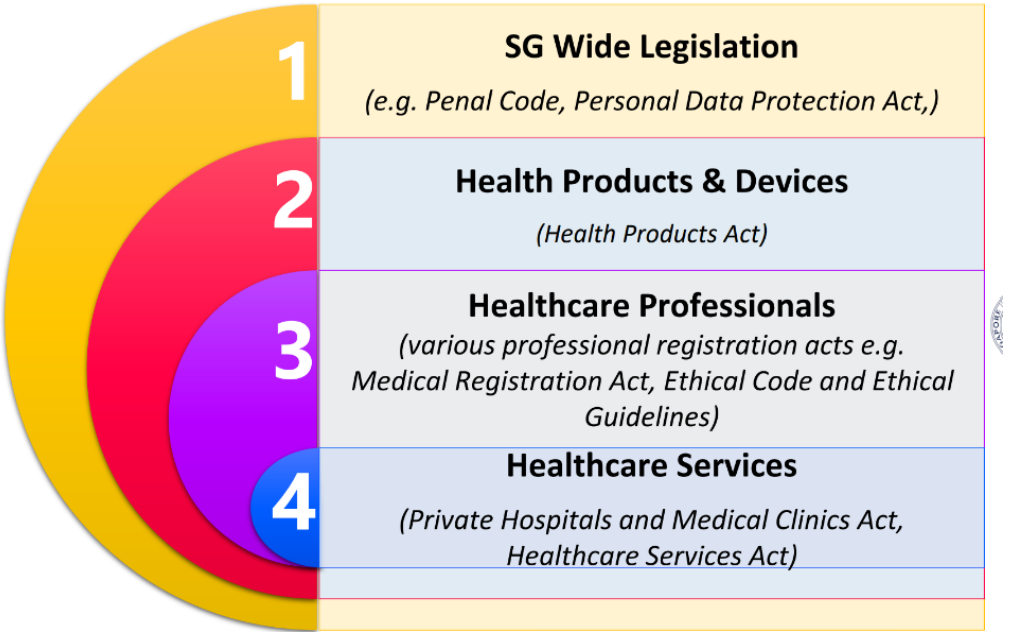

Figure 4:Coordinated approach of healthcare regulation. Adapted from the presentation given by the HRG team

With such a balanced and pragmatic approach, Singapore is trying to ensure that patient safety guaranteed while introducing appropriate laws and regulatory frameworks to enable and support upstream preventive care. This helps them to develop fit-for-purpose regulatory tools to support the development and adoption of innovative services.

Modes of Service Delivery (MOSD) Model for regulation

HRG has embarked on substantial regulatory transformations. The transition from PHMC reflects a shift from a location-centric approach to a more intricate framework. Departing from a focus solely on geographical considerations, the emphasis has evolved towards a dynamic interplay between premise-based and service-based models, thus facilitating the regulation of telemedicine services. This strategic realignment revolves around crafting a service delivery model that embraces a

spectrum of options, encompassing: 1) permanent premises; 2) conveyances; 3) temporary facilities; and 4) remote provisions (which would include telemedicine).

The impact of COVID-19 has notably propelled the adoption of telemedicine. It is evident that service providers are increasingly extending their reach to offer care in homes and communities now, which pose challenges for regulation under the existing act, the PHMC Act. In response to this dynamic environment, the Healthcare Services Act (HCSA) was conceived to replace the PHMC Act which is regulated by geographical location of service delivery. Its goal is not only to enhance the protection of patient safety and well-being but also to facilitate the introduction of new and innovative healthcare services. The HCSA follows a premises-based approach and is predominantly regulated by services such as Medical Clinic Service, Health Screening Service, Telemedicine Service, Clinical Laboratory Service, Clinical Genetic Service, and Clinical Genomic Service.

Within this healthcare services model, regulation is anchored in the specific services rendered. Beyond the established physical premises, HRG endorses using alternative approaches, such as mobile units or other convenient means, to facilitate service delivery. For instance, some clinics might conduct mammograms in mobile units or buses. It is noteworthy that a clinic holding a permanent primary location is now granted the flexibility to operate temporarily and remotely, concurrently.

Regulatory Sandbox

Furthermore, HRG introduced a telemedicine regulatory sandbox in 2018, establishing a secure testing environment for emerging innovative services within controlled parameters. This collaborative approach involves closely cooperating with service providers to define operational protocols. This allows them to provide services without immediate licensing, facilitating a practical trial phase during which on-ground data is gathered.

The comprehensive dataset of the observations of service operations during the sandbox period provides invaluable insights to tailor the regulatory framework to align with the distinct intricacies of each service.

