DO YOUR PART #BECYBERSMART

Healthcare digitalisation has increased personal data collection, exposing users to heightened cyberthreats and intensifying the urgency for data protection in the cyberspace.

APACMED AND CYBERSECURITY

APACMed's Digital Health Cybersecurity Working Group has been devoted to facilitate private-public collaborations in Asia to raise and share knowledge on medical device cybersecurity and advocate for harmonized policy frameworks.

From a newbie in the digital health ecosystem, the APACMed Digital Health Committee is now a recognised player. We provide strategic support to industry stakeholders, share knowledge and expertise, and advise governments. The Committee is proud to collaborate with the ministries of health, cybersecurity agencies and other government organisations as they strive to implement cybersecure healthcare ecosystems.

We've grown from 0 to **300 individual members** from **85 companies** in the last **two years**

APACMed
The voice of MedTech

APACMed

JOURNEY HIGHLIGHTS

FEB 2020

The APACMed Digital Health Cybersecurity Working Group was formed as part of the Digital Health Committee to support the MedTech industry in addressing cybersecurity challenges.

First Industry Consultation
The Cybersecurity working group shared the first Industry Comments and Recommendations on the Singapore's Ministry of Health (MOH)'s Draft Guidelines for Safe Development and Implementation of Artificial Intelligence in Healthcare.

MAR 2020

First webinar on Navigating Cybersecurity Policies and its Intricacies
The group organised a first webinar on the policies that regulate medical device cybersecurity in the US, Europe and Asia Pacific. We discussed the increasing need for harmonisation between these different policies and regulations, and provided insights into how the MedTech manufacturers and companies can operate both regionally and internationally while abiding global policies.

Cybersecurity Keynote at APACMed 2020 MedTech Forum
Stephanie Domas, former Executive Vice President of MedSec, a healthcare cybersecurity company exclusively focused on the unique challenges of protecting medical devices, gave a keynote presentation on Cybersecurity risks, management, and regulations during the APACMed 2020 MedTech Forum. She depicted the divergence between security and safety, provided recommendations on cybersecurity traceability metrics, and explained the risk transference amongst Health Technology Organisations and manufacturers.

JUN 2020

Interview with David Koh, Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency of Singapore
APACMed's Cybersecurity Chair, Jim Sarka, CIO & Vice President, Technology Asia Pacific at Johnson & Johnson, interviewed Mr. David Koh during the APACMed 2020 MedTech Forum. As the Commissioner of Cybersecurity, he has the legal authority to investigate cyber threats and incidents to ensure that essential services are not disrupted in the event of a cyber-attack. Concurrently, as Chief Executive of CSA, he leads Singapore's efforts to provide dedicated and centralised oversight of national cybersecurity functions.

OCT 2020

Mr. Koh gave an overview of Singapore's Cybersecurity Strategy and reiterated the importance of cybersecurity in the health sector. This interview led to an ongoing collaboration between APACMed and CSA.

First landscape of Medical Device Cybersecurity Policies in Asia Pacific
The Cybersecurity group published the first landscape of APAC cybersecurity policies, in collaboration with the consulting firm Accenture. The landscape provides a summary of guidance documents and directives from major global regulatory bodies and represents the first APAC repository of medical device cybersecurity policies for the MedTech companies and other players in the field. The database is updated quarterly.

DEC 2020

First Roundtable discussion with Singapore Government Agencies on Medical Device Cybersecurity Labelling Scheme CLS (MD) initiative
In 2021, the Cyber Security Agency of Singapore (CSA), Ministry of Health (MOH), Health Sciences Authority (HSA), and Integrated Health Information Systems started exploring the development of a Cybersecurity Labelling Scheme (CLS) for medical devices in Singapore to increase their resilience to cyber-attacks. The agencies have worked with APACMed to leverage industry expertise in medical devices and the collaboration is currently ongoing.

JAN 2021

Interview with J&J's Vice President Information Security & Risk Management, Marene Allison
Marene Allison, Vice President Information Security & Risk Management, Chief Information Security Officer at Johnson & Johnson, was interviewed by Christopher Martin, Principal for Policy Transformation & Head of Asia at Access Partnership during the APACMed 2021 MedTech Forum. In a post-pandemic world, cybersecurity became more important than ever. This session highlighted the strategic importance of medical device cybersecurity from multiple angles: manufacturing, hospitals, healthcare professionals, patients and governments.

OCT 2021

CyberStorm – MedTech response to cyberattack
During a cyber-attack, all the divisions of a medical device manufacturing company are impacted and mobilised. At the APACMed 2022 MedTech Forum, we explored their response medical in a Cyber War Game. This includes breach simulation, identification of strengths and weaknesses in company plan, and response readiness within the manufacturer's organization.

SEP 2022

Tips for Medical Device CYBERSECURITY

Cybersecurity is now essential as connectivity for medical devices increases. For medical device manufacturers, it is now easier to monitor device use, offer updates and interact with both patients and clinicians. But having confidential patient data flowing presents significant risks of data breach; taking cybersecurity seriously can help manage that risk. Here are some tips for you.

What is Cybersecurity?

Cybersecurity for a medical device is more than just privacy, it has three main aspects:
Confidentiality – We only want authorised people or systems to be able to read the data
Integrity – We only want authorised people or systems to change the data or perform an action
Authenticity – We want to know that people or systems are who they say they are, and that data comes from genuine sources

To enable these aspects of security we need to **implement authentication**, to prove that an entity is genuine, and **authorisation**, to control what the authorised entity can do or access.

How to Design Cybersecurity?

Identify and record the data that you need to protect – and identify what you need to protect it from.
Assess how serious a breach of confidentiality, integrity or authenticity would be, the likelihood of it occurring and what the greatest risks are.
Protect. Now you can move on to developing ways to ensure your assets are safe.

Remember: Not everything needs to be protected to the same degree.

In terms of the practical efforts that go into your cybersecurity planning, not everything needs to be protected. You need to use a risk-based development process to put the most effort and resources into the highest-risk items.

APACMed
The voice of MedTech

Join the APACMed community to help us shape a more accessible, harmonized, safe and cybersecure MedTech ecosystem.

For more information on our Cybersecurity working group, please contact our
Director for Digital Health **Roberta Sarno** (rsarno@apacmed.org) or
our Assistant Manager for Digital Health **Cindy Pelou** (cpelou@apacmed.org)

Sources:
https://www.med-technews.com/medtech-insights/digital-in-healthcare-insights/10-cybersecurity-tips-for-medical-device-developers/
https://staysafeonline.org/programs/cybersecurity-awareness-month/