REG-MEDTECH: Regulation and Standardization of Connected, Intelligent Medical Devices

Research team:
Dr Irina Brass and Dr Andrew Mkwashi, UCL
In partnership with BSI

PROJECT TIMELINE

Start date: 1 October 2021
Finish date: 31 March 2023

INTRODUCTION

The healthcare industry is undergoing a rapid transformation powered by digital technologies and systems. In recent years, there have been a lot of changes such as the accelerated adoption of **Internet-connected medical devices (MIoT)** and Artificial Intelligent (AI) systems that are typically implemented as software in medical devices or as **Software as a Medical Device (SaMD)**. Working in partnership with BSI (UK National Standards Body), the REG-MEDTECH Project investigates the critical changes that need to occur to current medical device regulations and standards to capture, minimise, and mitigate the risks associated with software and AI-based medical devices.

The project focuses on three critical areas: **cybersecurity, integrity of AI systems, data governance**.

PROJECT AIMS

- Conduct an **assessment of current gaps** in standards and regulations for connected, intelligent medical devices
- Address **organizational needs for ensuring the safety and performance** of software-based medical devices throughout their lifecycle
- Investigate **new approaches to standards, regulations, and policy** to address critical safety, security, and performance risks (eg. flexible regulatory pathways, distributed liability).

IMPACT

Our research so far has shown that there are emerging regulatory frameworks for responding to the critical cybersecurity, AI integrity, and data governance challenges posed by connected, intelligent medical devices. However, what is currently missing are standards and guidelines to help organisations implement, conform and comply to regulatory requirements.

METHODOLOGY

A four-step methodology was used in this project:

1. **Literature review**
2. **Review of current and in development standards** applicable to connected, intelligent medical devices
3. **Interviews with critical stakeholders**: software developers, device manufacturers, clinicians, security practitioners, lawyers, standards-makers, regulators.
4. **Roundtable in partnership with BSI and MHRA**: The Future of Medical Device Regulations and Standards – Dealing with Software Challenges, 27 April 2022

