Harmonised standards to the AI Act – for medical devices, too

Alpo Värri[1]

[1] Faculty of Medicine and Health Technology, Tampere University, Finland

Alpo Värri, Dr.Tech., Faculty of Medicine and Health Technology, Tampere University, FI-33014 Tampere University, FINLAND. Email: Alpo.Varri@tuni.fi

Abstract

The European Union artificial intelligence act (AI Act) establishes the rules for the application of artificial intelligence (AI) systems within the European Union. The AI Act is to be complemented with the harmonised standards that provide the presumption of conformity to the AI Act if implemented fully in the organisation that provides the AI system. The joint technical committee 21 (JTC 21) of CEN and CENELEC has been assigned the responsibility to prepare these standards. Work is under way to develop standards for AI risk management, AI cybersecurity, AI quality management, Quality and governance of datasets in AI, AI trustworthiness framework and AI conformity assessment. As medical devices incorporating an AI component are also within scope of the AI Act, these standards apply to medical devices, too. For this reason, medical device experts need to contribute to the AI standardisation work so that the resulting standards will be feasible in the health sector. The challenge in the work is to make several standards good and compatible with each other in the presence of a plurality of opinions and a hurry to produce the standards in time.

Keywords: artificial intelligence, medical devices, laws, standards

Introduction

The Artificial Intelligence Act (AI Act) 2024/1689 of the European Union (EU) [1] is said to be the first ever legal framework on artificial intelligence (AI) in the world [2]. The AI Act lays down the rules of the development of AI systems to their providers and the organisations that make use of the AI systems, the deployers. The AI Act defines four levels of risks for AI systems [2]. The AI systems which result in a clear threat to the safety, livelihoods and rights of people are banned altogether because the risk level is unacceptable. The so-called high risk AI applications pose serious risks to health, safety or fundamental rights. They can be deployed, but their development and use are subject to several restricting articles in the AI act. In addition to several explicitly named use cases listed in Annex III of the AI Act, such applications which are required to undergo a third-party conformity assessment by another EU regulation are high risk AI systems. This applies to medical devices regulated by the Medical Device Regulation of the EU [3] incorporating and AI component, bringing these medical devices within the scope of the AI Act. The so-called limited risk AI applications need to fulfil transparency

requirements of the AI act. This means that the affected persons of such systems must be made aware that they are interacting with and AI system instead of a human. Finally, most of the AI systems belong to minimal risk AI applications and there a virtually no obligations to such systems.

The articles 6 to 27 and Annexes IV, VIII, and IX of the AI Act address particularly the high-risk AI systems. To clarify the requirements, the EU Commission has made a standardisation request M/593 [4] to the European standardisation organisations CEN and CENELEC to produce standards to ten topics in the AI act in May 2023. These are:

1. Risk management systems for AI systems
2. Governance and quality of datasets used to build AI systems
3. Record keeping through logging capabilities by AI systems
4. Transparency and information provisions for users of AI systems
5. Human oversight of AI systems
6. Accuracy specifications for AI systems
7. Robustness specifications for AI systems
8. Cybersecurity specifications for AI systems
9. Quality management systems for providers of AI systems, including post-market monitoring processes
10. Conformity assessment for AI systems

CEN and CENELEC Joint Technical Committee 21 Artificial Intelligence (JTC21) to responds to this standardisation request. The overarching idea behind this set of standards is that when the provider of the AI system has fulfilled all the requirements of these standards which are harmonised to the purposes and requirements of the AI Act, the provider has reached the assumption of conformity to the AI Act, and it can bring its product to the market. The purpose of this paper is to describe what are the intermediate results of this work and what are the challenges that the work has encountered.

The European Commission has expressed its opinion that no vertical sectors such as transport, machinery or health care should produce its sector specific AI standards at this stage. Instead, the standardisation experts of these vertical sectors should contribute to the development of these horizontal AI standards in such a way that they are directly applicable to these vertical sectors. For this reason, these standards are intended to be applicable to medical devices incorporating an AI component, too.

