O Complementarity, Where Art Thou? Wading through the Medical Device Regulation and the AI Act Compliance: The case of Software as a Medical Device. A Primer

Francesca Gennari*

O COMPLEMENTARITY, WHERE ART THOU? WADING THROUGH THE MEDICAL DEVICE REGULATION AND THE AI ACT COMPLIANCE: THE CASE OF SOFTWARE AS A MEDICAL DEVICE. A PRIMER.
ABSTRACT: This article wants to answer a very concrete question: what is the legal regime applicable to Software as Medical Device (SaMD)? This question is prompted by the fact that Medical Software can also embed an AI system and, if that is the case, it needs to be compliant as well with the newly approved AI Act (AIA) and not only with the Medical Devices Regulation (MDR). By using the principle of complementarity adopted by the AIA, I will give a first outline of what this new combined compliance might look like. The short answer is that it does not appear to be easy for SaMD manufacturers to understand how to integrate new and partly new elements within the older legislation, the MDR, which has the objectives of the AI Act. KEYWORDS: Sustainable environment; ECHR draft protocol; future generations; climate justice; jurisdiction.

KEY WORDS: MDR; AI act; compliance; complementarity; notified bodies

SOMMARIO: 1. Introduction – 2. SaMD in the EU medical devices quality management system. The MDR and the MDCG guidance documents – 3. SaMD and the AI Act. What is new? – 4. Complementarity between the MDR and AIA. A short practical guide – 5. Open issues and operative suggestions – 6. Preliminary conclusions.

1. Introduction

This early-stage research article wants to answer just one important question: what is the legal regime applicable to Software as a Medical Device (SaMD) when it is AI-powered? It has been a few years since doctors, medical device companies, and Artificial Intelligence (AI) for medicine developers have claimed that the health sector is one of the most promising fields in which AI systems are going to be implemented.[1] From image diagnostics to genomics, AI has the potential of

* *PhD, Research Affiliate at Sant'Anna School of Advanced studies. Mail: Francesca.Gennari@santannapisa.it.*
This research was financially supported by the project "Biorobotics Research and Innovation Engineering Facilities "IR0000036" – CUP J13C22000400007". The article was subject to a double-bind peer review process.

making doctors' work more accurate and faster by relying on real-world data, while at the same time realising step by step a revolution in medicine leading to a more personalized and economically sustainable model than the actual one, which is based on standards, generalizations, and randomized clinical trials.[2] However, AI also has the potential to perpetuate discrimination and unfairness that was already present in the medicine field, specifically,[3] and in society in general terms.[4] These were part of the reasons for which the EU decided to pass a horizontal regulation on AI, the so-called AI Act (AIA), which the European Parliament and the Council of the EU approved last 13 March 2024 and entered into force on August 1st 2024.[5] This regulation combines a fundamental rights protection and risk management approach. For this article, it is important to note that the AIA will also apply to software with the characteristics of an AI system with medical applications. The applicable definition of AI system stems from the OECD one[6] and is intended mainly as software but has more specific characteristics: it must be a machine-based system that can work with different levels of autonomy which "exhibit *adaptiveness* after deployment and that, for *explicit or implicit objectives, infers*, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that *can influence physical or virtual environments*".[7] Nevertheless, even before the AIA's approval, there was already a compliance framework for medical devices (although not completely implemented): the Medical Devices Regulation (MDR).[8] The MDR also includes software as a possible medical device (MD) according to Article 2(1) MDR. Throughout this article, I will focus on the specific case of Software as a Medical Device (SaMD). The objective of this early study research is to help understand how one can wade across two complex product safety regulations such as the MDR and the

[1] E. J. Topol, *High-performance medicine: the convergence of human and artificial intelligence*, in *Nature Medicine*, 25, 2019, 44-56; partially contra E. Niemiec, *Will the EU Medical Device Regulation help to improve the safety and performance of medical AI devices?,* in *Digital Health*, 8, 2022, 1-8.

[2] P. Aurucci, *Il trattamento dei dati personali nella ricerca biomedica Problematiche etico-giuridiche,* Napoli, 2023, 55-59.

[3] Q. Feng et al., *Fair Machine Learning in Healthcare: A Review* in *ArXiv*, 2024, https://arxiv.org/abs/2206.14397 (last accessed 04/07/2024); H. Ledford, *Millions of Black People Affected by Racial Bias in Health-Care Algorithms* in *Nature*, 574, 608; K.L. Loewy, *Erasing LGBT People From Federal Data Collection: A Need for Vigilance*, in *American Journal of Public Health*, 107, 2017, 1217.

[4] C. Engel, L. Lindhart and M. Schubert, *Code Is Law: How COMPAS Affects the Way the Judiciary Handles the Risk of Recidivism,* in *Artificial Intelligence and Law*, 2024, https://doi.org/10.1007/s10506-024-09389-8 (last accessed 04/07/2024); B. A. Davis et al., *Examining Discrimination in Home Improvement Financing (Home Mortgage Disclosure Act 2012–2016) and Neighborhood Health in the United States,* in *Cities & Health*, 7, 2023, 1029.

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance),PE/24/2024/REV/1 OJ L, 2024/1689, 12.7.2024.

[6] OECD, *Explanatory Memorandum on the Updated OECD Definition of an AI System*, 2024, https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html (last accessed 04/07/2024).

[7] Article 3(1) AIA. Emphasis added.

[8] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC OJ L 117, 5.5.2017, p. 1–175.