Harnessing the Strength of Networks

In 2022, the Asia-Pacific Economic Cooperation (APEC) Network of Health Regulators was established, facilitating the exchange of regulatory insights and best practices concerning healthcare-related matters among economies in the Asia-Pacific region. This initiative aims to promote regulatory cooperation among APAC economies and address pertinent local and regional challenges. Notably, Professor Raymond emphasised the presence of shared challenges that warrant collective attention, particularly in conjunction with Thailand. This active engagement fosters the mutual sharing of valuable information and promotes collaborative efforts among regulators. The overarching goal is to establish a robust APAC network that not only facilitates APAC collaboration but also extends its reach to connections between APAC and European networks.

Moreover, the APAC Network and HRG are committed to expanding horizons through active engagements with international entities. These include associations such as the European Partnership for Supervisory Organisations (EPSO) in Health Services and Social Care aims to share and learn best practices, approaches, and challenges. This involves knowledge exchange with regulatory counterparts such as the Care Quality Commission (CQC), the National Health Services UK (NHS), Healthcare Denmark, the Finnish Health Delegation, and more.

Lessons for Thailand

In the face of the rapidly evolving landscape of digital health, regulators are confronted with a challenge that necessitates strategic and prudent action. This challenge encompasses several essential aspects:

- **Continuous Monitoring and Identification:** The role of regulators becomes pivotal in expertly monitoring and identifying emerging digital health trends amidst the swiftly evolving local landscape.
- **Informed Decision-Making:** Regulators assume the responsibility of consistently evaluating the risks and benefits linked with novel healthcare services or modalities.
- **Collaborative Partnerships:** Imperative collaborative partnerships with diverse stakeholders, ranging from licensees to international regulatory bodies, become instrumental. Sharing insights and best practices within these partnerships can facilitate the co-creation of robust and effective regulatory frameworks.
- **Balancing Safety and Innovation:** A complex equilibrium must be achieved where stringent regulations are strategically established to ensure patient safety, while simultaneously nurturing the innovation of digital health services. This balance extends to minimising the regulatory burden on stakeholders, thus fostering a conducive environment for growth.

Enhancing Health Information Security

Professor Raymond emphasised several key points, including the imperative of regularly patching and maintaining the system and exploring innovative regulatory framework, as well as implementing robust anti-malware and firewall measures. A comprehensive audit trail is essential, allowing real-time tracking of activities, timestamps, and user identification in the event of any unauthorised access. Ensuring the existence of a thorough data back-up system is paramount, this guarantees data integrity and recovery in cases of system disruptions. In instances of vendor outsourcing, meticulous adherence to established outsourcing policies is imperative. Additionally, raising security awareness among the staff is essential. This activity can entail thorough training to improve an understanding of self-cybersecurity and adherence to software standards.

The recommendation entails a strategic orchestration of monitoring, collaboration, and careful balance to foster an environment where patient safety is upheld, innovation thrives, and regulatory complexity is kept to a minimum.

National University Heart Centre, Singapore

Overview

The healthcare service system of Singapore is divided into three groups: 1. the National University Health System (NUHS), responsible for the Western region of the country; 2. the National Healthcare Group (NHG), responsible for the Central region; and 3. Singapore Health Services (SingHealth), responsible for the Eastern region. Each healthcare region includes service units, hospitals, clinics, and other facilities.

NUHS has the primary objective of creating a healthy community by adapting treatment approaches to changing times and promoting health among the population. NUHS possesses strengths in different areas of healthcare, including nursing, education, and research. Drawing from these strengths, NUHS can facilitate the development of the healthcare system, establish new care models and collaborate with the community, ultimately improving the quality of life for Singaporeans. In Singapore, there is a digital health system in place to enhance the healthcare system. Ensuring cybersecurity and implementing policies are essential to instill confidence among people and transform the way healthcare services are accessed by the population.

Stakeholder engagement activities

The meeting commenced with Professor James Yip, the Director of the National University Heart Centre, Singapore (NUHCS), presenting on the topic of Cybersecurity at NUHS, which included a discussion of a cyberattack event that occurred in 2018, as well as methods for addressing data breaches within the healthcare system. Subsequently, Professor James Yip led the delegation from Thailand's Ministry of Public Health on a visit to the NUHCS. This visit provided firsthand insight into the actual operations within Singapore's healthcare system, offering a practical understanding of how the healthcare system functions in Singapore.

The PowerPoint presentation used for the study visit can be found here.

