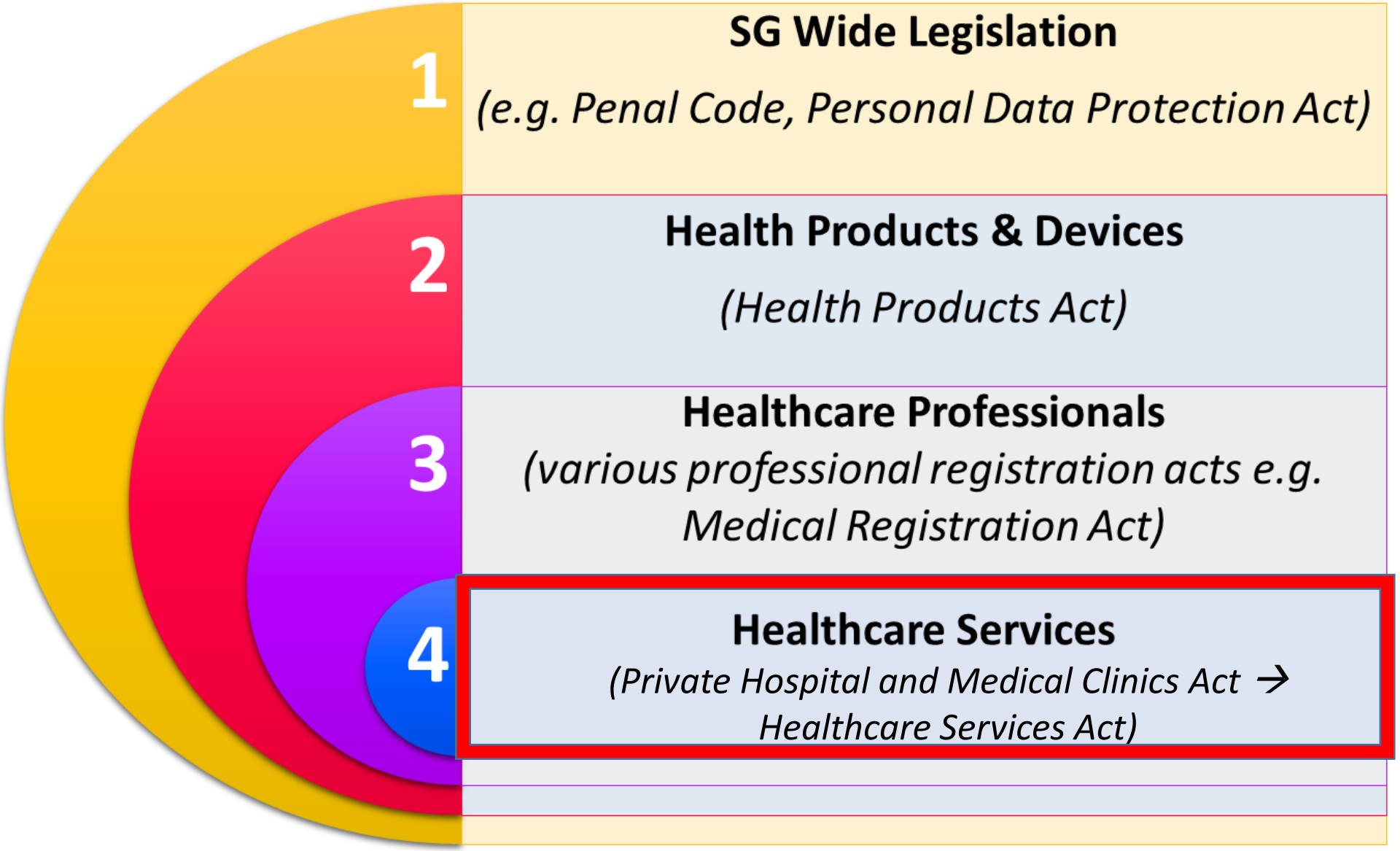
MINISTRY OF HEALTH
SINGAPORE

E-HEALTH REGULATION:
TELEMEDICINE, ARTIFICIAL INTELLIGENCE & CYBERSECURITY

30th EPSO-Conference
21 May 2021

Mr Praveen Raj Kumar
Senior Assistant Director | Health Regulation Group | MOH Singapore