AIA when there is the need to obtain the CE marking for SaMD.[9] This is not only done in the interest of the potential MDs' manufacturers or AI developers readers who are eager to put on the market their products and services as fast and as well as they can. It is also done in the interest of legal scholars at large for two reasons. Behind what might appear as arid and only technical compliance rules there are clear political, legal, and economic choices that are not evident rationales. However, these rationales underlie the policy choices and influence the well-being of millions of patients across the EU[10] and one of the most lucrative markets in the EU.[11] AI is our time's Copernican Revolution hence it is impossible to give a thorough assessment without understanding all its implications. One of the solutions is to involve the highest number of actors to study and comment on this process. EU legal scholars might still be perplexed insofar as the MDR compliance can be an interesting lens to understand epochal changes. To convince them, I argue that the relatively easy possibility to embed AI systems in consumer devices, MDs, and all other potential goods that are subjected to EU harmonization legislation is what makes the research question actual and of a consistent magnitude. If one thinks about it, the disrespect of these regulations- which are compliance safety regulations at their core- will have considerable effects in terms of both tort and contractual liability. If one of that product compliance requirements is not respected or is certified with negligence by a third party, how can a complainant prove their case? I will take as a case study SaMD because it offers a privileged perspective in connecting two disciplines, the MDR and the AIA, that are quite complex and that let emerge the key principle that will help understand the relationship between EU product safety regulations and the AIA.[12] This is the complementarity principle and it is set in Article 8(2) AIA. It is going to be the most important criterion concerning not only the MDR and the AI act but all the harmonized legislative acts that are recalled in Article 6(1) AIA, which concerns AI systems that can generate high-risk damages (more infra). As it will be argued further, the complementarity principle is not what is generally intended in International Criminal Law[13] or as guiding the application of the EU supplementary law[14] or as connected the relationship between the Commission and an EU Member

[9] I will argue infra on the preponderant product safety aspect rationale over the protection of fundamental rights one of the AIA.

[10] The European Patients Forum (EPF) estimates that through its members it can represent 150 million patients in the EU. EPF, *Annual Report-2023*, Brussels, 2023, 7, https://www.eu-patient.eu/contentassets/86bd0a8ae2d145ee9067614b6e690e62/annual-report-2023.pdf (last access 23/09/2024).

[11] Statista claims that the projected revenue in the Medical Devices market in the EU is likely to reach 144.10 billion US dollars in 2024. Prospectively, the market volume of Medical Devices Europe is likely to increase to reach 183.10 billion US dollars by 2029 worth. Statista, Medical Devices – Europe, https://www.statista.com/outlook/hmo/medical-technology/medical-devices/europe (last access 23/09/2024),

[12] See the list of legislations recalled at Annex I, AIA.

[13] ECCHR, "Complementarity principle", https://www.ecchr.eu/en/glossary/complementarity-principle/ (last access 23/09/2024).

[14] EUR-Lex. "The non-written sources of European Law" Supplementary law", https://eur-lex.europa.eu/EN/legal-content/summary/the-non-written-sources-of-european-law-supplementary-law.html (last access 23/09/2024).

State (MS) policy.[15] Instead, it is an emerging ordering criterion among subjects for which the EU has exercised the subsidiarity principle and harmonized subjects. In this case, the two harmonized disciplines would be the one concerning the medical devices, the MDR, and the AI, the AIA. In this case, it is a rationalisation principle that strives to eliminate rules which are the same or very similar in content but that need to be applied together, at the same time on the same object. This will be the case of SaMD which uses AI to work and is a medical device at the same time. While waiting for a clarification on its applications by the Commission, I will argue further that complementarity means that the main discipline is still, formally, the one that applies to the older harmonized discipline. The most uncertain point is how and when to add the elements that the newly approved AIA introduced. As there is no guidance on this matter, the rules about when to apply one discipline or the other, or a combination of the two, depend on the logic and the rationale of Article 8(2) AIA whose objective is to eliminate double and identical requirements. Hence, by using an exclusion logic about the existence or not of a requirement in the AIA or in the MDR, there are at least three main rules to decide which discipline to apply: i) if a rule/process/ requirement/duty is present in the AIA and not in the MDR, the AIA requirement will be added in the MDR conformity procedure; ii) if there is a rule /process/ requirement/duty that is present in both the AIA and the MDR but still adds a new element in terms of AI, one will have to evaluate how to integrate the AIA requirement in the MDR on a case by case basis; iii) if a rule /process/ requirement/duty is present in the MDR and not in the AIA, it will continue to exist. To do that, I will first summarise the concept of software as a medical device, SaMD, in the MDR and the connected guidance documents (2). Further, I will illustrate the relationship between SaMD and the different types of AI systems (3). Subsequently, I will outline a contrastive table on how the principle of complementarity will be applied and synthetised in a table (4). Then, I will point out some first impressions after analysing the previously cited table (5). In the end, there will be space for some preliminary conclusions (6). Further, as a methodological caveat, I will deal only with the aspects of compliance for MDs that also happen to be made of software that can be an AI system at the same time. Hence, I will exclude, or when impossible to do so, I will just hint, at all the issues concerning liability, which could stem from all the imperfections of the compliance process of AI as an MD. Even in terms of compliance, I will be synthetic in describing all the compliance requirements by the MDR and AIA in the interest of time and reading efficiency. I will also keep my focus on the EU regulatory landscape, for the same reasons. However, when relevant, I will cite the US sources that are relevant for an on-the-spot comparison.

2. SaMD in the EU medical devices quality management system. The MDR and the MDCG guidance documents

Before diving into the intricacies of SaMD, it is worth remembering the rationale underpinning the MDR. The MDR's rationale is not that different from the one of its predecessor, meaning the old

[15] EUR-Lex, "Complementarity between EC and Member State Policies", https://eur-lex.europa.eu/EN/legal-content/summary/the-non-written-sources-of-european-law-supplementary-law.html (last access 23/09/2024).

ISSN 2284-4503

Medical Device Directive (MDD).[16] The MDR sets up a system that divides MDs according to the level of risk they can bring to life and human health in case they malfunction or are defective.[17] This was also the main aim of the MDD.[18] Moreover, the MDR sets a minimum threshold of general safety and performance requirements that manufacturers need to respect.[19] In this, the MDR is not different from the MDD[20] and other types of EU product safety regulations such as the recently approved Machinery Regulation (MR)[21] and the General Product Safety Regulation (GPSR).[22] Coming back to the risk management division and the MD division in risk classes, in the MDR there are four risk classes for MDs: I, II a), II b), and III, in growing order of risk.[23] The more the MD is dangerous, the more the manufacturer needs to comply with specific product safety compliance requirements.[24] The result is that, for medium to high-risk products, the manufacturers put in place a quality management system whose basis is the concept of risk management as an iterative and continuous process of adjustment to the ever-changing circumstances in which the MD will have to function.[25] That is why one novelty compared to the previous regime is that the manufacturer must give clinical evidence that its MD is safe and effective.[26] Moreover, another noticeable change compared to the MDD is that the MDR builds a complex set of requirements concerning product monitoring, hence the traceability of the MD after it has been put into service. Thus, it makes it necessary for the manufacturer to have a post-market surveillance system which will need to be constantly updated.[27] This private monitoring is complemented by the member states' (MS) market surveillance systems through competent au-

[16] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices OJ L 169, 12.7.1993, p. 1–43.

