ISTITUTO DI DIRITTO, POLITICA E SVILUPPO

Sant'Anna
Scuola Universitaria Superiore Pisa

BRIEF
Biorobotics Research & Innovation Engineering Facilities

Standards and Liability: what about mixed functions IoT e-health devices?

Francesca Gennari

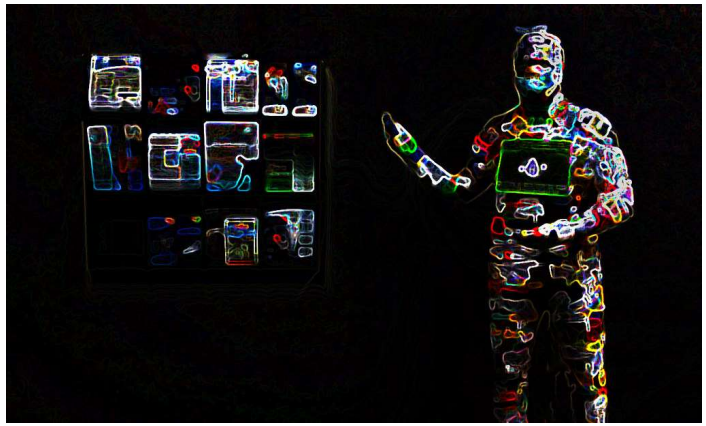
Privacy Technologist, BRIEF project
Lider-Lab