We take a layered and coordinated approach to health care regulation



MINISTRY OF HOME AFFAIRS

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

HSA Health Sciences Authority

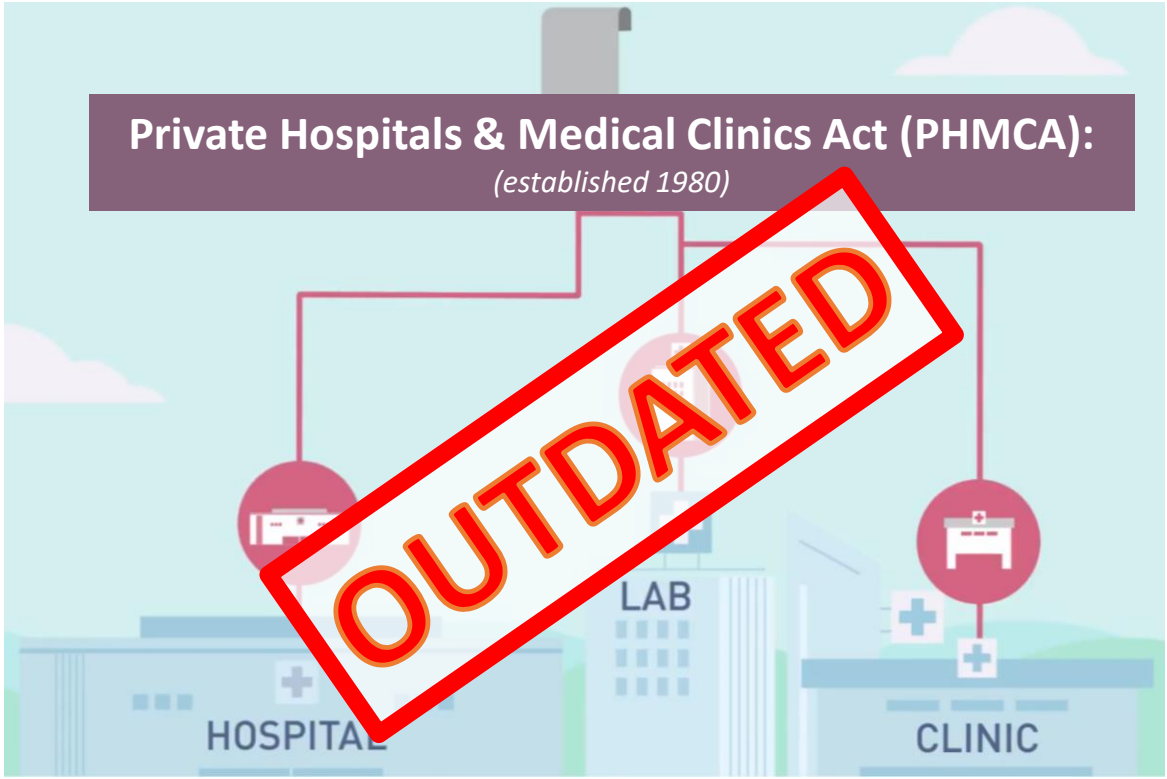
SINGAPORE MEDICAL COUNCIL

SINGAPORE PHARMACY COUNCIL

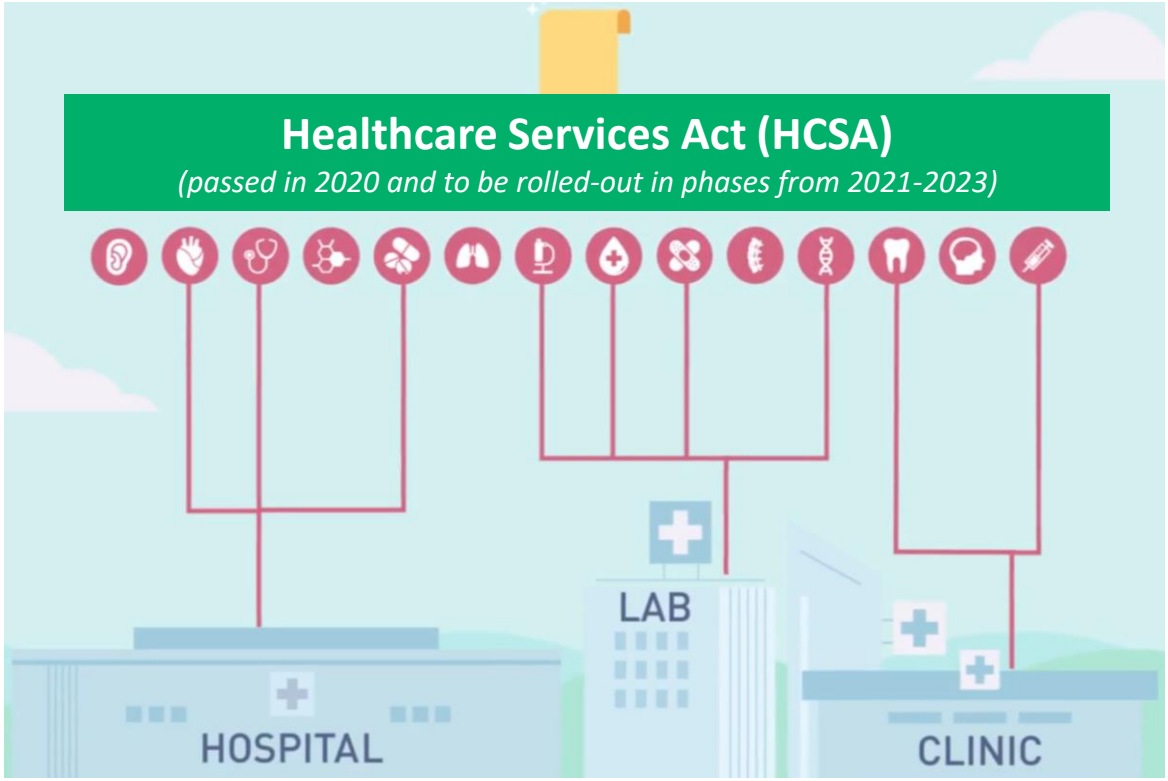
AHPC ALLIED HEALTH PROFESSIONS COUNCIL

MINISTRY OF HEALTH SINGAPORE

We are changing how we regulate healthcare services



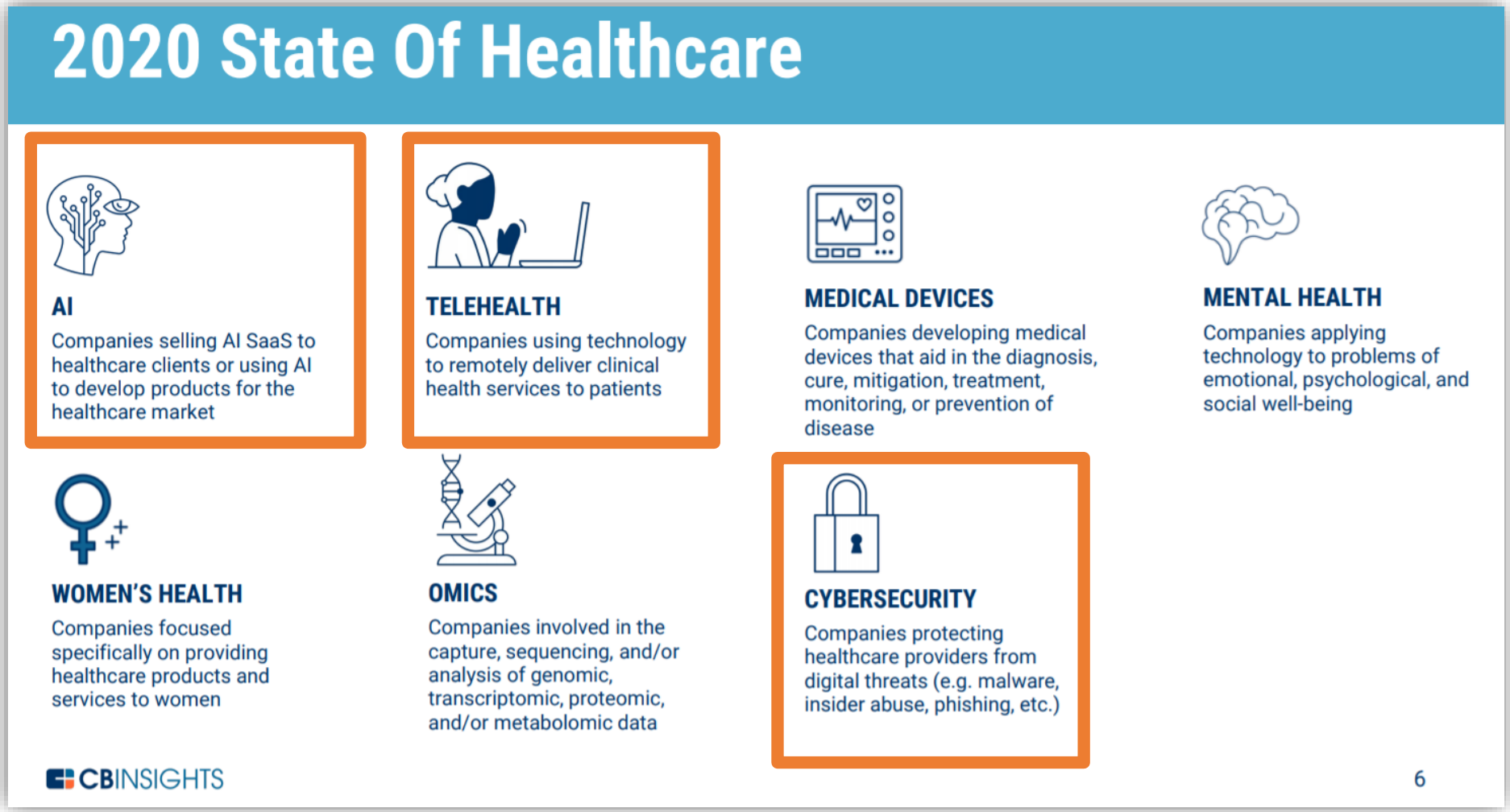
- **Fixed premises-based licences** which cannot be customised
- **Not 'future-proofed'** – *for advances in med-tech/services*
- **Not 'digitally ready'**



- **Services-based** – *including those delivered across multiple sites*
- **Modular and flexible**
- **Enhanced governance** – *to safeguard patient safety and welfare*

The Healthcare landscape is increasingly digital

"Following the money" is one of the tools we use to help us better predict healthcare trends. Several market watchers report significant investments in digital health:



We use several legislative and non-legislative tools to address these digital health trends

Regulatory Tools

Low Patient Risk → High Compliance Burden

	Stakeholder Education	Industry Self-Regulation	Guidelines / Standards	Regulatory Sandbox	Accreditation	Regulations/ Legislations
Telemedicine	**Empowering Consumers to use Telemed safely** *(website, sponsored ads, SEM)*		**2015 National Telemedicine Guidelines**	**Telemedicine Sandbox** *(Completed)*		**Licensing Telemedicine under HCSA ~2022/3**