Material and methods

The material for this study consists of the AI Act, the standardisation request M/593, and the numerous internal documents produced during the standardisation work of JTC21. The experiences gained and opinions expressed in multiple working group meetings of JTC21 can also be mentioned as material to this document although the internal code of conduct of these meetings prevent the attribution of any unpublished statements to any individual standardisation expert.

The methods used in standard development follow the internal rules of CEN and CENELEC for standard development [5]. The work needs to respect the intellectual property of these standardisation organisations and allow access to the working documents only to the standardisation experts and national mirror panel members of JTC21 in the CEN and CENELEC member countries and to the approved liaison organisations of JTC21.

Results

AI Risk management standard

The AI risk management standard is intended to be used as an integrated part of the existing risk management system of the AI provider. It must cover the entire life cycle of the AI system. It must address all identified risks to health, safety or fundamental rights of people. The definition of risk, "the combination of the probability of an occurrence of harm and the severity of that harm" resembles that of the risk management standard ISO 14971 [6] generally applied by medical device manufacturers. The goal of the standard is to identify risks, evaluate them and mitigate the residual risks to an acceptable level. What is new in this AI risk management standard is that it addresses also the risks to the fundamental rights of people, like that of right to privacy as defined in the EU General Data Protection Regulation [7]. In this case the typical risk-benefit consideration is not applied, but the risk has to be removed completely. The AI risk management standard can contain a risk catalogue to help its users to identify many relevant risks although no such catalogue can list all the potential risks in all sectors.

AI cybersecurity standard

The AI cybersecurity standard identifies AI specific security threats and specifies an AI cybersecurity risk management process. It also specifies AI specific security controls. These include controls on model interface and attacks in data, data exposure controls, controls for testing and other controls, but it does not list typical general cybersecurity controls found elsewhere. There is a need to coordinate this standard with the AI risk management standard so that they are compatible to each other.

AI quality management standard

The AI quality management standard points out the additional requirements to an already existing management system of the provider organisation when it develops an AI system. In the medical device domain, that management system is typically based on the ISO 13485 quality management standard [8]. The purpose of the standard is to support the organisation to check that the topics 2 to 8 in the list in the introduction section of this document are sufficiently covered and stay at an acceptable level. The concept of quality is slightly different from the common understanding of quality. In the context of the AI Act, quality means adherence to the requirements of the AI Act. This stems from the footnote 20 of the EU Commission's "Blue Guide" on the implementation of EU product rules [9].

AI conformity assessment standard

The AI conformity assessment standard is intended to provide procedures and processes for conformity assessment activities related to AI systems and quality management systems of AI providers. There already exists a family of conformity assessment standards in the ISO CASCO toolbox [10] and the AI conformity assessment standard can refer to these standards. The new standard brings value by describing what AI related specialities need to be addressed in the conformity assessment of AI systems. A separate standard will probably be produced to provide criteria for assessing the competence of persons who perform conformity assessments to AI systems.

Quality and governance of datasets in AI

This standard aims at specifying in more detail what *Article 10 Data and data governance* in the AI Act expects from data sets in training, testing and validating the AI model and how they are managed.

The data sets must be representative, relevant, complete and correct.

AI trustworthiness framework standard

In this standard, trustworthiness is defined as the ability to meet stakeholder expectations in a verifiable way. This standard attempts to address the following aspects of AI systems in the list of the introduction section: Governance and the quality of datasets, Record keeping through logging capabilities by AI systems, Transparency, Human oversight, Accuracy specifications for AI systems, and Robustness specifications for AI systems. It also contains requirements for each life cycle stage of the AI system. In managing bias, it refers to the document ISO/IEC TS 12791 [11]. The AI trustworthiness framework standard draft received more than a thousand comments in a ballot in late 2024 and the WG is working on them.

