



www.pwc.com/sg

IoT proliferation in MedTech

The evolving role of regulators, manufacturers, providers and consumers in a medical IoT ecosystem



A collaborative, data-driven, evidence-based report

Last year in collaboration with Asia Pacific Medical Technology Association (APACMed) and A*STAR, PwC were supporting partners for the first APACMed MedTech & Digital Health workshop. This one-day workshop offered a unique opportunity to explore global and regional trends in Digital Health, as well as engage in discussions around (1) Executing a Digital Strategy while Managing Regulatory and Cybersecurity Constraints, and (2) The Impact of Cybersecurity on Growth and Commercial Strategy. The workshop comprised a combination of panel discussions as well as interactive breakout sessions, facilitated by PwC. The event was of particular relevance to senior regulatory and commercial leaders as well as CIOs, heads of IT and hospital administrators. In this report, we discuss the challenges and concerns associated with connected medical devices and share potential resolution mechanisms for MedTech, regulators and providers.

Urooj Burney

PwC SEAC Cybersecurity & Privacy Impact
Centre Leader

Dr. Zubin J Daruwalla

PwC SEAC Health Industries Leader

With the convergence of technologies, from medical devices and genomics to the internet, the boundaries have also evolved between personalised health performance, population data management, and privatisation of information. We have progressed a long way from our health being managed on an individual basis by interpreting data extracted from different technology platforms. Connectivity of these platforms increases efficiency and enables scalability across populations. Subsequent population sampling improves performance on an individual basis. As we look for better and more personalised care enabled by connectivity, we must also consider the connectivity of the players along the healthcare delivery value chain, from product owners and providers to us.

Sidney Yee

Chief Executive Officer, DxD Hub & Executive Vice President, ETPL

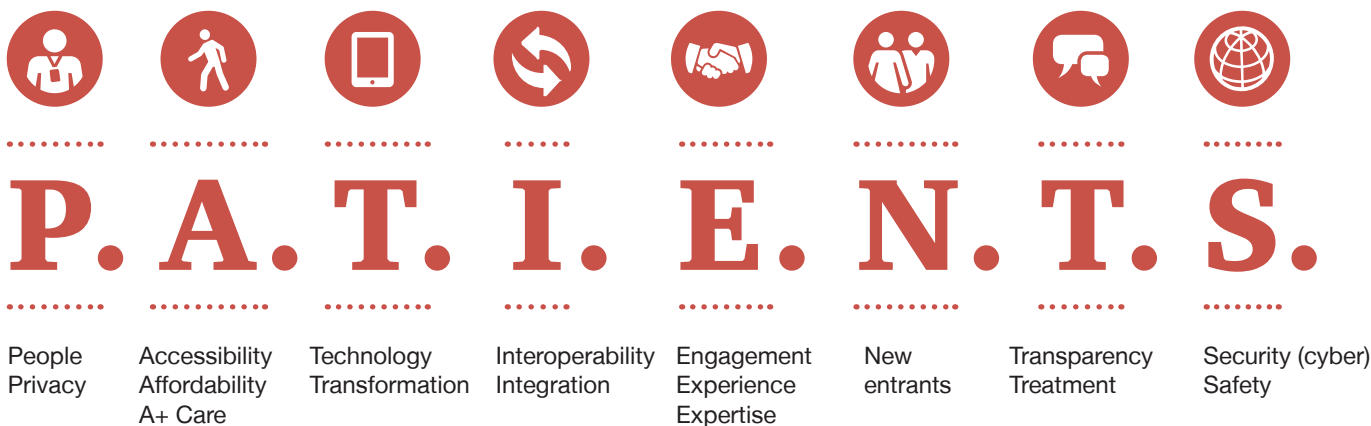
Contents

| | |
|--|-----------|
| Introduction | 4 |
| Understanding the challenges and concerns associated with connected medical device | 6 |
| Regulatory and compliance management | 6 |
| Secure deployment of connected medical devices | 8 |
| Data governance, protection and privacy | 9 |
| Medical device cybersecurity risk landscape – What ails healthcare organizations | 10 |
| Potential resolution mechanisms for MedTech, regulators and providers | 11 |
| The road ahead | 15 |
| Our authors | 17 |