Artificial Intelligence	**Ongoing engagements with** healthcare providers		**2021 Artificial Intelligence Healthcare Guidelines (AIHGle)**	**(TBC) Artificial Intelligence Sandbox**		**Software-As-A Medical Device regulated by Device Regulator**
Cybersecurity	**Upskilling healthcare service providers** *(engagements, e-trainings)*		**2021 Cybersecurity Essential Guidelines**			**(TBC) Enforceable Cybersecurity Standards**

We are ensuring the safe growth of telemedicine through several regulatory tools

Regulatory Tools

Low Patient Risk → High Compliance Burden

	Stakeholder Education	Industry Self-Regulation	Guidelines / Standards	Regulatory Sandbox	Accreditation	Regulations/ Legislations
Telemedicine	**Empowering Consumers to use Telemed safely** *(website, sponsored ads, SEM)*		**2015 National Telemedicine Guidelines**	**Telemedicine Sandbox** *(Completed)*		**Licensing Telemedicine under HCSA ~2022/3**
Artificial Intelligence	**Ongoing engagements with** healthcare providers		**2021 Artificial Intelligence Healthcare Guidelines (AIHGle)**	**(TBC) Artificial Intelligence Sandbox**		**Software-As-A Medical Device regulated by Device Regulator**
Cybersecurity	**Upskilling healthcare service providers** *(engagements, e-trainings)*		**2021 Cybersecurity Essential Guidelines**			**(TBC) Enforceable Cybersecurity Standards**

Telemedicine (TM) - A growing space with patient safety risks

Background

- **Context: ~2017; appearance of several standalone TM providers** offering "first consultations" with risks.
    - E.g. Patient authentication, treatment protocols, medication management, data/cyber security

- While doctors providing telemedicine are regulated, **the service itself is unregulated** (*not premises-based*).