Key discussion points

This section sheds light on the key discussion points that emerged during the visits to the site.

After introducing the cyberattack incident in Singapore in 2018, a highly insightful discussion regarding the nation's endeavors to fortify its cybersecurity measures took place. Several pivotal topics were deliberated upon, including:

Cybersecurity systems workstreams

The development of cybersecurity systems is divided into six important workstreams as follows:

1. **Technical**: This involves establishing a Cybersecurity Council and implementing 18 technical measures to be prepared for incidents. These measures include database activity monitoring, internet surfing separation, and advancements in security operation centers.

2. **Cybersecurity policy**: This workstream focuses on developing policies that outline responsibilities in various areas, such as incident reporting frameworks, risk management frameworks, and cybersecurity training.
3. **IHIS organisation**: This workstream is dedicated to designing organisational structures that ensure tasks are appropriately distributed. It includes cybersecurity roadmaps, fostering a cybersecurity culture, and updating cybersecurity awareness.
4. **Governance and data:** In this workstream, guidelines are created through dedicated task forces to establish clear roles in each department. The focus is on reviewing operations and enhancing the cybersecurity of the MOH.
5. **Critical Information Infrastructure (CII) ownership:** This workstream ensures the ownership of critical information infrastructure by complying with codes of practice and involving relevant stakeholders.
6. **Patient engagement:** The final workstream involves developing operational guidelines to effectively communicate with patients affected by personal data breaches. This enhances patient understanding and engagement.

Collectively, these workstreams contribute to the continuous enhancement of cybersecurity in the healthcare system. They safeguard patient data and ensure the system's resilience against cyber threats.

Policy revisions from government of Singapore.

- **Healthcare IT Security Policy and Standards (HITSPS):** An enhanced version of the Healthcare IT Security Policy and Standards (HITSPS V4) was released for enhanced cyber safety.
- **Cybersecurity Incident Reporting Framework:** Cybersecurity Incident Reporting Framework (V1) for PHIs was published.
- **Establish a Cybersecurity Risk Management Framework:** A new cybersecurity risk management framework was developed to ensure an appropriate methodology is adopted by all PHIs for regular monitoring of identified cybersecurity risks.
- **Cybersecurity Model with 3 Lines of Defence, which includes:**
    - IHiS, now Synapxe established the Cyber Defence Group (CDG) to oversee public healthcare's cybersecurity policy, governance, risk management and compliance.
    - CDG will perform the second line of defence for cybersecurity compliance and assurance, and regular reviews of both clusters' and national systems' compliance with HITSPS V4.
    - MOHH GIA's role as third line of defence has been formalised.
- **Cybersecurity TableTop Exercise (TTX) and Cyber Range Training:**
    - Scenarios will be developed with input from CSA to assess staff's familiarity with the Incident Response Plans and Playbooks.
    - The TX will be augmented with hands-on Cyber Range training for the Computer Emergency Response Team (CERT) to assess team's response in detecting, responding and recovering from simulated cybersecurity attacks in an environment to resemble a cluster's network.
- **Communications with Private Sector Providers:** A cybersecurity advisory was sent to licensees on Cybersecurity best practices arising from the recommendations in the COI report.

Cybersecurity awareness initiatives

Some of the cyber security awareness and outreach initiatives implemented after the 2018 cyberattack were:

- **Cybersecurity Training Roadmap:** A comprehensive Cybersecurity Training Roadmap has been meticulously designed to ensure the thorough and effective coverage of mandatory cybersecurity training for all staff levels within the public healthcare sector. This initiative encompasses a diverse range of roles, including IT professionals and security specialists. The roadmap is thoughtfully structured to cater to the specific needs and responsibilities of each staff tier, promoting a robust understanding of cybersecurity protocols and best practices.
- **Launch of Advanced and Specialised Cybersecurity Training:** Specific roles, such as data administrators, penetration testers, incident responders, and digital forensics personnel, have access to advanced and specialised cybersecurity training.
- **Mandatory Cybersecurity Awareness Training:** IT staff are required to undergo mandatory cybersecurity awareness training.
- **Introduction of Cybersecurity Training for Senior Executives and Board Members:** This training initiative aims to heighten awareness among senior executives and board members about personal cyber risks in addition to corporate threats.
- **Strengthening Cybersecurity Culture:** Intensified efforts are being made to enhance cybersecurity awareness among staff. Engagement activities and programs are being implemented to bolster the cybersecurity readiness culture, supported by key employee traits, which include:

Changes implemented after the cyberattack

- No more use of thumb drives or Dropbox; documents are now stored in Microsoft OneDrive.
- Messaging about patients no longer happens via WhatsApp; TigerConnect or Microsoft Teams is used.
- Email separation on mobile devices and laptops (Work vs Personal) using Mobile Device Management.
- External data collection through Forms.sg.
- Email screening with Data Loss Prevention (DLP) software.
- Annual Cyber and Data Protection training; signing of Terms of Use agreement.
- Yearly phishing exercises.
- Implementation of a Virtual Browser, providing protected internet access.
- Adherence to Healthcare Instruction Manual [9] for Data Management and ISP compliance.
- System owners of IT systems (not under central management) hold responsibility.
- All new potential equipment requires assessment by IT (Internet of Things); approval from the G7 group.

Lessons for Thailand

Transforming the current healthcare system into a digital one is a significant challenge. Among the various challenges in the development of digital health, data security stands out as a key concern. Data security plays a crucial role in instilling confidence in the utilisation of digital health services. To

effectively address this challenge, systematic education and meticulous planning are imperative. Measures must be undertaken, including establishing a secure and dependable data storage system, formulating government policies, enhancing the knowledge and skills of relevant personnel, and adopting modern equipment for implementation.

The construction of a robust and secure digital health system for the future demands a comprehensive strategy and precise execution. This plan encompasses aspects like data authentication, privacy, and compliance. Additionally, it entails nurturing a proficient workforce capable of managing digital systems. The integration of modern equipment and technology is essential to ensure the efficient and secure utilisation of digital health services. All these elements play a vital role in establishing a resilient and robust digital health ecosystem for the future.

Conclusion

In conclusion, this study visit to Singapore provided invaluable insights and opportunities for collaboration in further advancing telemedicine in Thailand. The challenges faced by Thailand in achieving universal telemedicine adoption, including technological disparities and internet connectivity issues, are significant but not insurmountable. Through strategic planning and drawing from the experiences of countries like Singapore, Thailand can chart a path towards a more robust digital health landscape. Lessons learned from Singapore's successes and challenges can undoubtedly help the development of an efficient and accessible telemedicine program in Thailand.

References

1. Earn, L.C. *International Health Care System Profiles: Singapore*. 2020 25/07/2023]; Available from: https://www.commonwealthfund.org/international-health-policy-center/countries/singapore.
2. How, C.H. and K.M. Fock, *Healthcare in Singapore: the present and future.* Singapore Med J, 2014. **55**(3): p. 126-7.
3. International Trade Administration.. *Singapore - Country Commercial Guide*. 2021 25/07/2023]; Available from: https://www.trade.gov/country-commercial-guides/singapore-healthcare.
4. Singapore - Country Commercial Guide. Available from: https://www.trade.gov/country-commercial-guides/singapore-healthcare.
5. Synapxe. Available from: https://www.synapxe.sg/.
6. Health Sciences Authority. *Regulatory Guideline for Telehealth Products*. 2019.
7. TRUST. Available from: https://trustplatform.sg/.
8. Health Promotion Board. *About us*. [cited 2023 20/07]; Available from: https://hpb.gov.sg/about/about-us.
9. Chia, Y.M.F., et al., *Disparity Between Indications for and Utilization of Implantable Cardioverter Defibrillators in Asian Patients With Heart Failure.* Circ Cardiovasc Qual Outcomes, 2017. **10**(11).