[17] Recital 2 MDR and K. SHATROV, C. R. BLANKART, *After the Four-Year Transition Period: Is the European Union's Medical Device Regulation of 2017 Likely to Achieve Its Main Goals?* in *Health Policy*, 126, 2022, 1234.

[18] Recital III MDD explained the necessity of harmonizing national provisions concerning safety and health protection of medical devices.

[19] Annex I MDR.

[20] The MDD divided the MDs in four different risk classes: I, IIa, IIb, III according to Article 9(1) MDD. Starting from these classes, then, the manufacturer could choose conformity procedures such as the ones described in Articles 11 and 12 and Annexes II, III, IV, V, VI, VIII which should grant the conformity of the MDs with the then ECC standards for the creation of the internal market. On the continuity between MDD and MDR and the efficiency of the latter see among others, A. NÜSSLER, T*he New European Medical Device Regulation: Friend or Foe for Hospitals and Patients?* in *Injury*, 2023, 54, 110907; and K. SHATROV and C. R. BLANKART, *op. cit*., 1234-1239.

[21] Article 8 and Annex II of Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC, PE/6/2023/REV/1 OJ L 165, 29.6.2023, p. 1–102.

[22] Chapter II of Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC. PE/79/2022/REV/1 OJ L 135, 23.5.2023, p. 1–51

[23] Article 51 MDR.

[24] Article 52 MDR in combination with Annexes IX to XI MDR and Annex XIII for custom-made devices.

[25] Annex I, Chapter I, 3, MDR.

[26] In this sense all MDR's chapter VI and Annex XIV are about clinical evaluation and investigations. For the criteria to conduct a clinical evaluation on certain classes MD see Article 61(3) MDR. On the need to have a clinical evidence system for medical devices and not for medicines as well, see, among others, A. G. FRASER ET AL., *The Need for Transparency of Clinical Evidence for Medical Devices in Europe* in *The Lancet*, 392, 2018, 521.

[27] See more in depth Chapter VIII which also gives guidelines on the MS's market surveillance main rules (section 2 of the same chapter).

thorities (these authorities are or will depend on the national health ministries). The rationale behind putting into the market a safe MD is easy to grasp. This applies as well to related services that have medical functions. This result will be achieved also by having a single database where to find all the approved MDs, called EUDAMED,[28] and by the fact that the approved devices have a unique identification number, named UDI.[29] These last two requirements are certainly enabled by new kinds of technologies, such as RFID tags, Internet of Things (IoT) objects, and AI-based security systems which allow to always be able to locate a device.[30] It is noteworthy to point out that perhaps the real motivation for general safety and performance requirements was a series of past medical device scandals and the struggles that EU citizens experienced in trying to find an accountable and liable subject.[31]

From an EU policy point of view, one can place the MDR as part of the new legislative framework[32] of the EU Commission, which followed the MDD New Approach.[33] In the case of the MDR, the manufacturer needs to design and create a product that follows state-of-the-art standards. In case the risk that its product potentially generates is low, the manufacturer's self-certification is enough to obtain the CE conformity label such as for class I MD. When the risk is higher, a third party, called Notified Body (NB), must verify that the product is not dangerous and that it respects a minimum level of health and safety requirements.[34] This is the case for all the other classes of risk except the first one, meaning II a, IIb, and III in the new MDR. Notified Bodies can be either private, public, or public/private auditing and certifying entities that are selected by MS and approved by the EU Commission.[35] Their function is to enhance trust in the health and safety of the products.[36] In the MDR they received extensive attention because of the previously said MD scandals[37] which were also enabled

[28] Articles 33-34 MDR describing the main features of EUDAMED.

[29] Articles 27- 29 MDR on the UDI's main features and Annex VI MDR.

[30] J. LUZAK, *A Broken Notion: Impact of Modern Technologies on Product Liability* in *European Journal of Risk Regulation*, 11, 2020, 635.

[31] F. GENNARI, *What Liability with the Internet of Things? Insights from the European Case-Law of the PIP Affair,* in *Global Jurist,* 23, 2, 2023, 125; B. VAN LEEUWEN, *La responsabilité des organismes notifiés du fait d'implants mammaires défectueux: TÜV Rheinland devant les tribunaux français et allemands* in *Revue internationale de droit économique*, t. XXIX, 2015, 69.

[32] European Commission, New Legislative Framework, https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en (last access 23/09/2024).

[33] European Commission, Enhancing the implementation of the New Approach Directives https://eur-lex.europa.eu/EN/legal-content/summary/enhancing-the-implementation-of-the-new-approach-directives.html (last access 23/09/2024).

[34] P. ROTT, *Certification of Medical Devices: Lessons from the PIP Scandal*, in P. ROTT (ed.), *Certification – Trust, Accountability, Liability*, Cham, 2019, 189.

[35] At the moment of speaking there are 31 NBs in the EU. More information available at https://webgate.ec.europa.eu/single-market-compliance-space/#/notified-bodies/by-country (last access 04/07/2024).

[36] V.I. DASKALOVA and M.A. HELDEWEG, *Challenges for Responsible Certification in Institutional Context: The Case of Competition Law Enforcement in Markets with Certification* in P. ROTT (ed.), *Certification – Trust, Accountability, Liability*, Cham, 2019, 24-28.

[37] In the new MDR, there is an entire chapter (Chapter IV MDR) and one annex (Annex VII MDR) dedicated to them and their obligations but still no form of accountability or liability is foreseen for patients which might have experienced damages because of a NB's negligence in evaluating the safety of an MD. The only exception is whenever the NB has outsourced some of its functions to a subcontractor which has carried out the conformity assessment for the MD in question. See Article 37(2) MDR.