Introduction

In this age of integrated healthcare service delivery, medical devices are becoming more network-connected in order to quickly receive and transmit health information for the treatment and care of patients. Network connectivity, also commonly referred to as the Internet-of-Things (IoT), although beneficial from the consumer experience perspective, presents a new set of privacy and cybersecurity threats to the ecosystem. In the US, the FDA has expressed the challenge stating, “Networked medical devices, like other networked computer systems, can be vulnerable to security breaches.”¹ Unsecured medical devices could translate not only to business interruption and reputational damage risks but more importantly, potential endangerment of patients.

At PwC, we believe that all aspects of care delivery, including the use of connected medical devices should ultimately be patient-centric. Connected devices should be deployed and applied in a manner that ultimately ensures our patients’ privacy, and improves accessibility and the overall patient experience without compromising privacy and security.



¹ FDA. (2018). The FDA's role in Medical Device Cybersecurity - Dispelling Myths an Understanding Facts. Retrieved from US Food and Drug Administration.

The question that arises is how everyone, including regulators, providers, medical device manufacturers, and patients can address the issues and risks. We identify key challenges and steps toward a better prepared and well equipped ecosystem on its transition to an IoT-enabled medical technology environment².

And since failing to prepare equates to preparing to fail, we explore three key factors amongst many that would support the culmination of a state of adequate preparedness:



- **Regulatory and compliance management:** With regulators having limited capabilities for horizon scanning of emerging technologies as well as being constrained by the allocation of resources focused on technology and specifically security, there is lack of clear guidance and standards for MedTech companies and providers. In turn, these organisations focus more on the business of medical devices rather than creating their own internal standards and compliance procedures to drive a more secure product. However, this trend is changing as more MedTech vendors realise the impact of device breaches on their brand and business.



- **Secure deployment of connected medical devices:** Increased vulnerabilities arise due to shared environments and functional and operational responsibilities that are amplified given a lack of regional guidelines. Latent vulnerabilities may also go undetected given an inability to periodically perform integrated ecosystem checks. Lastly, absence of a security culture that drives best practice within MedTech and health provider organisations when it comes to the deployment of these devices only attenuates the aforementioned vulnerabilities.



- **Data governance, protection and privacy:** MedTech companies face capability gaps in safeguarding the devices against data vulnerabilities. These vulnerabilities emerge as the devices are deployed into larger networks through the IoT. As a manufacturer, it becomes increasingly difficult to keep track of deployment use cases as well as the potential threats that result from non-standard deployments or system integrations. Robust data governance, and greater collaboration between manufacturers and providers, especially focused on the deployment use cases, is required on an ongoing basis as the technology environment develops and scales.

² Roundtable findings (2017). APACMed- PwC Digital Health Roundtable

In order to achieve a better prepared and well equipped ecosystem, we believe the following are the five most critical steps³:

- Establish a multi-stakeholder forum for cyber information sharing among MedTech players, providers, software developers and regulators.
- Develop a capability roadmap for MedTech companies, regulators and providers that incorporates horizon scanning.
- Develop and enhance the CISO function to drive a, “Secure-by-design” mindset for product development.
- Deploy technical controls such as penetration and vulnerability testing for medical devices, as well as the networks they reside on, conduct these early and often, and engage with regulators early.
- Develop a Coordinated Disclosure Program (CDP).

Understanding the challenges and concerns associated with connected medical devices

Regulatory and compliance management

The regulators’ prime responsibility is to ensure that approved products meet the desired standards of quality, safety and performance. Figure 1 provides a list of regulators advancing medical device standards globally⁴. With the advent of connected devices, predicting risks and devising mitigation strategies has gotten more challenging. The consensus across the board is that cybersecurity risks can never be completely eliminated but can be effectively mitigated with support from MedTech companies and providers. One of the challenges for regulators is the lack of in-house capabilities to conduct effective horizon scanning for new technologies and keep up with emerging MedTech applications. Partnering with the right entity with adequate capabilities is a simple solution that addresses this particular challenge. Figure 2 provides a list of key members of the cybersecurity community that promote stakeholder interaction and issue best practices⁵.