Annexes

Annex 1: Agenda

The detailed agenda for the study visit can be found below

Date	Time	Program/Topic	Venue
Wed, **2 Aug (Day 1)**	05:30 AM	Meet at Suvarnabhumi Airport - Thai Airways Flight: TG403 - Departure time: 08:00 AM	Suvarnabhumi Airport, Thailand
	11:15 AM	Arrive at Changi Airport, Singapore	Changi Airport, Singapore
	12:30 PM	Transfer to Harbourfront Centre	
	01:00-02:30 PM	Lunch at Black society	Black society, 1 HarbourFront Walk, #02-156/157, Singapore 098585
	02:30-03:00 PM	Transfer to Chief Health Scientist Office (CHSO)	
	03:00-05:00 PM	Visit to **CHSO** - Sharing of **TRUST Platform** by Ms Koh Mingshi (Director, CHSO, MOH)	Harbourfront Centre, 1 Maritime Square (Lobby A), #12-10, Singapore 099253 Meeting Room 12-1
	05:00-06:00 PM	Transfer to Crystal Jade Pavilion (VivoCity)	
	06:00-07:30 PM	Dinner at Crystal Jade Pavilion (VivoCity) with SPH	Crystal Jade, 1 HarbourFront Walk, #01-112, Singapore 098585
	07:30 PM	Transfer to hotel and time at leisure	Park Avenue Rochester
Thu, **3 Aug (Day 2)**	07:45 AM	Meet at hotel lobby	Park Avenue Rochester
	07:50-08:30 AM	Transfer to IHiS	
	08:30-10:00 AM	Visit to **IHiS** - Discussion on Health Cybersecurity	6 Serangoon North Avenue 5, 01-01/02, Singapore 554910
	10:00-11:00 AM	Transfer to Health Regulation Group (HRG)	
	11:00-12:00 PM	Visit to **HRG** Meeting with Assoc Prof Raymond Chua, Deputy-Director of Health, **Health Regulation Group**, MOH Singapore - Regulator for telemedicine - Potentially new legislation and health information bill	Meeting Venue: Harbourfront Centre, Level 9 Boardroom, Lift Lobby C, 1 Maritime Square, Singapore 099255
	12:00-01:00 PM	Transfer to Tuan Yuan Restaurant	
	01:00-03:00 PM	Lunch at Tuan Yuan Restaurant	Tuan Yuan Restaurant, 127 Kim Tian Rd, #01-01, Singapore 160127
	03:00-03:30 PM	Transfer to Health Promotion Board (HPB)	
	03:30-05:00 PM	Visit to **HPB**	Health Promotion Board, Level 3 Inspire Room, 3

Date	Time	Program/Topic	Venue
		- Discussion on Digital methods for health promotion - HPB to share on PPH strategy and related initiatives/partnerships HPB has embarked on to tackle key health risks and behaviours - Collaboration opportunities and future	Second Hospital Ave, Singapore 168937
	05:00-06:00 PM	Transfer to Long Beach DEMPSEY	
	06:00-07:30 PM	Dinner at Long Beach DEMPSEY	Long Beach DEMPSEY, 25 Dempsey Rd, Singapore 249670
	07:30 PM	Transfer to hotel and time at leisure	Park Avenue Rochester
Fri, **4 Aug (Day 3)**	08:15 AM	Check out and meet at hotel lobby	Park Avenue Rochester
	08:30-09:00 AM	Transfer to National University Hospital (NUHS)	
	09:00-09:45 AM	*Visit to **NUHS** - Observe the use of digital health in the frontline and their security system (cybersecurity)	NUHS Tower Block Level 13 Boardroom, 1E Kent Ridge Road, Singapore 119228
	10:00-10:30 AM	Visit to **National University Heart Centre, Singapore (NUHCS)** - Observe the use of digital health in specialist services	
	10:30-11:30 AM	Visit to **Tahir Foundation** - Observe AI assistant for Emergency Call Center	
	11:30–12:00AM	Transfer to Changi Airport	
	12:00-01:30 PM	Lunch at PUTIEN Jewel Changi Airport	PUTIEN Jewel Changi Airport, 78 Airport Boulevard, #02-249, Jewel, 78 Airport Blvd., #02 - 249 Singapore Changi Airport, Singapore 819666
	01:30 PM	Check-in at Changi Airport - Thai Airways Flight: TG414 - Departure time: 15:55	Changi Airport, Singapore
	05:15 PM	Arrive at Suvarnabhumi and travel home	Suvarnabhumi Airport, Thailand

Annex 2: List of participants

The list of participants who attended this study visit are as follows.

No.	Name	Organisation
1	Dr. Sopon Mekthon	Ministry of Public Health
2	Dr. Pongsathon Pokpermdee	Ministry of Public Health
3	Dr. Piya Hanvoravongchai	the National Health Foundation
4	Dr. Withita Jangiam	Samut Sakhon Provincial Public Health Office
5	Dr. Supharerk Thawillarp	Ministry of Public Health
6	Ms. Aree Moungsookjareoun	World Health Organization (WHO)
7	Dr. Wanrudee Isaranuwatchai	Health Intervention and Technology Assessment Program (HITAP)
8	Ms. Nitichen Kittiratchakool	Health Intervention and Technology Assessment Program (HITAP)
9	Ms. Papada Ranron	Health Intervention and Technology Assessment Program (HITAP)
10	Mr. Thanayut Saeraneesopon	Health Intervention and Technology Assessment Program (HITAP)
11	Mr. Thanakit Athibodee	Health Intervention and Technology Assessment Program (HITAP)
12	Ms. Jiratorn Sutawong	Health Intervention and Technology Assessment Program (HITAP)
13	Ms. Annapoorna Prakash	Health Intervention and Technology Assessment Program (HITAP)