ISSN 2284-4503

by NBs' negligence. The Court of Justice of the EU (CJEU) indirectly ascertained this behaviour in the notorious *Schmitt* case.[38] The French Cour de Cassation followed the CJEU's input and granted compensation to the victims based on the then-applicable MDD, contrary to Germany.[39] To sum up, this thorough and lengthy conformity process allows the product to be put into the market, or, if it is a service, to be put into service, and to circulate across all the twenty-seven EU MS.

All these old[40] and new product safety rules apply as well to software. In the MDR, the software is a SaMD only if two cumulative conditions are met, like for all other MDs. The first one is that it must have at least one of the monitoring, diagnostic, and therapeutic functions described by Article 2(1) MDR[41] and that the intended purpose is that the object is an MD.[42] This last condition only depends on the manufacturer. The MDR defines intended purpose as "the use for which a device is intended *according to the data supplied by the manufacturer* on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation."[43] This last condition is crucial: in fact, an object could have a medical function but could also not be an MD at the same time. For instance, a smartwatch can monitor the heartbeat and alert

[38] *Elisabeth Schmitt v TÜV Rheinland LGA Products GmbH*, C-219/15, ECLI:EU:C:2017:128. For a comment of the case see A. WALLERMAN, *Pie in the Sky When You Die? Civil Liability of Notified Bodies under the Medical Devices Directive: Schmitt*, in *Common Market Law Review*, 2018, 55, 265-278.

[39] The French *Cour de Cassation* recognised the right of the injured women to receive compensation from TUV France, finding that its mother branch, TUV Germany, had been negligent in its audit of PIP defective breast prosthesis. See *Cour de Cassation, Première Chambre Civile, Arrêt n° 616 du 10 octobre 2018* (17–14.401), ECLI:FR: CCASS:2018:C100616. This was not the case in Germany, where NB was not considered part of the contractual relationship between the patient and the producer of the defective product. Judgement of the VII Civil Senate of 22.6.2017 - VII ZR 36/14, ECLI:DE:BGH:2017:220617UVIIZR36.14.0 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=78997, and Judgement of the VII Civil Senate of 27.2.2020 - VII ZR 151/18, ECLI:DE:BGH:2020:270220UVIIZR151. 18.0, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2021&nr=104766&linked=urt&Blank=1&file=dokument.pdf (last accessed 04/07/2024).

[40] In the MDD, software was not formally included in the definition of MD, but given its growing importance, the Commission, through the experts group Medical Devices Coordination Group issued the *Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices (MEDDEv 2.1/6)* in which it was included.

[41] Article 2(1) in particular recites as follows: "For the purposes of this Regulation, the following definitions apply: (1) 'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of, or compen sation for, an injury or disability, — investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, — providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means. The following products shall also be deemed to be medical devices: — devices for the control or support of concept ion; — products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point". Emphasis added.

[42] Article 2(1) and Article 51(1) in combination with Annex VIII, Chapter II, 3.1 MDR.

[43] Article 2(12) MDR. Emphasis added.

the owner if there are alterations to their vitals. Monitoring to prevent a disease is one of the medical functions set in Article 2(1) MDR. However, the manufacturer is not likely to certify this device as an MD also because of the complex set of compliance duties which include the organization of clinical investigations, and of post-market surveillance constantly updated mechanism described before. It is worrisome, but the intended purpose of the manufacturer is going to become a problem with the development of more complex software (including AI and the IoT) which drives or is on its own a SaMD. The rationale of the MDR is to provide safer medical devices and, if the intended purpose of the manufacturer is, in practice, the most important rule on the decision about whether a device is a medical device, this will likely cause an increase in the marketing of *de facto* medical devices powered through AI and/or the IoT, which will be less safe than certified medical devices.[44] They would be only consumer devices from an EU regulatory point of view and only the GPSR would apply. On the one hand, it is true that the GPSR is more recent than the MDR and considers software as part of connected products such as IoT objects.[45] However, it lacks a refined quality management system of product requirements and third-party certification system elements which in the MDR is present. One must admit, however, that the new GPSR has improved in the detail of general safety requirements and there is a new focus on cybersecurity and AI which is not as explicit in the MDR[46]. Nevertheless, the primacy of the intended purpose is not going to change anytime soon as the CJEU established its essential character in at least two important judgments. In the recent *Snitem*[47] case, and even before that, in the *Brain Products*[48] case, the CJEU granted that the manufacturer's intended purpose interpreted as the product description of the device, is the element to look at also in case of doubts concerning the medical functions of the device. Ludvigsen and others have provided an interesting guide on how to interpret the "implicit/indirect" intention of the manufacturer, especially when a device can have a *de facto* medical function but the manufacturer's intended purpose is that it is a consumer object.[49] Nevertheless, I fear that if their way of reasoning is not integrated into

[44] F. GENNARI, *Mixed-Functions IoT devices: a Regulatory and Liability Requirements' Maze. A First Overview*, in *European Journal of Risk Regulation*, forthcoming (2024).

[45] Recital 25, and Article 3(1)GPSR. This article defines a product as "any item, *whether or not it is interconnected to other items*, supplied or made available, whether for consideration or not, including in the context of providing a service, which is intended for consumers or is likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them." Emphasis added

[46] Article 5 GPSR lays down on all economic operator the duty to ensure general level of object safety. Article 6 GPSR lists all the elements that should be considered also (g) cybersecurity features and (h) "*the evolving, learning and predictive functions* of the product", which in practice refers to AI systems mentioned supra in 1. Emphasis added.

[47] *Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé*. C-329/16, ECLI:EU:C:2017:947. For a commentary of the case, T. MINSSEN, M. MIMLER and V. MAK, *When Does Stand-Alone Software Qualify as a Medical Device in the European Union?—The Cjeu's Decision in Snitem and What It Implies for the Next Generation of Medical Devices* in *Medical Law Review*, 28, 2020, 615.

[48] *Brain Products GmbH v BioSemi VOF and Others*, C-219/11, ECLI:EU:C:2012:742.

[49] K. LUDVIGSEN, S. NAGARAJA and A. DALY, *When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law* in *European Journal of Risk Regulation*, 1, 13, 2022, 90-91.

ISSN 2284-4503

some specific guidelines by the EU Commission's Medical Devices Coordination Group (MDCG),[50] or, better, by the CJEU itself through perhaps a preliminary ruling and by giving a more articulated interpretation of Article 2(1)'s intended purpose meaning, manufacturers will not have the incentive to market new technologies with medical functions as medical devices under the MDR.