Another industry concern amongst a number of the smaller MedTech companies and providers is the lack of clarity on guidelines. As a result, many allow commercial pressures to take precedence over more conscientious regulatory planning, thereby increasing security risks. However, some multinational MedTech companies are taking more proactive security measures. For example, one organisation has centralised its APAC data center and regularly reviews its firewalls. This has reportedly helped prevent over 50,000 cyber-attacks in a month. They have also encrypted all data linked to their devices installed in their patients’ homes, all the way to the their data center⁶.



³ Mick Coady, J. F. (n.d.). It's time to improve cybersecurity for networked medical devices. Retrieved from PwC Cybersecurity and Privacy Blog.

⁴ IMDRF (2017). List of international medical device regulators. Retrieved from the International Medical Device Regulators Forum

⁵ HealthIT Security (2017). List of Medical Device cybersecurity community members. Retrieved from the HealthIT Security blog

⁶ Roundtable findings (2017). APACMed- PwC Digital Health Roundtable

Figure 1: List of Regulators Advancing Medical Device Standards











| Agency | Role |
|--|---|
|  <p>Health and Human Services (HHS) Office for Civil Rights (OCR)</p> | The OCR ensures equal access to certain health and human services and protects the privacy and security of health information. Additionally, the OCR enforces compliance with the HIPAA security, privacy, and hitech breach notification rules. |
|  <p>China Food and Drug Administrations</p> | Regulatory body similar to the FDA, streamlining regulation processes for food and drug safety. Recently formulated the guiding principles for the technical review of the safety registration of medical devices, with enforcement commencing in 2018. |
|  <p>US food and Drug Administration</p> | Regulatory body responsible for protecting and promoting public health through contril and supervision of numerous channels. Maintains the premarket and Postmarket guidance for management of Cybersecurity in medical devices. |
|  <p>Joint Commission</p> | The Joint Commission (JCo) accredits and certifies healthcare organizations and programs in the United States, and is recognised nationwide as a symbol of quality that reflects an organisation's commitment to meeting certain performance standards. JCo maintains expectations for safety of medical devices in hospital systems. |

Figure 2: Key members of the medical device cybersecurity community that promote stakeholder interaction and issue best practices

| Agency | Role |
|--|--|
|  <p>Healthcare Information and Management Systems Society (HIMSS)</p> | A non-profit organisation dedicated to improving healthcare in quality, safety, cost-effectiveness, and access through use of information technology and management systems; |
|  <p>National Health Information Sharing and Analysis Center (NH-ISAC)</p> | The official healthcare information sharing and analysis center for sharing cyber and physical security threat indicators, best practices, and mitigation strategies |
|  <p>Medical Device Innovation, Safety and Security Consortium (MDISS)</p> | A non-profit organisation committed to advancing quality heralthcare with a focus on the safe and security of medical devices |
|  <p>International Organization for Standardization (ISO)</p> | An independent, non-governmental international organisation that develops internation standards that support innovation and provide solutions to global challenges |
|  <p>Association for the Advancement of Medical Instrumentation (AAMI)</p> | An organisation for advancing the development, safety, abd effectiveness of medical technology |
|  <p>eHealth Initiative</p> | Non-profit organisation that engages doctors and patients in order to standardise and reform the use of health information technology |



Secure deployment of connected medical devices

Research has shown that interfaces to infusion pumps, default hard coded administration passwords, and access to the Internet across internal networks are just a few of the prevalent vulnerabilities discovered in devices used in a healthcare environment⁷. These vulnerabilities may result in incidents that impact the device, an organisation's network and most importantly, compromise patient safety.

Recognising this as a potential vulnerability, the US FDA in 2015/16, released premarket and postmarket device security guidance⁸, shifting the onus of identifying and managing cybersecurity risks onto MedTech companies. MedTech companies are now required to provide information such as hazard analysis of cyber risks. Furthermore, they are also required to adopt coordinated vulnerability disclosure policies and practices such as ISO/IEC 29147:2014 - Guidelines for the Disclosure of Potential Vulnerabilities in Products and Online Services⁹, and ISO/IEC 30111:2013 - Guidelines for how to process and resolve potential vulnerability information in a product or online service¹⁰.

