MedTech Europe response to the Draft Medical Device Manufacturer Internet of Things (IoT) Code of Conduct

31 March 2020

MedTech Europe ('MTE') appreciates the opportunity to provide input on the Global Digital Health Partnership's ("GDHP") Draft Medical Device Manufacturer Internet of Things (IoT) Code of Conduct ("CoC"), through the Office of the National Coordinator's website.

MTE is the European Trade Association for the medical technology industry including diagnostics, medical devices and digital health. MedTech Europe's mission is to make innovative medical technology available to more people while helping healthcare systems move towards a sustainable path. MTE encourages policies that support the medical technology industry to meet Europe's growing healthcare needs and expectations. It also promotes medical technology's value for Europe focusing on innovation and stakeholder relations, using economic research and data, communications, industry events and training sessions.

1. Recommended updates to enhance Device Manufacturer adoptability

Terminology & scope: the GDHP Code of Conduct (CoC) introduces IoT concepts and IoT in healthcare. It will be helpful for adoptability to clarify what definition for IoT the GDHP refers to, which will also help manufacturers understand better the scope of the CoC. We recommend adopting the term "network-connected medical devices", "network connected in vitro diagnostic systems", and "Software as a Medical Device (SaMD)" which are used by most guidelines and regulations we know.

It might be helpful to clarify that "network-connected medical devices", which replace devices that were once standalone instruments interacting only with the patient or medical provider, include a wide range of products as diverse as infusion pumps, remotely monitored cardiovascular implantable electronic devices, homecare cardio-monitoring, chemotherapy dispensing stations, surgical robots and wearable consumer products. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems or networks, ultimately contributing to the Internet of Medical Things (IoMT) or Internet of Medical Devices (IoMD).

Target audience: In addition to the CoC's scope and terminology, the CoC could be more specific about the target audience, e.g. helpful to clarify who this document is addressing - manufacturers only, or healthcare authorities, healthcare providers and regulators as well. It is necessary to consider that security in healthcare is a joint effort that concerns all stakeholders and implies shared responsibilities among them.

We would like to call to attention the following (non-exhaustive) list of regulations that build on the theme of continuous device lifecycle management in several international standards, including:

- Global: The International Medical Device Regulators Forum (IMDRF) Principles and Practices for Medical Device Cybersecurity (to be published soon)

- Europe:
    - The European Commission's NIS Directive
    - The Regulation EU 2017/745 on medical devices (MDR) and Regulation EU 2017/746 on in vitro diagnostic medical devices (IVDR): cybersecurity is addressed in Annex I of both regulations.
    - More specific guidance is delivered in the recently published MDCG 2019-16 Guidance on Cybersecurity for medical devices
- United Kingdom: Code of Practice for Consumer IoT Security
- United States:
    - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices
    - Post market Management of Cybersecurity in Medical Devices
    - Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Canada: Guidance Document: Premarket Requirements for Medical Device Cybersecurity
- Australia: Therapeutic Goods Administration documents:
    - Medical device cybersecurity guidance for industry
    - Medical device cybersecurity information for users

2. Recommended Global Device Manufacturer adoptability considerations

Existing regulations, international standards and guidelines on cybersecurity for medical devices, such as those mentioned in the previous section, build a comprehensive regulatory framework that medical device manufacturers are adopting and implementing for the entire lifecycle of their medical devices, including in Software as Medical Device (SaMD). Therefore, it might be helpful to clarify the contribution/role of this CoC vis-à-vis these existing documents.

While we understand that the proposed CoC aims to address a global community of manufacturers, it currently references only the FDA's guidance, and some other US references. It would benefit from looking at a wider array of local and/or regional regulations or guidance (please see some examples in the previous section).

In the interest of global harmonisation and a greater adoptability by medical device manufacturers, the proposed CoC would also benefit from:

- accepted international security and risk management standards,
- alignment with already existing global and regional guidance documents and regulations
- coordination with local and regional regulators, stakeholder organisations and manufacturers.

The International Medical Device Regulators Forum (IMDRF) is a group of medical device regulators, currently including representatives of medical device competent authorities of Australia, Brazil, Canada,

China, European Union, Japan, Russia, Singapore, South Korea and the US, as well as the World Health Organisation acting as an official observer. It is an established and recognised regulators forguidinge on strategies, policies and directions, aiming to accelerate international medical device regulatory harmonisation and convergence

The IMDRF is expected to publish soon a guidance on Principles and Practices for Medical Device Cybersecurity, based on a public consultation. We suggest that the GDHP review this guidance and consult with the IMDRF to avoid the possible points for confusion and/or contradiction among the related stakeholders and regulators.

3. General draft comments

MedTech Europe welcomes the efforts of GDHP members to align on a Medical Device Manufacturer Internet of Things (IoT) Code of Conduct; nevertheless, we believe the draft should be better coordinated with the cybersecurity agencies in the GDHP member countries that in many cases have already delivered cybersecurity guidance for the medtech industry, for users and for healthcare organisations.

Based on the above mentioned, we recommend:

- Clarify the scope, i.e. what is in scope and what is excluded; whom is this document addressing; what regulations are being addressed? Add a statement about the purpose and intention of this new document.
- Add a reference to the concept of shared / joint responsibility that reflects a wide consensus among cybersecurity experts and is developed for example in the forthcoming IMDRF guidance.
- Add a definition list to create clarity on the terminology used in the document. Preferably use definitions from acknowledged international standards organisations.
- Offer more substance, context, and framework in the section ‘Best Practices and Recommendations’. Be clear on pre- and post-market requirements during the lifecycle of the device (including the stages of deployment and de-commissioning).
- The best practices and recommendations only deal with ‘what’, not the ‘why’, ‘how’ and ‘who’. The document includes suggestions of good practices, which are common to many other documents about cybersecurity and privacy from other international and national organisations.
- Consider adding a discussion of region-specific rules regarding privacy and data protection.
- In the references section:
    - Add references regarding security standards, risk management standards and regulations that are applicable to the global stakeholder community.
    - Include reference to other international guidelines listed in the first section.
    - Ensure that all references are up to date and hyperlinks are working (especially for information from commercial security vendors).
    - Explain that references are not exhaustive.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

For questions or more information, please contact Michael Strübin, Director Digital Health, at m.strubin@medtecheurope.org