- **Outcome:** We want TM to be a useful and safe part of the healthcare landscape & will be licensing it under HCSA in ~2022/23.

- To regulate, we needed to **better understand the practices and risks.**

Telemedicine (TM) - A growing space with patient safety risks

Sandboxing TM

- A safe space for us to work with providers to **co-create effective and efficient regulations.**
  - Put **safe-growth parameters** for providers & **test regulations** for burden & efficacy.

- Sandboxed **11 private providers from 2018-2021**, and collected >40K points of teleconsult data → **assessed providers**' clinical governance, leadership, financials, data-handling, etc.

In a regulatory sandbox with
MINISTRY OF HEALTH
SINGAPORE

What we found

- **Telemedicine is generally safe for patents with mitigations in place:**
  - No major patient safety issues / complaints / data breaches reported.
  - Little difference in utilisation rates (a proxy for patient safety) of public healthcare between TM and non-TM comparable patient profiles.

Key learnings from our Sandboxing experience

1. Do doctors understand the uses and limitations of TM?
2. Which modality of TM should doctors use (video, audio, text)?
3. How should inbound / outbound TM be managed?

Clinical

4. Do patients understand the limitations of TM?
5. How to ensure standards are maintained for medication prescription and delivery?
6. What if a patient collapses mid-way during the consult?

Technical

7. How are clinical records stored?

Key Question: What has been your TM regulatory experience? How do you upskill your inspectors for TM?

1 Do doctors understand the uses and limitations of TM?

Issues & Risks

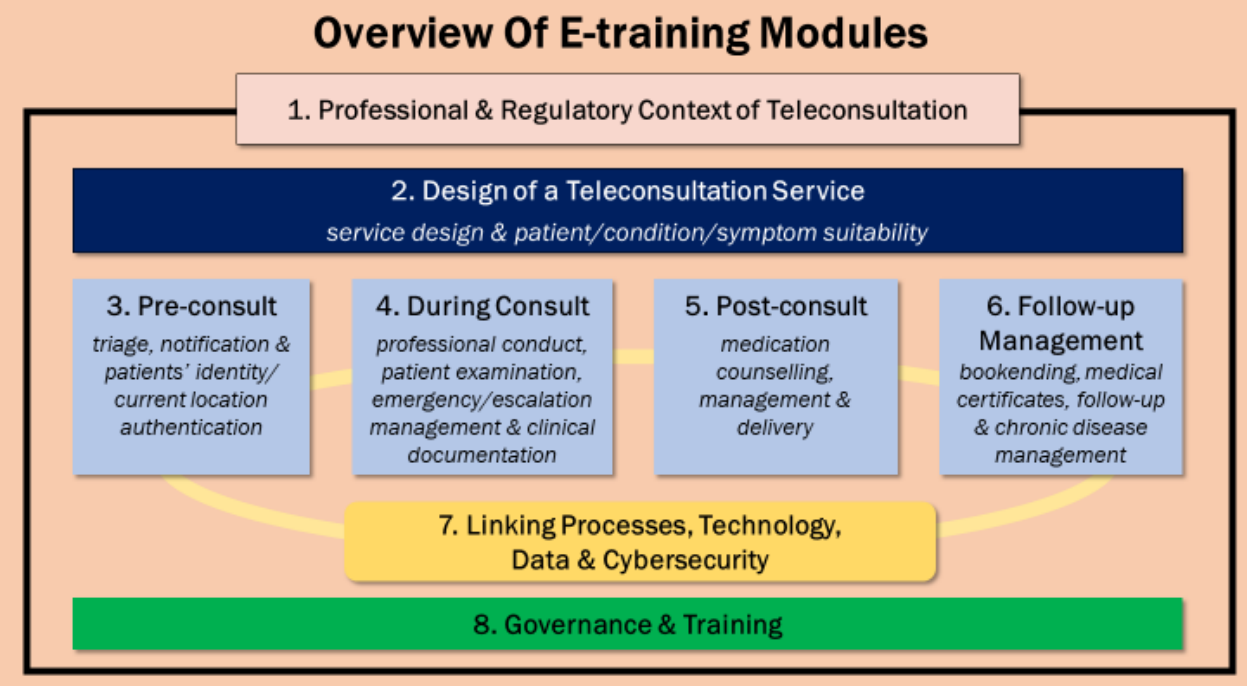
- Doctors have an **uneven understanding** of how to use TM safely.
- **Only broad TM guidance from the Singapore Medical Council –** relying on professional judgement.
- **Uneven understanding + unclear guidance = variable application** of TM leading to patient safety issues (e.g. types of patients that can be safely seen via telemedicine, triage, escalation, meds).

Our Guidance

- The need for clear **governance, professional, process and technical guidance** to support the safe delivery of TM

Distilled Sandbox Learnings into a free E-training

- Launched March 2020 - 2hr online training supplemented with scenario questions.
- Helps doctors (primarily) **better understand safe use, limitations and implementation when designing and delivering TM.**
- Completed by ~6,900 doctors/dentists nurses, allied health professionals, platform developers and admins (>90% positive feedback).