Colloquium on cybersecurity in the health sector

EUI – Centre for Judicial Cooperation

28 April 2023 – Online

Outline of the presentation

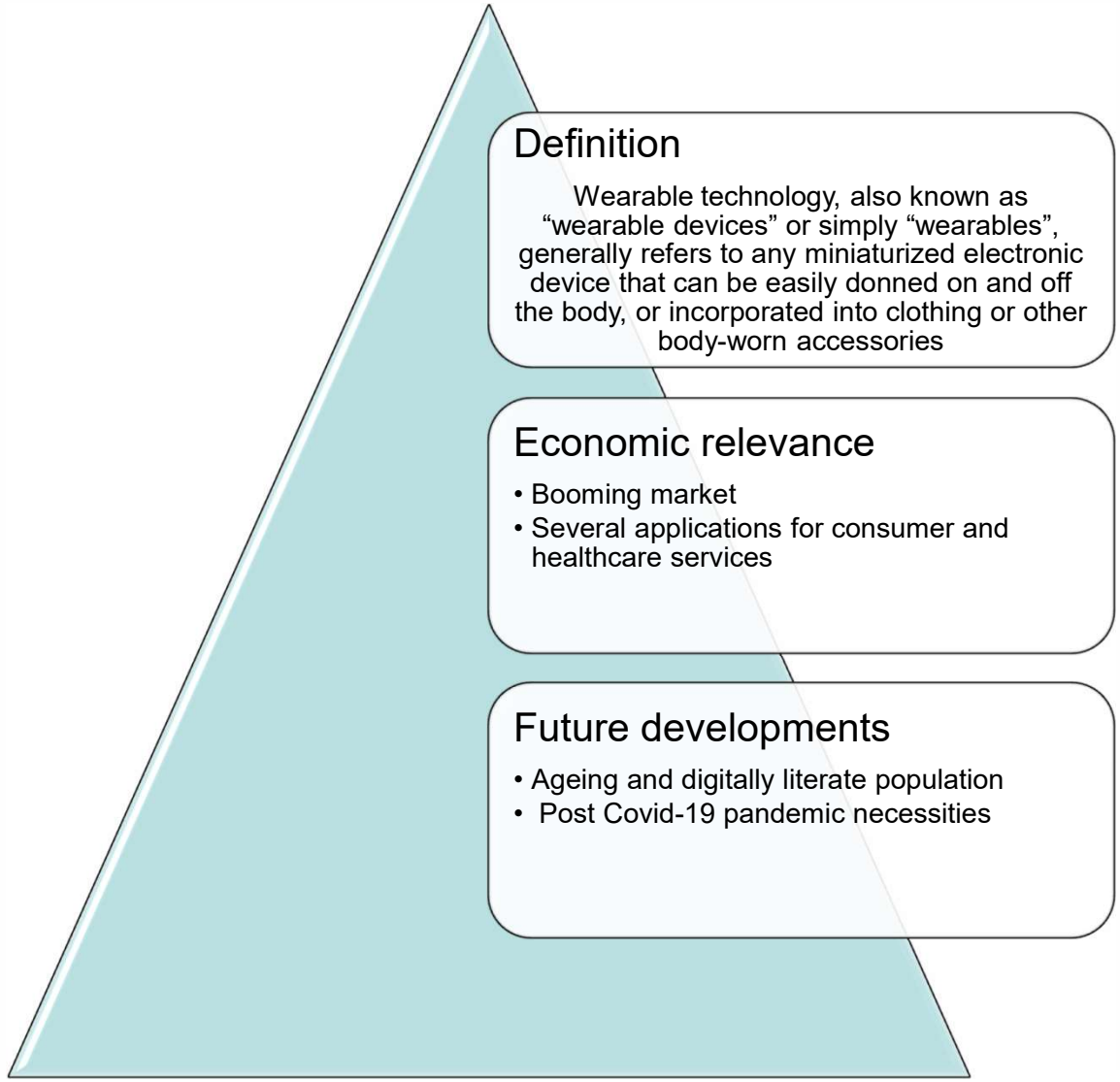


1) Wearables: social importance and definitions

2) Standards for the IoT: an initial overview

3) Liability rules on mixed function IoT e-health devices. An analysis according to the EU enacted and proposed acts

1) Wearables



Definition

Wearable technology, also known as “wearable devices” or simply “wearables”, generally refers to any miniaturized electronic device that can be easily donned on and off the body, or incorporated into clothing or other body-worn accessories

Economic relevance

- Booming market
- Several applications for consumer and healthcare services

Future developments

- Ageing and digitally literate population
- Post Covid-19 pandemic necessities

2) Wearables

Underpinning paradigm is IoT technology

- Different layers
- Centralised paradigm → main functions are carried out in the **cloud** but **sensors** are still **essential**
- Low cyber security levels (especially the commercial applications)
- Centrality of certifications and standards for safety and security