However, even before the MD manufacturer decides to market software (which can also be an AI system, more on this later) as a SaMD, they will need to understand – leaving momentarily the issues concerning the intended purpose aside – whether the software in question is a medical device or not. In this section of the article, we are going to focus on the rules within the MDR first, and then on the MDCG guidance documents concerning the qualification of software as SaMD. The MDR does not give indications on this issue in the main text. In a way, the generality of the MDR towards software and connected objects is a good thing for now as it does not make this legislation old before it has received full implementation.[51] The general implementing rule number 3 in Annex VIII frames the SaMD as still something functional to the main device. As a result, the class of risk is determined by the class of risk of the device that the software drives.[52] The same rule also specifies that if software acts independently from the device, then the manufacturer will need to assess its class of risk separately from the one of the device(s) with which the SaMD to classify might work. This distinction is bound to become more and more difficult to practically apply as it will be further analysed (*infra* Section 4). The first reason is that software never acts in a void, but always within an internet structure that is also made up of hardware.[53] As an example, think about cloud storage services: they cannot exist on their own as they depend on a very concrete server infrastructure.

The second set of criteria that needs considering, once the manufacturer established that their software is a SaMD, is in Annex VIII, rule 11. This set of rules gives inputs on how to assess the risk of the SaMD. It is interesting to notice that even when the AIA was not even remotely a proposal, the MDR considered that software could in theory cause a wide range of risks for humans, from almost non-existent damages to death. The preliminary rule to keep in mind when trying to assess the risk class of the medical device is implementing rule 3.3 of Annex VIII. It states that the medical functions of software are divided into two groups. The first one concerns SaMD which is used to provide informational support to doctors with diagnoses and other therapeutic purposes. It is not surprising that this is the first example of SaMD as it has been demonstrated that AI-powered SaMD with diagnostic or therapeutic functions is the MD kind that has been most successful and started being marketed as MD in the US and the EU even before talks about the AIA.[54] This kind of (AI-powered) SaMD should

[50] The MDCG is an expert pool on different issues concerning medical devices and in vitro products appointed by the EU Commission and it is structured in several working groups and is created by Article 103 MDR. To know more https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties/medical-device-coordination-group-working-groups_en, (last access 23/09/2024).

[51] E. STEINDL, *Consumer Neuro Devices within EU Product Safety Law: Are We Prepared for Big Tech Ante Portas?* in *Computer Law & Security Review*, 52, 2024, 105945.

[52] This is also one of the main differences with the definitions of SaMD in the MDR compared to the SaMD as defined by the International Medical Devices Regulators Forum, which only considers SaMD only if its function is independent from the device. See IMDRF, *Software as a Medical Device (SaMD): Key Definitions*, 2013, 6.

[53] C. REED, *Internet Law. Text and Materials, second edition,* Cambridge, 2004, 7-23.

[54] C. JONES, J. THORNTON and J. C WYATT, *Artificial Intelligence and Clinical Decision Support: Clinicians' Perspectives on Trust, Trustworthiness, and Liability*, in *Medical Law Review*, 31, 2023, 501; M. NAGENDRAN and others,

be considered class II a (medium-low risk). Further, the SaMD can have the same functions (support in therapy and diagnostic), but the kind of negative outcome on the patient will determine the labelling of risk under the MDR. If it causes death or "an irreversible deterioration of a person's state of health"[55] then it will be class III. Instead, if it can cause a "serious deterioration of a person's state of health or a surgical intervention" it will be class IIb.[56] The second group of SaMDs are the ones concerning monitoring of "physiological processes",[57] which are generally considered as belonging to group IIa. The exception to this rule applies only when the SAMD does the monitoring of "vital physiological parameters"[58] and "where the nature of variations of those parameters is such that it could result in immediate danger to the patient".[59] In that case, the SAMD "belongs to class IIb".[60] The rest of SAMD is considered as class I as a residual option.[61]

As the almost final piece of this puzzle, we must add the 2019 MDCG Guidance (hereinafter Guidance 2019) on how to understand whether the software is a SaMD or not.[62] The Guidance 2019 is a soft-law document whose purpose is to integrate the unclear or too general provisions in the MDR about SaMD. Despite its soft-law character, it is authoritative as it is authored by the medical devices expert of the MDCG and applied by all the stakeholders who might be interested in marketing SaMD. This guidance tries to answer one question: when is software SaMD? Publishing this document was necessary because – as already pointed out *supra* – it is not easy at all to understand whether a SaMD is such from the text of the MDR. This is because the focus might be too broad or too narrow according to the different importance that we might give to two different MDR requirements. If the focus is more on the definition of Article 2(1) MDR, then, quite an important set of software could be SaMD as many types of software in consumer objects can have medical functions as described in Article 2(1) such as vitals monitoring. If, on the other hand, there is too much attention on the intended purpose, the risk is that MDs are *de facto* marketed as consumer objects with fewer costs and compliance to bear. Consequently, a manufacturer could draw up the description of the intended purpose in a way that makes it explicit that their product or service is not an MD. According to the CJEU, this needs to be considered when deciding if a product is or is not an MD.[63] Perhaps, to avoid the (practical) over-reliance on the intended purpose criteria, the MDCG has tried to give less arbitrari-

Artificial Intelligence versus Clinicians: Systematic Review of Design, Reporting Standards, and Claims of Deep Learning Studies in *BMJ*, 2020, 368, m689; U. J. MUEHLEMATTER, P. DANIORE and K. N. VOKINGER, *Approval of Artificial Intelligence and Machine Learning-Based Medical Devices in the USA and Europe (2015–20): A Comparative Analysis*, in *The Lancet Digital Health* 3., 2021, e195; F. PESAPANE ET AL., *Artificial Intelligence as a Medical Device in Radiology: Ethical and Regulatory Issues in Europe and the United States* in *Insights into Imaging*, 9, 2018, 745.

[55] Annex VIII, Rule 11, 6.3.

[56] *Ibidem.*

[57] *Ibidem.*

[58] *Ibidem.*

[59] *Ibidem.*

[60] *Ibidem.*

[61] *Contra*, Ludvigsen Nagaraja and Daly who instead consider software as belonging to class I as the default option. K. LUDVIGSEN, S. NAGARAJA and A. DALY, *op.cit.*, 84.