2 Which modality of TM should doctors use (video, audio, text)?

Issues & Risks

- Doctors have an **uneven understanding** of which TM modalities to use.
- **No specific guidance from the Singapore Medical Council.**
- Risk/issues such as **using text-based first consults** with new patients.

Our Guidance

- Given our internet connectivity and mobile phone penetration rates, synchronous (i.e. **'live') video consults should be the gold standard** and essential for first-consults.
- Enables **better assessment of key visual cues, patient authentication and therapeutic presence.**

	Simple acute conditions/symptoms	Specialist (including chronic) conditions*
First consultations (i.e. new or referred patients, or known patients presenting with new conditions/symptoms)	✓ VIA "LIVE" VIDEO CONSULTATIONS	✗
Follow-up consultations	✓	✓
	VIA ANY TELEMODALITY DEEMED APPROPRIATE BY DOCTOR	

**First consultations with specialists should be done in-person. The nature of the condition will require in-person examination, diagnostic or confirmatory investigational tests prior to determining if teleconsultation is appropriate.*

3 How should outbound / inbound TM be managed?

Issues & Risks

- **TM reduces barriers to care and allows doctors to see patients in different jurisdictions** – both inbound and outbound.
- Lack of parity in understanding could **lead to legality issues and patient safety risks.**

Our Guidance

Outbound

- Doctors in Singapore **can teleconsult with patients in other countries**, and when they do so, they are expected to **abide by the same standards as applicable locally.**
- They should also **check and abide by rules/regulations of countries that patients reside in.**
- Ideal to **tele-collaborate with patients' primary doctor** located in same country as patients.

Inbound

- **Overseas doctors must be registered locally.**
- **Prescriptions, medical certificates from overseas doctors are not recognised** in Singapore.
- Foreign clinics/doctors are encouraged to **collaborate with a locally-registered doctor to ensure care is safe, contextualized, and appropriate.**
- Reality:
  - Recognise that we have **limited levers;** and
  - **Leverage on consumer education** to mitigate risks.

Key Question: How have you managed/controlled the risks of cross-border telemedicine provision?

Next Steps for Telemedicine

- Completed and **closed the Sandbox in Mar 2021.**

- Recognised the growth of TM in 2020 (COVID-19) and transitioned to a **Voluntary Listing of Direct TM service providers - ~700 listed providers to-date:**
  - Helps patients make an informed choice when choosing TM providers.
  - Interim measure prior to HCSA licensing (~2022/23).
  - To be listed, providers need to complete the e-training and agree to a set of compliance statements (e.g. modality, patient notifications, escalation protocols, med mgmt.).

- **Consulting stakeholders on draft TM regulations in ~2022** prior to licensing.

- **Raising patient awareness** on using TM safely via consumer education.

- Working on **specialty-specific guidance.**

Key Questions:
- **What has been your TM regulatory experience?**
- **How do you upskill your inspectors for TM?**

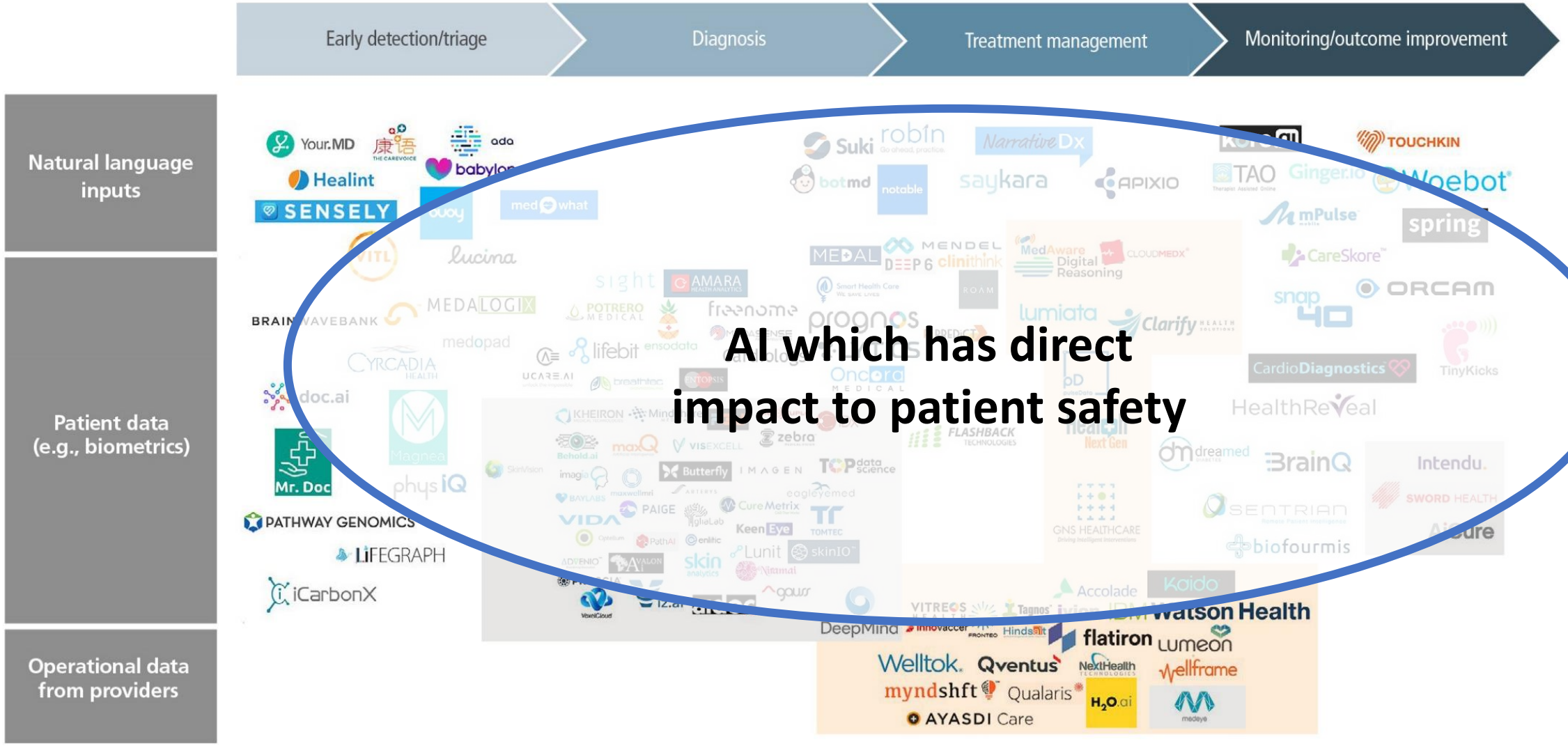
We are proactively addressing the rapid developments & implementation of AI in healthcare