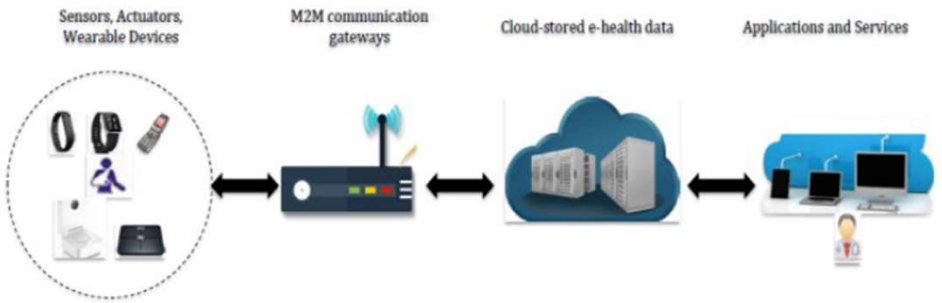


Fig. 1. Remote e-health monitoring

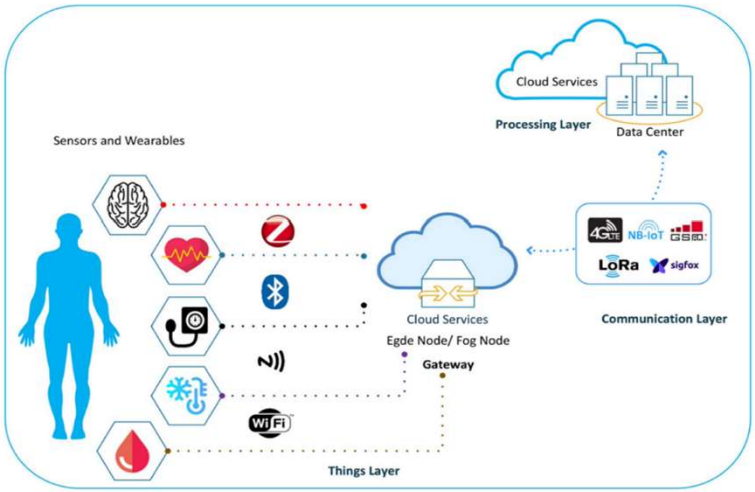


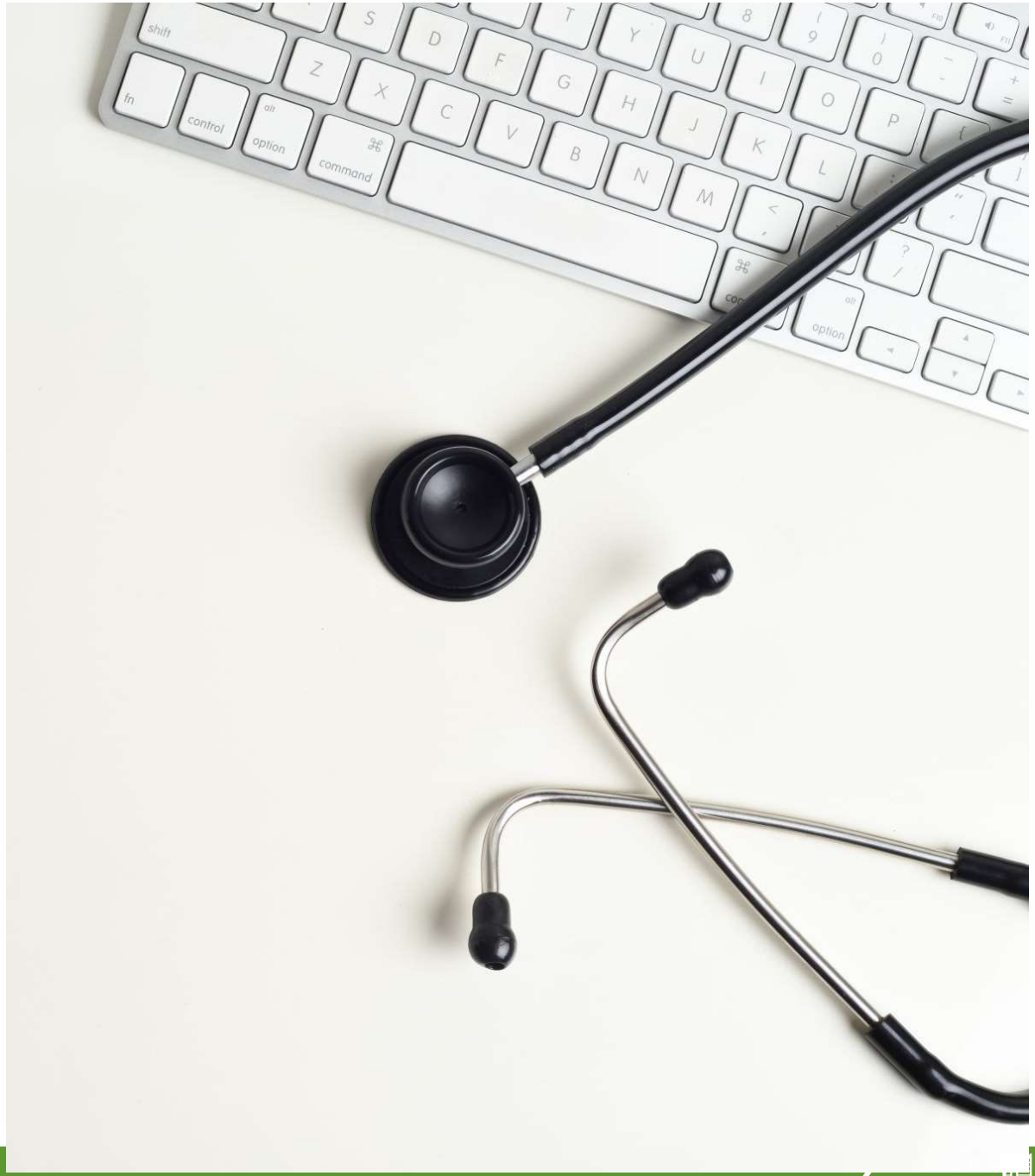
FIGURE 1. Three-tier architecture of the IoT healthcare system.[1]