When asked as to which network connected medical devices matter, the answer is any which interact with patients, provide treatment or care, and/or store, process, or transmit electronic protected health information (ePHI). An illustrative and non-exhaustive list of examples of network connected medical devices includes:

- Imaging devices (MRI, CT, ultrasound, nuclear imaging, portable imaging systems)
- Wearable and home monitoring (activity trackers, pedometer, sleep apnea)
- Picture archiving and communication system (PACS)
- Infusion pumps
- Anesthesia apparatuses
- Ventilators

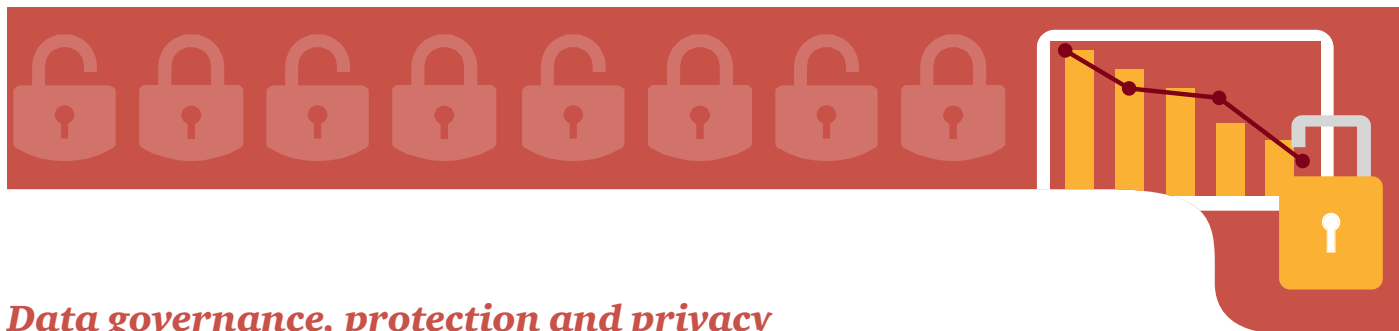


⁷ PwC. (2018). Managing cybersecurity risks in the health sector. Pricewaterhouse Coopers.

⁸ FDA. (2016). Postmarket Management of Cybersecurity in Medical Devices. Retrieved from US Food and Drug Administration

⁹ ISO. (2014). Information technology -- Security techniques -- Vulnerability disclosure. Retrieved from International Organisation for Standardisation

¹⁰ ISO. (2014). Information technology -- Security techniques -- Vulnerability disclosure. Retrieved from International Organisation for Standardisation



Data governance, protection and privacy

Traditionally, MedTech companies focused on quality of the product across the various development and manufacturing stages given that the devices were designed to function as standalone systems with a defined rate of obsolescence and replacement. Today, the lifetime of devices are extended and consequently manufacturers are obligated to maintain the quality of a device for a longer period of time and not just during design and production but also once it is deployed, per its use case, through a series of updates across firmware, software and, in some cases, hardware. To further add to the challenge, medical devices are now increasingly network connected in order to quickly receive and transmit health information for the treatment and care of patients.

The expanded use of IoT, coupled with the desire to make use of the information collected on a medical device in and across other healthcare systems, has made medical devices open and vulnerable to cybersecurity threats. Vulnerabilities that could allow malicious individuals, such as organised crime groups, hackers and insiders, unauthorized access to sensitive patient and device information. These cyber intrusions may be used for economic espionage, generating profits from health information, or potentially put patients' wellbeing at risk. Following a malicious attack last year, Melbourne Health performed a holistic assessment to check for data leakage and predict any future vulnerabilities. It has also since implemented a more refined segmentation of its network and put stringent policies and procedures in place in the interest of protecting their patients and their data¹¹.