Regulatory Tools

Low Patient Risk → High Compliance Burden

	Stakeholder Education	Industry Self-Regulation	Guidelines / Standards	Regulatory Sandbox	Accreditation	Regulations/ Legislations
Telemedicine	**Empowering Consumers to use Telemed safely** *(website, sponsored ads, SEM)*		**2015 National Telemedicine Guidelines**	**Telemedicine Sandbox** *(Completed)*		**Licensing Telemedicine under HCSA ~2022/3**
Artificial Intelligence	**Ongoing engagements with** healthcare providers		**2021 Artificial Intelligence Healthcare Guidelines (AIHGle)**	**(TBC) Artificial Intelligence Sandbox**		**Software-As-A Medical Device regulated by Device Regulator**
Cybersecurity	**Upskilling healthcare service providers** *(engagements, e-trainings)*		**2021 Cybersecurity Essential Guidelines**			**(TBC) Enforceable Cybersecurity Standards**

Artificial Intelligence (AI) – appearing throughout our care system



Note: Many companies span multiple stages of the patient journey or data types, therefore relative positioning is indicative

Source: L.E.K. research

Core competency in clinical pathway optimization

Core competency in image analysis

While there are system benefits, there are risks

- **AI Medical Devices (AI-MDs) are regulated by our device regulator (Health Sciences Authority)** i.e. those which treat, diagnose, assess and monitor patients.
- However there has been **no contextualized guidance on implementation risks.**

HSA Health Sciences Authority

MINISTRY OF HEALTH SINGAPORE

Risks

AI-MD

- AI-MD which treat, diagnose or manage care are regulated by HSA under the Health Products Act.
- HSA ensures the quality, safety and efficacy of AI medical devices

Process

Accountability

Algorithm

Data

Implementation

- **No contextualized guidance on how to implement and use AI-MD safely in healthcare**
- **Requires partnership between developers and implementers** to ensure safe deployment and risk mitigation.

Note: Risks have been modified from Ernst & Young's 4 risks of AI

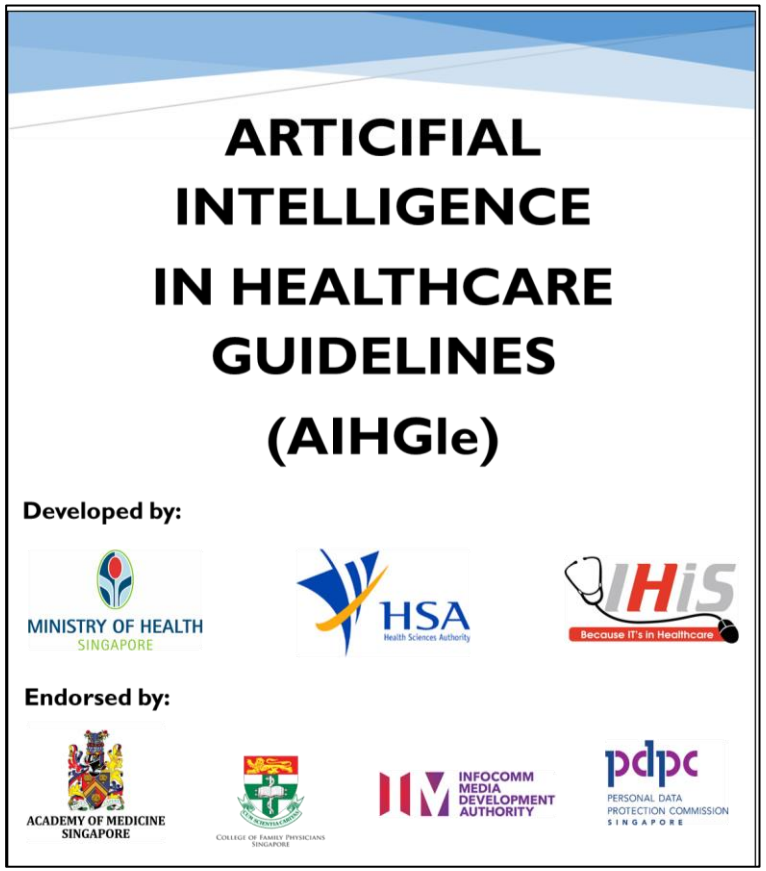
Developed AI in Healthcare Guidelines (AIHGle) to supports the safe growth of AI

Objectives of the AIHGle *("Agile")*

- **Recommendations for <u>developers</u> and <u>implementers</u> to ensure basic safety** for AI in clinical healthcare settings, based on key principles (fairness, responsibility, transparency, explainability, patient-centricity).
  - Both groups are not mutually exclusive
  - Guidance also applies to in-house developed AI-MDs

Features

- **Non-legislative**, and complements HSA's current AI-MD regulatory requirements.
- Focuses mainly on **higher-risk clinical use AI (i.e. AI-MDs),** but applicable to other AI in healthcare (e.g. research, training, administration).
- **A 'living document'** to be periodically refined updated to incorporate good practice.