3) Wearables

Early stage research focus actually is on how what could appear mainly consumer IoT applications for leisure and sports activities who could have also have important health functions

- Monitoring of vitals (hearth rate)
- Connection with emergency services

This is interesting because of their vast application and because there will not only be a national health system funded devices but also private healthcare ones which might interact with other consumer IoT application



4) Wearables: the software problem

Medical Device Coordination Group (MDCG) guidelines as whether to consider software a medical device 2019

*"Medical device software is software that is intended to be used, **alone** or in **combination**, for a purpose as specified in the definition of a "medical device" in the medical devices regulationor in vitro diagnostic medical devices regulation."*

Decision step 1: if the product is software according to Section 2 (Definitions and Abbreviations) of this guidance, then it may be a medical device software, proceed to decision step 2; if the product is not software according to the definition of this guidance, then it is not covered by this guidance but may still be covered by the Medical Devices Regulations.

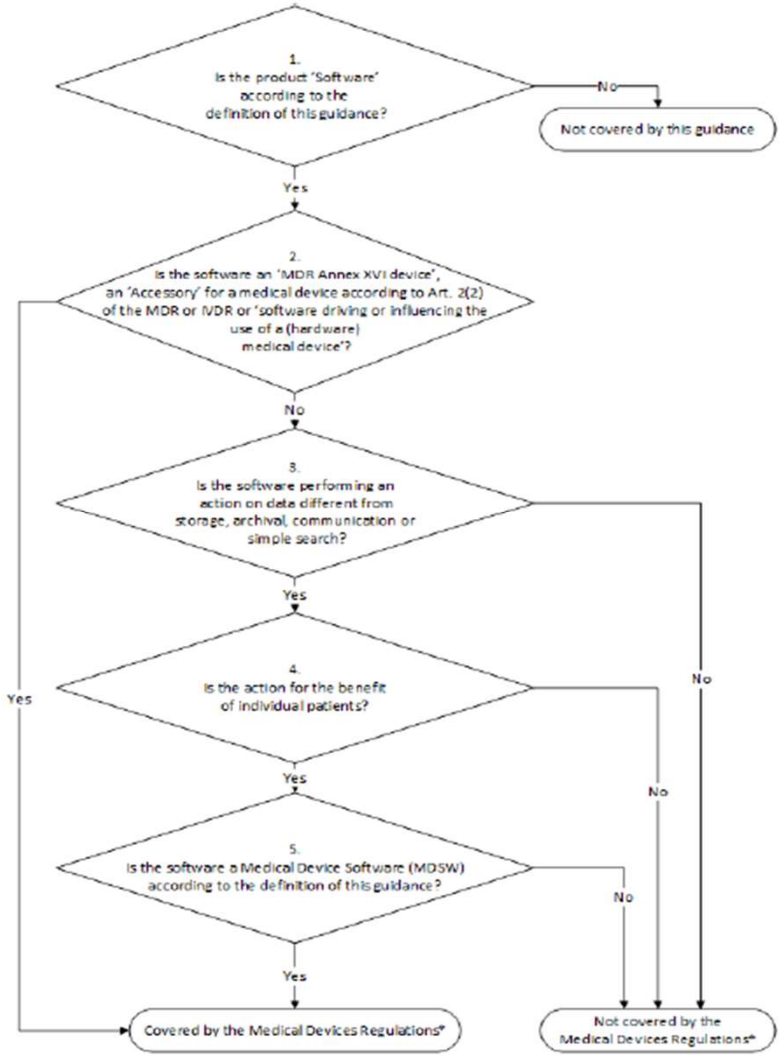
Decision step 2: if the product is an MDR Annex XVI device, or is an accessory for a medical device19, or is software driving or influencing the use of a medical device, then it must be considered as part of that device in its regulatory process or independently if it is an accessory. If it is not, proceed to decision step 3.