Providers in Singapore are also increasingly adopting methods to capture, report and integrate device data into their analytics processes to improve efficiency and patient outcomes. There are now a multitude of startups developing apps and web presence to collect, use and process medical data – in short, there is increased proliferation of sensitive health, personal and even financial information being transacted within provider organisations and the end consumer. Given this rapidly changing environment, there is a need to improve oversight on how this sensitive data is shared and used by various parties who have authorized access to it. The recent cyber attack in Singapore on the nation's largest healthcare cluster, SingHealth which resulted in the country's biggest data breach¹² only reiterates the need to improve the above mentioned and much needed oversight. It is imperative that regulators revisit and review the framework for mandatory versus voluntary reporting in light of device compromises, breaches and adverse events as well as develop guidelines on the use of data, sanctions and related penalties in case of misuse, device compromise and breach.



¹¹ News, I. (2016). Malware attacks Melbourne Health Systems. Retrieved from IT News.

¹² Tham, I. (2018). SingHealth Cyber Attack: How it Unfolded. Retrieved from The Straits Times.

Medical device cybersecurity risk landscape – What ails healthcare organizations

Increased Cyber Threats:



Healthcare organisations are a key target for cyber criminals due to the high financial value of health records and associated personally identifiable information (PII) on the black market. One health record can be worth upwards of \$51 per record¹³. The threat actors are further emboldened given the historic underinvestment by healthcare organizations in IT modernisation and Cybersecurity.

Lack of Attention to Cybersecurity Software Risk:

Historically, attention has been focused on the development and functionality of hardware, rather than software and the associated risks thereof. Many medical devices run out-of-service operating systems (e.g. Windows XP, 2000, etc.), cannot run antivirus software, do not utilise encryption and use hard-coded passwords. Manufacturers also face a time consuming process in gaining approvals of their “gold” build that creates inherent vulnerabilities as software ages while the devices go through the approval process and previously undetected vulnerabilities are found and exploited during that period.



Inability to quantify risk and impact:



While most organisations are familiar with potential impacts from cyber events, such as financial loss, business interruption, regulatory fines and sanctions, brand damage – they lack the in-house capability to define and quantify the actual impact across any one of these areas. This lack of insight creates a false sense of security that limits active investment to cover security needs during development, manufacturing, approval, deployment and use. Creating such a view raises the security discussion from a technical requirement to a more pressing risk management requirement that now needs to be addressed at the board and executive levels of the organisation, be it manufacturer or provider.

¹³ Scene, H. (2014). What's the Black Market Value of a Health Record. Retrieved from EMR & HIPAA by Healthcare Scene.

Potential resolution mechanisms for MedTech, regulators and providers

Establish a MedTech information sharing / security advisory committee with multi-group representation

Use a neutral forum driven by industry organisations such as APACMed as a convener to drive focused and enhanced dialogues on cyber needs, trends and actions between MedTech organisations, providers, software players and regulators. Consumer feedback mechanisms should also be considered for inclusion, depending on the type of device and its use.

The NH-ISAC (National Health Information Sharing and Analysis Center) is a global organisation and active participation in the APAC region will enable effective information sharing across a number of topics that, in combination, may enable various parties to understand trends – for business, for threats, for regulation, for monitoring and response, and may ease the burden of individual Chief IT Officers (CIO/CTOs) and Chief Information Security Officers (CISOs) trying to identify such information in their individual data sets. A platform that supports such data sharing and can perform relevant analyses should also be considered to support the findings and necessary actions that each of the parties may take.

Develop a capability roadmap

In addition to continued engagement with other industry stakeholders, MedTech companies, regulators and providers need to have a clearer view of medium to long-term capabilities to prepare themselves for an age where connected devices become ubiquitous and where deployment use cases are continuously evolving.

MedTech has traditionally invested in biomedical engineering, software and commercial capabilities. However, there is now a clear case to develop security-by-design cyber capabilities that allow the build out of device remediation strategies, risks and mitigation plans.

From a provider perspective, understanding IT and network integration capabilities is mission critical because the provider organisation is the literal last mile delivery of patient services, and by far, has the potential for the highest impact – patient safety. Provider organisations need to establish the CISO function and fund them with necessary budgets and personnel to drive the deployment of secure networks, monitor for attacks and have tested plans for response and recovery from cyber incidents.