Other AI standards

The standards described above are not alone sufficient to cover all the parts of the standardisation request M/593. JTC21 has studied other AI standards, particularly coming from JTC1/SC42 Artificial Intelligence [12] to fill in the identified gaps to the standardisation request. There are several SC42 standards that fill the gaps partly, but gaps are still remaining and need to be addressed somehow. An example of these is the ISO 24940 AI system logging standard being drafted in SC42.

The difficulty in using the global AI standards by SC42 is that the features required by the AI Act may not pass all the ballots in SC42 and the standard is not complete in the sense of the standardisation request M/593. The European version of the SC42 standard will then need to indicate which parts of the AI Act requirements are included in the standard and what are missing. This explanation is in the so-called Annex ZA of the European version of the standard.

Discussion

The task of preparing harmonised standards to the AI Act in the ten areas listed in the introduction above has turned out to be a difficult one and this short document can only scratch the surface of the work. Still, progress has been made in all standards described above. An additional challenge is to make all the standards to be developed consistent to each other. The development process involves the reconciliation of opinions to reach sufficient consensus, and the time required for this has already resulted in postponing the deadline from April 2025 to August 2025.

The specification of the technical requirements for AI systems requires expertise and understanding how the requirements could work in different sectors where AI systems are employed. One example of such difficulty is the proposal to require a consultation of the affected persons about their opinion on how well the AI system respects their fundamental rights. This may be quite relevant in some contexts but in the case of medical devices this can be an unnecessary burden. For example, if an embedded medical device which processes physiological signals, employs AI methodology to detect if any of its signal cables is disconnected or contains only disturbances, such consultation would not make sense. It is therefore important, that medical device experts contribute to the work to make the standards feasible to the health sector, too.

The results of the AI standardisation work will be evaluated by the European Commission. *Article 41 Common specifications* in the AI Act states that if the standards produced are not sufficiently good to provide presumption to be in conformity with the requirements of the AI Act or the standards are

delayed too much, the Commission may establish common specifications to be followed instead. It will be interesting to see how the Commission succeeds in the preparation of these specifications if it turns out that the available European standardisation experts fail in it.

Conflict of interest

The author declares no conflict of interest.

References

[1] EUR-Lex. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. European Union; 2024 [cited 2025 Jan 20]. Available from: http://data.europa.eu/eli/reg/2024/1689/oj

[2] European Commission. AI Act. European Commission; 2024 [cited 2025 Mar 5]. Available from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[3] EUR-Lex. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices. European Union; 2017 [cited 2025 Jan 20]. Available from: http://data.europa.eu/eli/reg/2017/745/2025-01-10

[4] European Commission. C(2023)3215 - Standardisation request M/593. Standardisation request to European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence. European Commission; 2023 [cited 2025 Jan 20]. Available from: https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en

[5] CEN. Reference documents. CEN; 2025 [cited 2025 Mar 5]. Available from: https://boss.cen.eu/reference-material/refdocs/pages/

[6] International Organization for Standardization (ISO). ISO 14971:2019 Medical devices — Application of risk management to medical devices. ISO; 2019.

[7] EUR-Lex. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union; 2016 [cited 2025 Jan 19]. Available from: http://data.europa.eu/eli/reg/2016/679/oj

[8] International Organization for Standardization (ISO). ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes. ISO; 2016.

[9] European Commission. Commission notice - The 'Blue Guide' on the implementation of EU product rules 2022. Official Journal of the European Union. 2022;65:C 247. EU; 29 June 2022 [cited 2025 Mar 26]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

[10] International Organization for Standardization (ISO). CASCO. Conformity Assessment tools to support public policy. ISO; 2025 [cited 2025 Mar 5]. Available from: https://casco.iso.org/home.html

[11] International Organization for Standardization (ISO). ISO/IEC TS 12791: 2024 Information technology — Artificial intelligence — Treatment of

unwanted bias in classification and regression machine learning tasks. ISO; 2024.

[12] International Organization for Standardization (ISO). ISO/IEC JTC 1/SC 42. Artificial Intelligence. ISO [cited 2025 Mar 10]. Available from: https://www.iso.org/committee/6794475.html