Decision step 3: if the software does perform an action on data, or performs an action beyond storage, archival, communication20, simple search, lossless compression (i.e. using a compression procedure that allows the exact reconstruction of the original data) then it may be a medical device software (Refer to section 3.1 for more guidance on these software functions) proceed to step 4.
Decision step 4: is the action for the benefit of individual patients?

Examples of software which are not considered as being for the benefit of individual patients are those which are intended only to aggregate population data, provide generic diagnostic or treatment pathways (not directed to individual patients), scientific literature, medical atlases, models and templates as well as software intended only for epidemiological studies or registers.

Decision step 5: Is the software medical device software (MDSW) according to the definition of this guidance?

p. 8
Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR

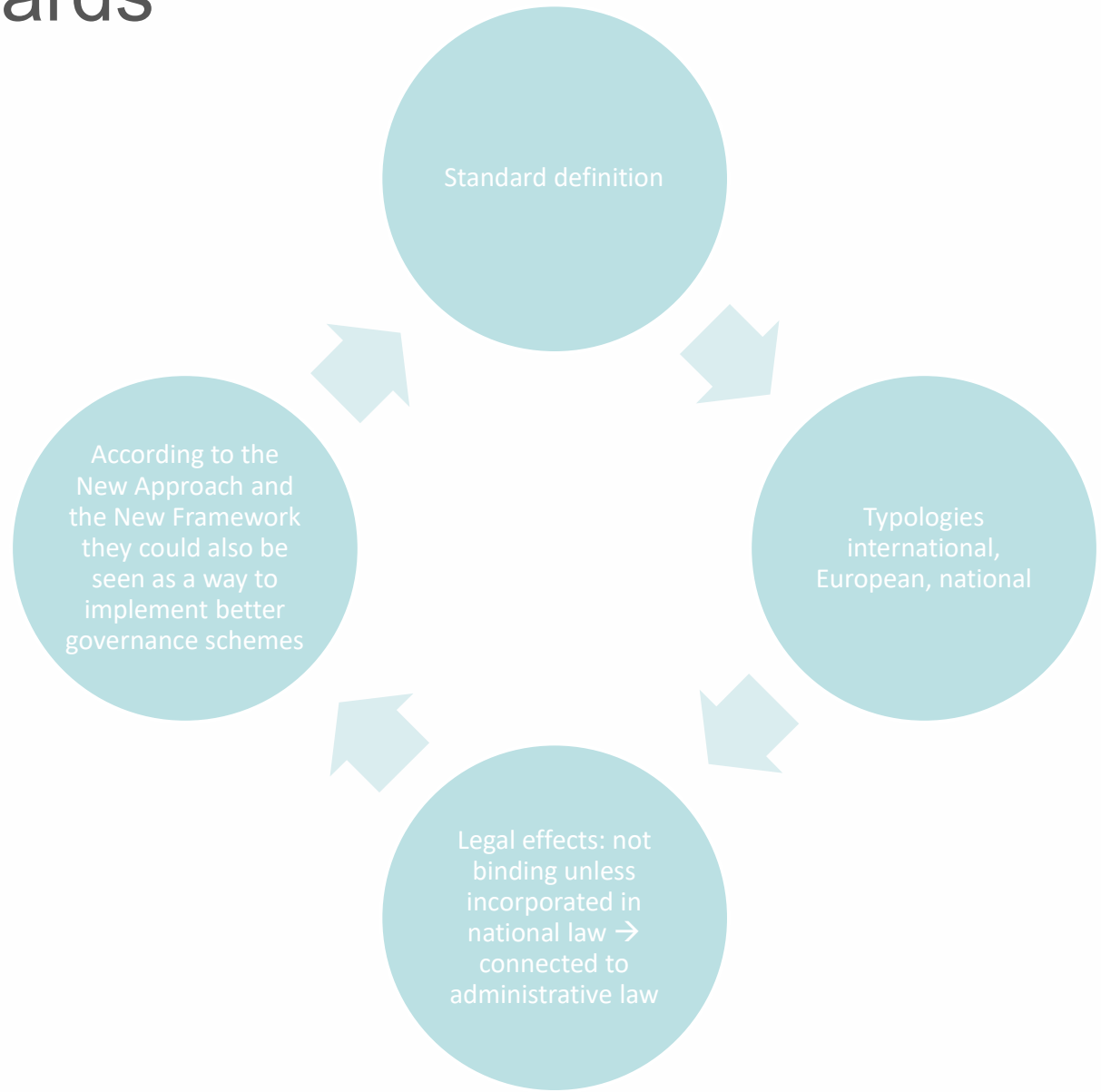