From a regulatory perspective, it is critically important to keep tab on regulatory best practice from leading agencies such as the US FDA and others. It is also critical to develop a horizon scanning mindset that allows a better understanding of the future of connected medical devices going forward.

Regulators, especially in Asia, can also take on a more active role in consumer awareness around data security and privacy.

Manufacturer Medical Device Cybersecurity Program Development

A robust Medical Device Cybersecurity Program Framework should align with industry best practice and regulatory guidance. The following list can be used as an initial reference point when setting up the CISO function:

- National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF);
- U.S. Food and Drug Administration (FDA) Pre/Post-Market Guidance;
- International Standards Organisation (ISO) 14971 (Quality Management), 29174 (Vulnerability Disclosure), 30111 (Vulnerability Remediation);
- Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR) 57 (Product Risk Analysis Methodology).

Furthermore, a medical device cybersecurity strategy must be supported by foundational capabilities that address technical control gaps, identify high risk areas and prioritise product-level assessment efforts so that regulators can be engaged during the approval process.

Manufacturers have not historically included products in day-to-day information security processes. In order to address increasing cybersecurity threats and shifting regulatory requirements, manufacturers need to begin incorporating products into these processes (e.g. vulnerability management, patch management, monitoring, incident response, and training and awareness, amongst others).



Deploy technical security controls such as penetration testing early and often during the development, deployment and use phases, and engage early with regulators



Testing

Testing the medical device early and often can help MedTech companies determine and address vulnerabilities prior to a cyber intrusion that may impact the organisation and/or patient. Comprehensive penetration testing should include real world simulation¹⁴ of threats facing medical device environments with the focus of efforts displaying specific risks to patient privacy and patient safety in a network-connected medical device environment. A comprehensive testing methodology should be prescriptive on the methodology and process for technical testing and evaluation of medical devices, applications and systems while providing the necessary process for documenting evidence that testing and evaluation has been performed. The testing program should also incorporate the following leading industry practices:

- Abuse Case Testing;
- Communications Analysis;
- Application Layer Testing;
- Supporting Infrastructure Testing;
- Reverse Engineering;
- Run-Time; and
- Logic Manipulation.

The results of these tests should be documented and reported to regulators during the product development lifecycle to continue developing more robust risk assessments and mitigation plans. Additionally, testing should feed into the overall maintenance strategy for the device during its deployed lifecycle.

Maintenance

- Maintain a detailed, up to date and accurate inventory of medical devices. Additionally, confirm means of location tracking and monitoring have been deployed to mobile equipment.
- Define vendor maintenance scheduling and establish a secure means of remote and on-site maintenance.
- Validate that unused generic user accounts are deleted.
- Conduct vulnerability assessments and penetration testing.
- Ensure an appropriate security incident response function is in place, complete, and maintains the necessary stakeholders.
- Assess enterprise level IT governance controls and other technical security controls.

¹⁴ PwC. (2016). Game of Threats™ - A cyber threat simulation. Retrieved from Pricewaterhouse Coopers.