[62] MDCG, *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 -MDR and Regulation (EU) 2017/746- IVDR.* 2019.

[63] See para 24 *Snitem* case, and *Brain products* case paras 17-18.

ness to the meaning of SaMD in all its applications. These guidelines apply as well to the "twin" regulation of the MDR, the In Vitro Devices Regulation (IVDR).[64] The guidelines define software in a very general way "[…] as a set of instructions that processes input data and creates output data."[65] Then, all the relevant definitions of both the MDR and IVDR apply, including the definition of MD and medical purpose. However, this guidance needs application only as long as it is not annulled by the CJEU through as preliminary ruling. This is because the CJEU has the last word concerning the interpretation of acts of the EU, its institutions, agencies, and bodies, including the ones created by legal acts such as the MDCG.[66] Until this moment, however, the CJEU could not review these guidelines through preliminary reference cases or other procedures. In what then, this 2019 Guidance is useful? It is useful as it reinforces the implicit division between dependent and independent software which is addressed in other terms compared to the MDR. In the 2019 guidance there is a distinction between software that drives the MD and software that is independent of other devices. Nevertheless, the guidance makes a further distinction: software can be present within an MD but can also not be an MD when it "is intended to drive or influence the use of a (hardware) medical *device and does not have or perform a medical purpose on its own*, nor does it create information on its own for one or more of the medical purposes described in the definition of a medical device".[67]

In the end, the 2019 Guidance provides a clearer decision tree which gives some simple rules to follow to qualify software as SaMD.[68] The first question a manufacturer must ask themselves is whether the product is "software according to the guidance".[69] Given the generality of the definition, quite a huge number of applications (even AI-based ones) could be in this guidance's field of application. If the answer to this question is positive, then the manufacturer must understand whether the product "is an MDR Annex XVI device,[70] or is an accessory for a medical device, 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."[71] If this is not the case, then one must wonder whether the action is for the benefit of individual patients. If also that is true, then one must ask if it has the meaning of medical device software under the guidance. If yes, the answer is yes, then the MDR applies.

What does it all mean concretely? *Supra* I explained that depending on the SaMD's risk classification there were different procedures that the manufacturer could choose from. They are listed in Annexes from IX to XI.[72] Here follows a synthetic table of the several combinations that Article 52 MDR sets

[64] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.
OJ L 117, 5.5.2017, p. 176–332.
[65] Guidance 2019, 5.
[66] Article 19(3)(b) TEU.
[67] *Ibidem*, Emphasis added.
[68] Guidance 2019,9.
[69] Guidance 2019,9.
[70] These are products without an intended medical purpose that for policy reasons have been included in the list of MDs. Some examples are contact lenses, lasers and intense pulse light treatment, and equipment used for brain stimulation.
[71] Guidance 2019, 9, emphasis added.
[72] Article 52(1) MDR.

out starting from the least risky (I) to the riskiest of all (III). To connect all the elements listed until now, here follows a table indicating the classes of risk, the conformity procedures, what these procedures consist of (in general) and an example of SaMD for each class.[73]

MDR Risk class	Conformity procedure according to Article 52	Type of the procedure	How does it work	Example for SaMD
I	None just **technical documentation (Annex II and III)**	Conformity Self-declaration	The manufacturer self-declares that they have respected all the duties established in the MDR and that they have followed the state-of-the-art requirements and the contents of Annex II and III. In short, the manufacturer self-certifies their own MD (for the declaration of conformity	It is plausible to think about a SaMD which alters the presentation of data for a medical purpose e.g. "searching image for findings that support a clinical hypothesis as to the diagnosis or evolution of therapy" or "software which locally amplifies the contrast of the finding on an image display so that it serves as a decision support or sug-

[73] Even if not formally mentioned, all these SaMD applications could also be employed in custom-made devices. However, it is a specific topic that needs its own explanation, a part of which will appear in I. FAGIOLI, A. MAZZARINI, E. TRIGILI, F. GENNARI, S. CREA, N. VITIELLO, *The Role of Artificial Intelligence and Machine Learning in Personalizing the Control of Robotic Lower limb Prostheses*, forthcoming 2025.

			see Article 19 and Annex IV)	gests an action to be taken by the user" Guidance. P.7.
II a	**Chapters I and III of Annex IX** + technical documentation	Annex IX CONFORMITY ASSESSMENT BASED ON A QUALITY MANA GEMENT SYSTEM AND ON ASSESSMENT OF TECHNICAL DOCUMENTATION Chapter I, Quality Management System; Chapter III Administrative provisions	The quality management system of the manufacturer is subjected to an audit by a NB and must ensure some administrative provisions such as keeping at the disposal of competent authorities the relevant documentation concerning the obtention of the conformity declaration.	SaMD in this case can be both software that is used for diagnosis purposes (e.g. radiology application to find out cancers or other diseases) and/or for monitoring physiological parameters. As an example of this, one can think of a wearable heart-beat monitoring device which also has an app for visualizing the concerned vitals and whose vitals are shared with the patients' MD.
II b	(except custom-made or investigational devices) **Chapter I and III**	Annex IX CONFORMITY ASSESSMENT BASED ON A QUALITY MANA GEMENT	The description for the previous procedure applies here but there	An application of SaMD in this case could be a software which provides insulin