The Guidelines cover various aspects of AI-MD development and implementation

- **Clear responsibilities between developers and implementers**
- **Clinical input for AI-MD development**
- End-user inputs for holistic development of AI-MD
- Develop an understanding of current clinical practice baseline
- Fair and Representative AI-MD Training Datasets
- Achieving sufficient explainability of AI-MD
- Validation of AI-MD performance
- Clinical governance for AI-MD implementation
- **Transparent end-user (e.g. medical practitioners, patients) communications on their interactions with AI-MD**
- Post-deployment monitoring & review of AI-MD
- Emerging developments in AI (e.g. continuous learning AI-MD, synthetic data).

Service Level Agreements (SLAs) help to set clear responsibilities between developers and implementers

WHY?

- **Unclear ownership and responsibility over different aspects of development and implementation** of AI-MD.
  - E.g. No clear apportioning of responsibilities when there are adverse events, or patient safety compromised

DESIRED OUTCOME

- Establish **mutually-agreed responsibilities between developers and implementers** to mitigate possible issues arising from development, implementation and deployment of AI-MD.

HOW?

- **Establish Service Level Agreements (SLAs) between developers and implementers**:

Design *e.g. seeking clinical inputs relevant to AI-MD's intended use, relevance of training datasets, setting performance baselines.*	**Build** *e.g. documentation of AI-MD development protocol and reference standards.*	**Test** *e.g. evaluation and validation of AI-MD model to ensure patients would be "no worse off".*
Use *e.g. appropriate approval authority for implementing AI-MD, operational workflow and staff training.*	**Monitor** *e.g. "ground-truthing" of AI-MD's performance, consistent and continued performance evaluation.*	**Review** *e.g. ad-hoc review of patient safety issues, annual performance review.*
	Intellectual Property (IP) *e.g. access to specific info on algorithmic design.*	

Clinical input is necessary for AI-MD development

WHY?

- **Unclear if/how clinical inputs are sought in the development phase.**
  - Lack of clinical input may result in poor design and failed implementation.

HOW?

- **Developers should take ownership over the clinical inputs obtained** for the development of the AI-MD.
  - An **AI-MD development team should include clinicians (or relevant domain experts)** to guide and lead the seeking of the necessary clinical inputs.

DESIRED OUTCOME

- Developers should obtain clinical inputs from **individual(s) with relevant expertise on areas such as:**
  - **Clinical problem statement** e.g. clarity on the issues, intended use, baselines, patient inclusion/exclusion criteria, possible clinical workflows.
  - **Data representativeness** e.g. demographics, clinical context, existing biases, appropriate input type (image, text, numbers).
  - **Algorithm testing approach** e.g. input quality (e.g. type & resolution of images), "boundary conditions" between valid/invalid input e.g. (between patient inclusion/exclusion criteria).
  - **Identifying causal relationships between inputs and outputs of the AI-MD**.
  - **User manual** e.g. alignment with AI-MD's clinical intended use.

End-users should be aware that they are interacting with an AI-MD

WHY?

- End-users **may be unaware/unsure of what to expect when they are interacting with an AI-MD.**
- Developing awareness and understanding are important to **build 'end-users' trust in the AI-MD.**

DESIRED OUTCOME

- End-users are **clearly made aware that they are interacting with an AI-MD** and have **sufficient information to make informed decisions.**
  - E.g. whether clinicians should continue the use of an AI-MD, or patients meet the inclusion/exclusion criteria and consider seeking in-person care instead.

HOW?

Suggested information that should be communicated to end-users:

Type of End-User	Suggested Information
Medical Practitioner	• Clarity that they are **interacting with** an AI-MD • **Limitations** of the AI-MD (e.g. inclusion/exclusion criteria (if required) • **Date of most recent AI-MD audit** *(audit will be covered later)* • **Contact person** for healthcare institution to obtain specific AI-MD performance info if required
Patient	• Clarity that they are **interacting** with an AI-MD • **Limitations** of the AI-MD (e.g. inclusion/exclusion criteria (if required) • **Name of the healthcare institution** that is using the AI-MD (for accountability) • **Contact person** for healthcare institution in case of adverse events, questions on using the AI-MD, or to seek in-person care

Next Steps – Publishing and Disseminating

- **Targeting to publish the AIHGle** in later 2021.
- **Continue engaging stakeholders** (healthcare providers, developers, Gov Agencies) to understand the efficacy and value of the guidelines, and how to help them implement in their development pathways.
- This document will be **continuously updated** as the sector develops.
  - E.g. synthetic data sets, continuous learning AI-MD.
- Explore if we want to **sandbox the governance controls for AI in healthcare institutions.**

Key Questions:

- **Have you considered regulating AI in healthcare as a service? Why/Why not? What is your threshold for regulating?**
- **Which kinds of risks, stakeholders, and contexts have you considered?**