1) Standards

This causes problems in terms of interoperability and the role of standards as interoperability standards could be relevant for EU law from multiple points of view

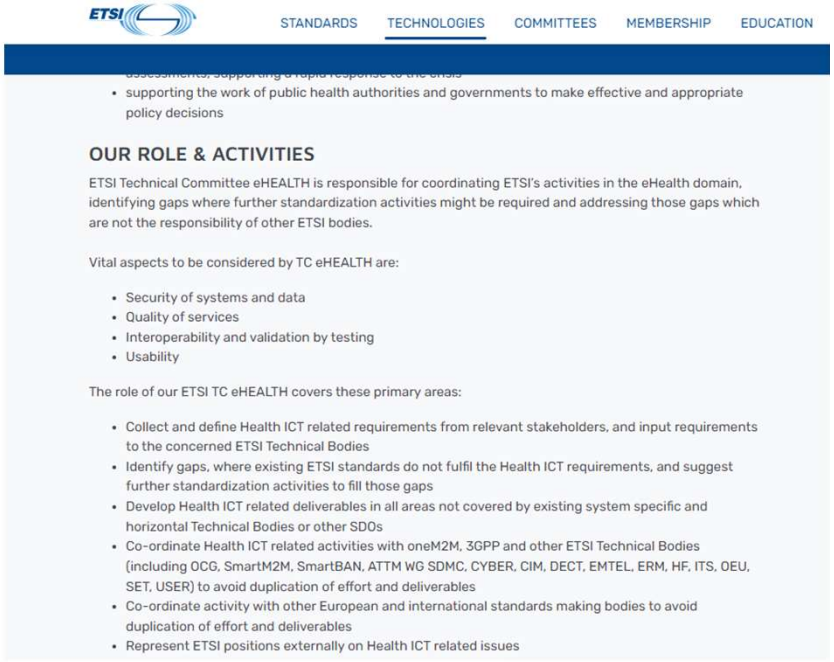
- Standard Essential Patents (SEPs)
- The Cyber security act v. MDR
- The EHDS
- Product liability directive + Product Liability directive update proposal
- AI act + AI civil liability proposal
- Data Act
- General Product Safety Regulation

2) Standards


Standard definition
Typologies international, European, national
Legal effects: not binding unless incorporated in national law → connected to administrative law
According to the New Approach and the New Framework they could also be seen as a way to implement better governance schemes

3) Standards

- Harmonised standards: the EU Commission asks the three main EU Standard Developing/Setting Organisations (SSOs/SDOs)
- At the moment the IoT standards: ISO ETSI
- There is an *ad hoc* working group on standards which is part of the Medical Device Coordination Group (MDCG)