	Annex IX However, for class II b implantable devices assessment of technical documentation applies for every device (Section I Annex IX). Or, the manufacturer may choose to apply a conformity assessment based on type examination as specified in Annex X coupled with a conformity assessment based on product conformity verification as specified in Annex XI.	SYSTEM AND ON ASSESSMENT OF TECHNICAL DOCUMENTATION Chapter I,Quality Management System; Chapter III Administrative provisions Or ANNEX X: CONFORMITY ASSESSMENT BASED ON TYPE-EXAMINATION + CONFORMITY ASSESSMENT BASED ON PRODUCT CONFORMITY VERIFICATION	will also be an assessment by a NB of the technical documentation. Alternatively, the manufacturer will need to request the NB to carry out an assessment not on the basis of a sample of the production of MDs. Then, this procedure will need to be completed with the either one of the two procedures indicated by Annex XI. The first one is called production quality assurance and it is an audit of the quality management system. Alternatively, the	dose recommendations to a patient regardless of the method of delivery of the prescribed dose, whether via an insulin pump, insulin pen or insulin syringe. This can lead to an irreversible change of the state of health as described in rule 11 on software risk classification

			product verification's procedure aim is to grant the conformity certification after the examination of every manufactured device-.	
III	(other than custom made devices or investigational devices) conformity assessment as specified in Annex IX. Alternatively , the manufacturer may choose to apply a conformity assessment as specified in Annex X coupled with a conformity assessment as specified in Annex XI	Annex IX CONFORMITY ASSESSMENT BASED ON A QUALITY MANA GEMENT SYSTEM AND ON ASSESSMENT OF TECHNICAL DOCUMENTATION Or ANNEX X: CONFORMITY ASSESSMENT BASED ON TYPE-EXAMINATION + CONFORMITY ASSESSMENT BASED ON PRODUCT CONFORMITY VERIFIC ATION	An alternative between previous descriptions of the two classes	It could be the case of a SaMD powering a next generation pacemaker or defibrillator which analyses in real time the vitals of the patient. If it does not respond quickly and in the right way to an emergency the patient might die

Table 1. Correspondences between MDR risk classes and conformity procedures for SaMD

The real issue is that the manufacturer can follow the rules detailed in Annexes IX to XI and, from devices classes IIa to III, request the audit and assessment of an NB. Nevertheless, in the MDR the indication of these procedures is general, as they are thought for a wide range of products that go from contact lenses to innovative SaMD. The practical details are left *de facto* to NBs. Moreover, the clinical evaluation of the MD is an essential step of the MDR conformity procedures and is valid for all the classes of risk.[74] In addition to that MDs belonging from class IIa (implantable) IIb a to III will need to be certified compliant also by showing that their manufacturer carried out clinical investigations[75] and all the classes of risk will need to provide clinical evidence that their MD is safe. That is why the MDCG published a new guidance for SaMD to evaluate the clinical soundness of the deployment of SaMD (Guidance 2020).[76] These criteria explain basic rules that already doctors or any person involved in academic research should be familiar with concerning the collection of clinical evidence and the validation of clinical data. More uncertain is whether a small-medium manufacturer or a university researcher has a clear idea of how to conduct a clinical investigation, which in any case results in more costs and more time employed before having a SaMD put into the market. Moreover, most classes of risks will require the need for an NB audit. However, despite there is an evident justification in having a more protected right to health and safety through the MDR thanks to the requirement of clinical evidence and post-market surveillance, most of the actors involved in the creation of medical devices do not have the same resources as the international manufacturing groups. In some countries such as Italy, biomedical research of this kind (especially for rehabilitation robotics and AI for health development) is carried out in research institutions such as in university hospitals or facilities or SMEs that do not have (yet) a comprehensive quality management system, nor MDR compli-

[74] Article 61 (1) and Annex I and III, IV MDR.

[75] Article 61-80 and Annex XIV.

[76] To give more context, this guidance follows criteria that should already apply to the scientific research in general, such as "[...] establishing and maintaining a clinical evaluation (MDR) plan and criteria applied to generate the necessary CLINICAL EVIDENCE based on the characteristics of the device; identification of the relevant data pertaining to the performance and/or safety of the device and any remaining unaddressed issues or gaps in the data; Appraisal of the relevant data in terms of quality and contribution to the Clinical Evaluation; Analysis of the available data and its relevance with regard to demonstrating conformity with thr relevant General Safety and Performance requirements; Documenting the relevant data, their assessment and the clinical evidence derived therefrom in the clinical evaluation (MDR); updating the clinical evaluation and its documentation throughout the life cycle of the MDSW concerned with data obtained from implementation of the manufacturer's Post Market Clinical Follow-up / Post Market Performance Follow-up (PMCF /PMPF) plan […]". All these requirements are schematised in a flowchart within the same document at page 9. Each of these principles is explained in a more granular way in the following pages and annexes are explaining how to generate clinical evidence (Annex I) and an example of clinical evaluation and how to consider relevant scientific literature, clinical investigation, and clinical performance studies (Annex II). MDCG, 'Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software', 2020, 9-21 and ff.

ance experts as the ones required by the MDR.[77] The drawback of this is that there might be innovative ideas that are not going to pass the review of the Ethical Committee. Not knowing that one must follow good compliance practices to be MDR compliant and, more specifically, the ISO 14155:2020[78] standard to conduct clinical investigations to market an MD (SaMD included) impacts the chances that the SaMD clinical investigation plan is rejected by the competent national ethical committee. This problematic situation also partly explains, as well as the pandemic, the delays in the final implementation of the MDR.

3. SaMD and the AI Act. An additional risk-management hierarchy

As previously mentioned in the introduction, SaMD is a hot topic not only as far as the MDR is concerned but also when AI is. After explaining what an AI system is in the introduction and describing what the SaMD is according to the MDR and relative guidance documents, it is now time to connect these two parts of the article. The *fil rouge* between the MDR and the AIA is software. It is the foundational element both of "traditional" SaMD and AI systems as we know them. However, the relationship between SaMD and AI seems the one the biggest Russian doll has with the smaller ones. With all the information gathered until this moment, it is easier to create a diagram of software applied to medical things. At the outer layer- the biggest Russian doll to follow on the example- there is software integrated into a medical device, but that does not have a medical function and that its manufacturer does not consider as an MD. This would be the largest outer layer of our scheme concerning software applied to medical devices. To clarify even further, it is the software that the MDCG guidance wanted to exclude from the MDR field of application. We can name it simply as software (not MD). Then, a subset of this first kind of software used in MD is a properly certified or certifiable MD and can either drive hardware or be a standalone software. This is what we could call "traditional" SaMD. To have a SaMD we need to i) check that the function of the device is a medical one according to Article 2(1) MDR; ii) make sure that the intended purpose of the manufacturer, and iii) to assess its risk class through Article 51 and Annex VIII rules 3 and 11.