Across the digital healthcare landscape, we also need to manage cybersecurity risks

Regulatory Tools

Low Patient Risk → High Compliance Burden

	Stakeholder Education	Industry Self-Regulation	Guidelines / Standards	Regulatory Sandbox	Accreditation	Regulations/ Legislations
Telemedicine	**Empowering Consumers to use Telemed safely** *(website, sponsored ads, SEM)*		**2015 National Telemedicine Guidelines**	**Telemedicine Sandbox** *(Completed)*		**Licensing Telemedicine under HCSA ~2022/3**
Artificial Intelligence	**Ongoing engagements with** healthcare providers		**2021 Artificial Intelligence Healthcare Guidelines (AIHGle)**	**(TBC) Artificial Intelligence Sandbox**		**Software-As-A Medical Device regulated by Device Regulator**
Cybersecurity	**Upskilling healthcare service providers** *(engagements, e-trainings)*		**2021 Cybersecurity Essential Guidelines**			**(TBC) Enforceable Cybersecurity Standards**

Data protection and promotion of cyber hygiene

Background

- Accelerating **digital transformation** in the healthcare sector:
  - Systems increasingly interconnected with personal/medical data shared across healthcare providers to support care continuity.
- **Cyber threats** increasing in scale and sophistication across all sectors:
  - With healthcare being an even more attractive target for hackers.
  - Personal health information *50x more valuable* than financial information on the black market.
- **Protecting and securing healthcare data** is critical:
  - Important part of managing clinical risk and upholding patient safety and welfare.

What we have done so far

- **To support the healthcare sector,** we are launching the **Cybersecurity Essentials Guidelines in the coming months**, which are intended as a basic set of endpoint cybersecurity guidelines **for <u>all healthcare licensees:</u>**
  - Measures recommended are intended as baseline cyber hygiene, pitched at safeguarding the IT set-up of a small healthcare entity (e.g. standalone GP clinic).
  - Designed to take into account implementation feasibility.
  - For healthcare licensees, this may be translated into enforceable standards in future.
- Additional guidelines ("**Cybersecurity Enhanced+ Guidelines**") will be shared in the later part of this year and is catered for mid-to-large licensees with more complex IT set-ups and more endpoints.

What is the Cybersecurity Essentials Guidelines about?

1 **Know what needs to be secured**

Manage your IT assets – *know what you store digitally and where*

2 **Implement measures to secure data, detect, respond to and recover from breaches**

Considerations

- **Technical** – *admin & user access, security, audit logs, backups*
- **Procedural** – *vendor mgmt., incident reporting*
- **Manpower** – *cybersecurity awareness*

3 **Put measures into practice**

Translate guidelines into organisational policies - *for employees and vendors, to ensure consistency in practice*

What is the Cybersecurity Essentials Guidelines about?

Create and maintain an updated inventory of all IT assets
Count and list all IT assets connected to the corporate IT network, including hardware, software and medical devices with network connectivity

1. Restrict **administrator privileges** so as not to give attackers privilege rights to compromise systems
2. Choose systems with **multi-factor authentication** functionality to ensure authorised access
3. Update **security patches** regularly to reduce system-known vulnerabilities
4. Deploy **anti-malware** protection to mitigate the risk of malware infection
5. Secure your **network perimeters** to restrict all unauthorised network traffic
6. Monitor and review **audit trails and security logs** for unauthorised access
7. Perform **regular backups** of all critical data and systems to protect against unexpected data loss
8. Develop **outsourcing policy** to ensure proper screening and selection of vendors and contractors
9. **Report data breaches** promptly to mitigate the impact and uphold patient confidentiality
10. Raise **security awareness** among employees who access systems and data

Review the Cybersecurity Essentials Guidelines and translate them into **policies and processes** for your organisation

We will continue providing support and work with providers on their baseline cyber hygiene

- Encouraging healthcare providers to **meet all the recommendations** under the Cybersecurity Essentials Guidelines, review their current cybersecurity posture, and **do more to identify gaps if possible**.

- We will also be:
  - Rolling out a **dedicated cybersecurity webpage** on MOH's website.
  - Developing **cybersecurity e-training** as an added avenue to communicate the Cybersecurity Essentials Guidelines.
  - Reviewing if **additional implementation support** can be given to providers to adopt the recommendations.

- **Collecting feedback** from providers on the Guidelines and implementation uptake.

Key Questions:

- **How have you approached crafting your regulatory strategy and scope?**
- **How have you built up expertise to audit cybersecurity compliance?**
- **How are your healthcare providers upskilled with this knowledge and do Governments/inspectorates provide support to do so?**

Key Discussion Questions

1. Telemedicine:

a) What has been your TM regulatory experience? How do you upskill your inspectors for TM?

b) How have you managed/controlled the risks of cross-border telemedicine provision?

2. AI in Healthcare Guidelines:

a) Have you considered regulating AI in healthcare as a service? Why/Why not? What is your threshold for regulating?

b) Which kinds of risks, stakeholders, and contexts have you considered?

3. Cybersecurity:

a) How have you approached crafting your regulatory strategy and scope?

b) How have you built up expertise to audit cybersecurity compliance?

c) How are your healthcare providers upskilled with this knowledge and do Governments/inspectorates provide support to do so?

MINISTRY OF HEALTH
SINGAPORE

Thank You

Praveen Raj Kumar – Praveen_RAJ_KUMAR@moh.gov.sg
Chan Weng Chee - CHAN_Weng_Chee@moh.gov.sg