ETSI STANDARDS TECHNOLOGIES COMMITTEES MEMBERSHIP EDUCATION

- supporting the work of public health authorities and governments to make effective and appropriate policy decisions

OUR ROLE & ACTIVITIES

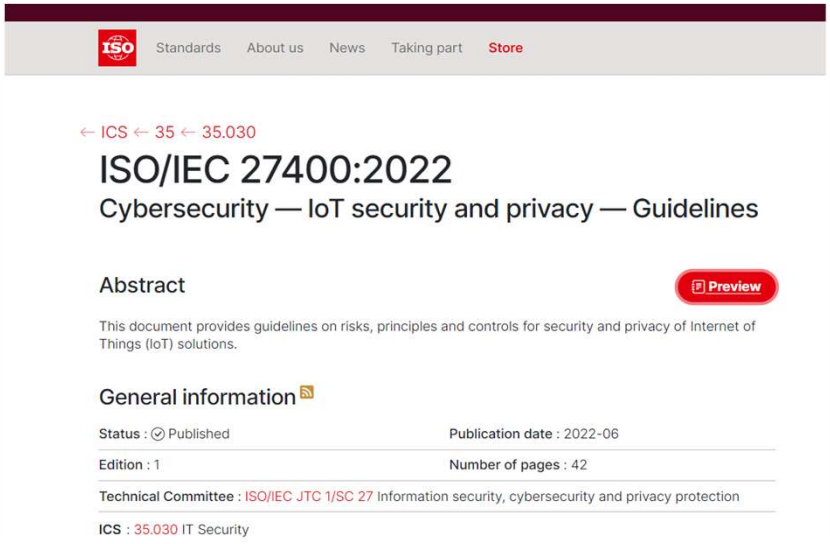
ETSI Technical Committee eHEALTH is responsible for coordinating ETSI's activities in the eHealth domain, identifying gaps where further standardization activities might be required and addressing those gaps which are not the responsibility of other ETSI bodies.

Vital aspects to be considered by TC eHEALTH are:

- Security of systems and data
- Quality of services
- Interoperability and validation by testing
- Usability

The role of our ETSI TC eHEALTH covers these primary areas:

- Collect and define Health ICT related requirements from relevant stakeholders, and input requirements to the concerned ETSI Technical Bodies
- Identify gaps, where existing ETSI standards do not fulfil the Health ICT requirements, and suggest further standardization activities to fill those gaps
- Develop Health ICT related deliverables in all areas not covered by existing system specific and horizontal Technical Bodies or other SDOs
- Co-ordinate Health ICT related activities with oneM2M, 3GPP and other ETSI Technical Bodies (including OCG, SmartM2M, SmartBAN, ATTM WG SDMC, CYBER, CIM, DECT, EMTEL, ERM, HF, ITS, OEU, SET, USER) to avoid duplication of effort and deliverables
- Co-ordinate activity with other European and international standards making bodies to avoid duplication of effort and deliverables
- Represent ETSI positions externally on Health ICT related issues