Develop a Coordinated Disclosure Program

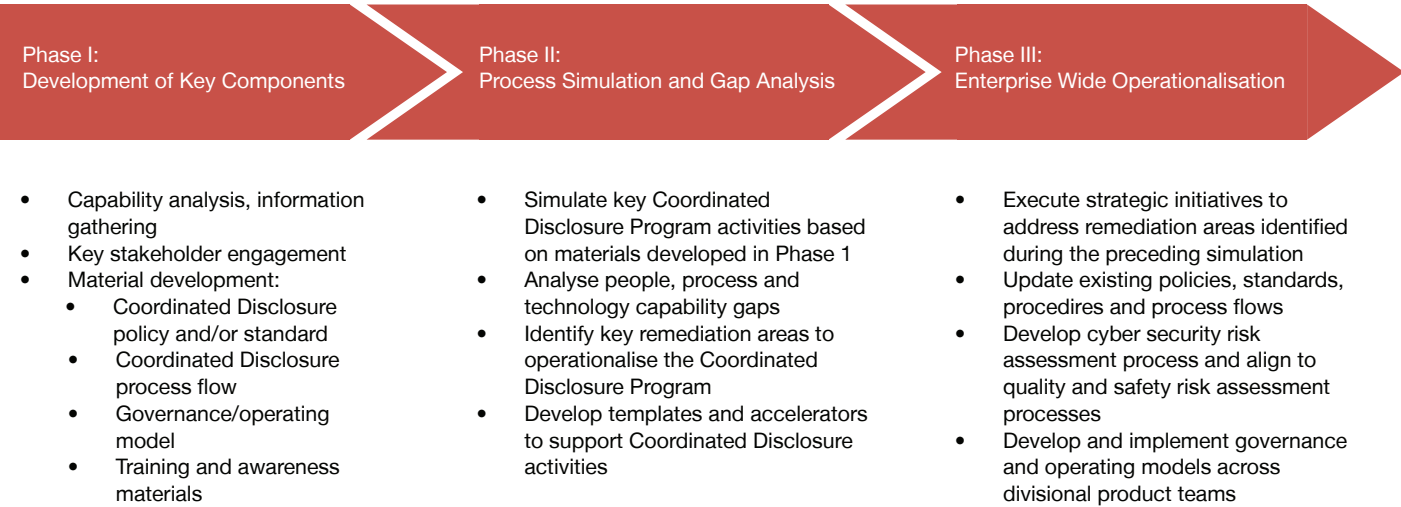
The US Food and Drug Administration (FDA) Postmarket Guidance for Medical Device Cybersecurity recommends manufacturers of medical devices implement certain critical components of a comprehensive cybersecurity risk management program, including adoption of a coordinated vulnerability disclosure policy and practice.

Coordinated Disclosure is a process by which outside parties are able to disclose medical device cybersecurity vulnerabilities to manufacturers through anonymous, secured processes, and provides the manufacturer with additional mechanisms by which cybersecurity vulnerabilities can be confirmed, assessed, and remediated.

A coordinated disclosure program is essential for medical device manufacturers handling vulnerabilities or cybersecurity risks that may be discovered and reported within the organisations’ product portfolio. A typical approach to developing such a program includes:

- Collecting a capabilities analysis and information.
- Developing key coordinated disclosure program components such as a policy and playbook and operating model for coordination activities.
- Conducting a training workshop with awareness materials outlining the program and expectations.

Figure 3: Three Phase Coordinated Disclosure Plan Approach





The road ahead

Life saving and life changing progress is being made across the board in the research and development of new devices and capabilities to address our patients' healthcare needs. However, the market is evolving more rapidly than regulatory frameworks are being defined. Being first to market or first to innovate new features and functions remains the mandate for medical device companies and even provider organisations. In such an environment, introducing a new requirement for security – across the various organisations – becomes a delicate balancing act between costs and benefits.

Each of the entities in this ecosystem – regulators, manufacturers, providers, and even consumers – have a significant role to play in changing the dialog and in enforcing necessary security requirements into their individual practices. This cannot be achieved without a coordinated and collaborative effort. All entities in the ecosystem need to make investments to bolster their information and cyber security functions and to elevate those functions beyond a technical purview and bring them into the executive purview. The threats are not diminishing and systems remain vulnerable, but if the necessary investments are made, these entities will have taken the much needed step to changing their internal culture and mindset as it relates to the application of security to drive better patient outcomes.

Our authors



Freddy Wee

Partner
Cybersecurity & Privacy
E: reddy.wee@sg.pwc.com



Urooj Burney

Cybersecurity & Privacy Impact Centre Leader
PwC South East Asia Consulting
E: urooj.h.burney@sg.pwc.com



Dr. Zubin J. Daruwalla

Health Industries Leader
PwC South East Asia Consulting
E: zubin.j.daruwalla@sg.pwc.com



Sumanth Kambhammettu

Senior Manager
PwC South East Asia Consulting
E: sumanth.kambhammettu@sg.pwc.com