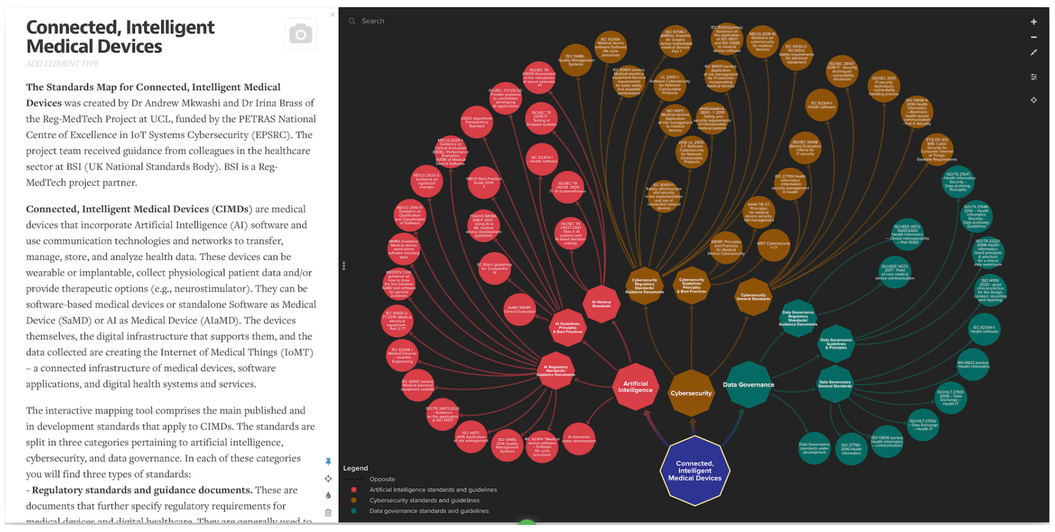

Figure 1: Standards Mapping Tool for Connected, Intelligent Medical Devices

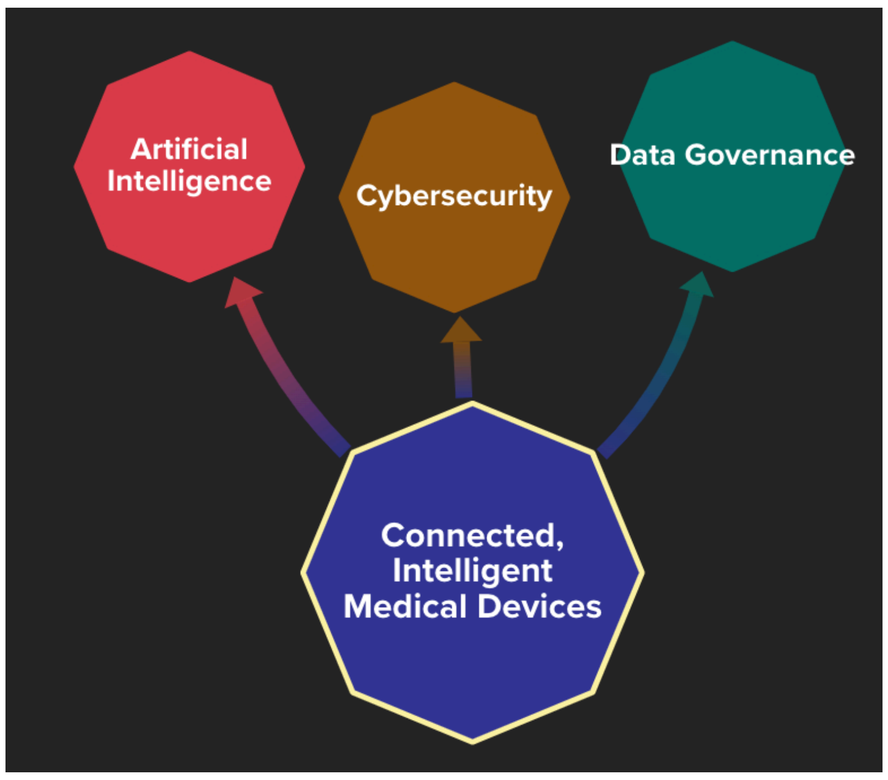

Figure 2: Three key research issues

SUMMARY OF DATA SOURCES

Stakeholder Category	Number of Interviews	Number of Roundtable Participants	Total
Government authority	2	4	6
Notified bodies / Regulatory agency	3	7	10
Academic and research institution	3	9	12
Medical device manufacturing	0	3	3
Health facility	4	12	16
Industry association / other	2	11	13
Total number of data sources	**14**	**45**	**60**

KEY OUTCOMES

Evidence from our interviews, roundtable, and our examination of existing literature provide a basis for articulating several critical gaps in regulatory frameworks and standards that apply to connected, intelligent medical devices.

This project produces an open and free access **Mapping Tool** of existing and in progress standards for connected, intelligent medical devices, and a **White Paper** on how to address current standardization gaps that support both innovation and regulatory requirements.

MAJOR FINDINGS

1. **Mismatch between pace of innovation and standards-making process** to support emerging regulatory frameworks
2. **Liability concerns**: product liability, software, and cybersecurity liability. Balance between manufacturer responsibility/ software developer/ user responsibility. Distributed liability across supply chain
3. **Risk classification**, especially for AI-based devices or AIaMD
4. Greater **software complexity** and cybersecurity challenges
5. **Legacy components**: devices are the endpoint of a larger digital healthcare infrastructure
6. **Black box issues**: specifications on how to practically achieve transparency and explainability; how to demonstrate conformity
7. Critical **gaps in data quality and data governance standards**
8. **Bias** in training data and algorithmic learning processes

ACKNOWLEDGEMENTS

This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC under grant number EP/S035362/1.

USER PARTNERS

British Standards Institute (BSI)
Medicines and Healthcare products Regulatory Agency (MHRA)