ISO Standards About us News Taking part Store

← ICS ← 35 ← 35.030

ISO/IEC 27400:2022

Cybersecurity — IoT security and privacy — Guidelines

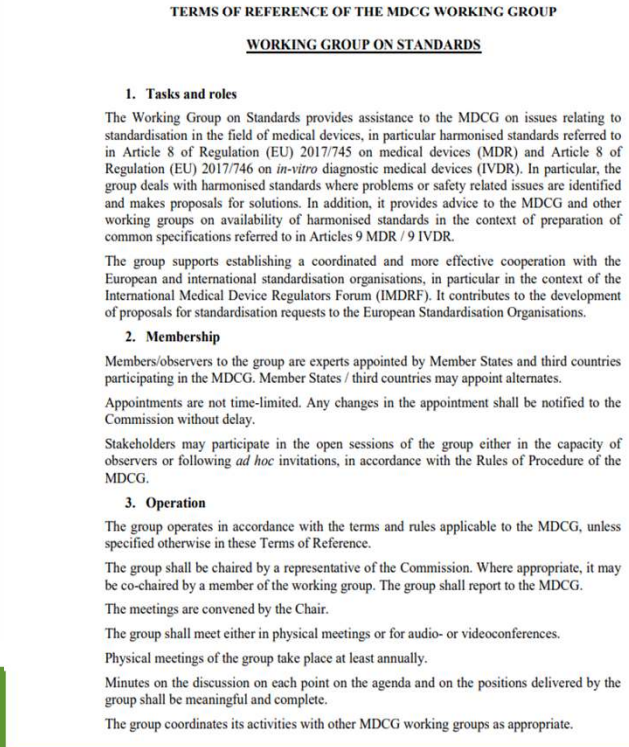
Abstract

Preview

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

General information

Status : Published	Publication date : 2022-06
Edition : 1	Number of pages : 42
Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	
ICS : 35.030 IT Security	



TERMS OF REFERENCE OF THE MDCG WORKING GROUP

WORKING GROUP ON STANDARDS

1. Tasks and roles

The Working Group on Standards provides assistance to the MDCG on issues relating to standardisation in the field of medical devices, in particular harmonised standards referred to in Article 8 of Regulation (EU) 2017/745 on medical devices (MDR) and Article 8 of Regulation (EU) 2017/746 on *in-vitro* diagnostic medical devices (IVDR). In particular, the group deals with harmonised standards where problems or safety related issues are identified and makes proposals for solutions. In addition, it provides advice to the MDCG and other working groups on availability of harmonised standards in the context of preparation of common specifications referred to in Articles 9 MDR / 9 IVDR.

The group supports establishing a coordinated and more effective cooperation with the European and international standardisation organisations, in particular in the context of the International Medical Device Regulators Forum (IMDRF). It contributes to the development of proposals for standardisation requests to the European Standardisation Organisations.

2. Membership

Members/observers to the group are experts appointed by Member States and third countries participating in the MDCG. Member States / third countries may appoint alternates.

Appointments are not time-limited. Any changes in the appointment shall be notified to the Commission without delay.

Stakeholders may participate in the open sessions of the group either in the capacity of observers or following *ad hoc* invitations, in accordance with the Rules of Procedure of the MDCG.

3. Operation

The group operates in accordance with the terms and rules applicable to the MDCG, unless specified otherwise in these Terms of Reference.

The group shall be chaired by a representative of the Commission. Where appropriate, it may be co-chaired by a member of the working group. The group shall report to the MDCG.

The meetings are convened by the Chair.

The group shall meet either in physical meetings or for audio- or videoconferences.

Physical meetings of the group take place at least annually.

Minutes on the discussion on each point on the agenda and on the positions delivered by the group shall be meaningful and complete.

The group coordinates its activities with other MDCG working groups as appropriate.

1) Liability

Type of Standard	Type of Liability
International standard	Tort liability (exceptions for some countries)
Harmonised standard (EU standard)	Not clear. Possibly new PLD when the application is low-risk and AI civil liability when high risk application + administrative liability (new general product regulation)
National standard	Administrative form of liability, eventually civil liability

2) Liability. A practical case

Smart-watch, Exergame apparel

Damage (material but also non material)

Software is the cause of the damage → is the software used as a medical device (monitoring) → liability rules Article 10(16) : obligation for the manufacturer to be compliant with the PLD (have enough funds) → Actual PLD, Articles 4, 6 and 9 for the consumer and Article 7 for the manufacturer to exempt himself. However, things might change with the approval of the AI act and the new AI civil liability act (articles 3 and 4) and PLD update (articles 7,8,9,10) depending on whether the AI system is high or low risk

Hardware is the cause of the damage → administrative provisions connected to General Safety Product regulation and if more specific and relating to the electronic part of the device which is not a medical device→ administrative liability. But also product liability directive and its update

Thank you for your attention

Francesca.Gennari@santannapisa.it