How does AI, which has been already employed for a few years in certified medical devices[79] get its place in this series of layers/progressively smaller Russian dolls? I have already explained the generality of the MDR and the lack of any mention whatsoever of AI. To be fair, up until 2019, the publishing year of the MDCG guidance on medical software, there had not been a proposal such as the AIA. To deal with AI-based SaMD, the MDCG could have relied only on soft-law documents such as the Ethi-

[77] To get more statistical data on the Italian MD manufacturing landscape visit the Confindustria Medical Devices division, https://www.confindustriadm.it/il-settore-in-numeri-2024/ (last access 23/09/2024). See also Article 15 MDR about the qualifications and duties of the person responsible for regulatory compliance.

[78] See more at https://www.iso.org/obp/ui/#iso:std:iso:14155:ed-3:v1:en (last access 23/09/2024).

[79] It is much easier to identify how many AI-based MDs are marketed on the US market compared to the EU market as the EUDAMED database and the UDI system are not still completely implemented. To get an idea of the kind of AI-based SaMD on the US market see FDA, Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices (last access 23/09/2024).

cal Guidelines for a Trustworthy AI[80] and the trustworthy AI checklists[81], authored by the same group of High-Level Experts appointed by the EU Commission. Even if the MDCG had wanted, it could not have provided a comprehensive legal framework for AI systems as the first AIA proposal was presented only in April 2021.[82] However, as explained in Section 1, there were already AI applications for medical purposes in the EU and the US even before comprehensive AI regulation.[83] This proves the existence of a further subset within SaMD. The latter includes AI-based SaMD. For instance, let us think of software driving a surgical robot for the first case, and software applied to radiology as the second case. If this kind of software has also the characteristics listed by the definition of AI system in the AIA (and is in general powered by well-known AI techniques such as machine learning and deep learning), then we will have to combine all the duties examined on the SaMD both in the MDR and the MDCG guidance and apply them and adding them to the ones that the AIA is adding as well on AI systems. However, the Russian doll of SaMD does not stop here. Because of the fast development due to the scalability and generality of the altogether new paradigm introduced by foundation models,[84] such as Chat-GPT, or Gemini, a new layer of SaMD must be considered and it can be called foundation-model-based SaMD. It must not be excluded that this recent technology stemming from 'traditional' AI techniques might soon be integrated into medical devices and be able to drive them. Let us think for instance of conversational robots or chats which were trained extensively, and their use is a medical one as support to psychological or psychiatric therapy.[85] Their ability to respond to the patient is due to the use of large language models which are none other than a specific subset of the foundation model category. Here follows the practical representation of the different subsets of the SaMD Russian doll described so far.

[80] Ethical Guidelines for a Trustworthy AI https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (last access 23/09/2024).

[81] Assessment list for trustworthy artificial intelligence (ALTAI) for self-assessment https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (last access 24/09/2024).

[82] Proposal for a Regulation of The European Parliament and of The Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts com/2021/206 final.

[83] U.J.MUEHLEMATTER, P. DANIORE and K.N. VOKINGER, *op.cit*.

[84] R. BOMMASANI ET AL., *On the Opportunities and Risks of Foundation Models*, in *ArXiv*, 6-13, 2022, https://arxiv.org/abs/2108.07258, (last access 04/07/2024).

[85] J. LAPOOK, *Mental Health Chatbots powered by artificial intelligence developed as a therapy support tool*, in *CBS news*, 7 July 2024, https://www.cbsnews.com/news/mental-health-chatbots-powered-by-artificial-intelligence-providing-support-60-minutes-transcript/ (last access 23/09/2024) .

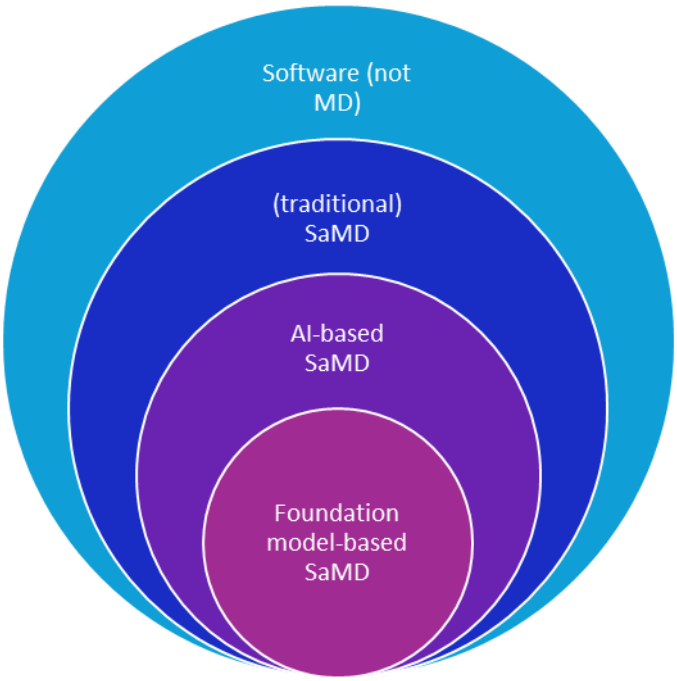

Figure 1. Software and Medical devices

Especially for the last two subsets of the diagram, meaning AI-based and foundation model-based SaMDs, it is clear already that it will be necessary to harmonize the compliance rules stemming from the MDR and the newly adopted AIA at the same time. This is caused by the fact that the two regulations, both the MDR and the AIA will be applicable as the AI- or foundation model-based SaMD is at the same time an AI system and a certified or certifiable MD. What will the manufacturer need to do then? One of the most serious issues in the aftermath of the AIA's vote into law would be for the EU Commission (in this case, maybe the newborn AI office?[86]) and the MDCG SaMD group to issue a clear path to follow. In the meantime, in this article, I will explain how for some aspects AI SaMD compliance might be simpler than for other AI systems but still complex to figure out as a whole.[87] As a first example of this, there will still be the need to clarify when and where the AIA's novelties will need to be applied within the existing MDR conformity procedures.

4. Complementarity between the MDR and AIA. A short practical guide

To answer Section 3 question, it is necessary to adopt both a regulatory and a product-based logic, as far as SaMD product compliance is concerned. Let us not forget that, arguably, the AIA is a product

[86] Article 64 AIA and European Commission, European AI Office, https://digital-strategy.ec.europa.eu/en/policies/ai-office (last access 23/09/2024).

[87] This was the conclusion reached within a webinar titled "Ensuring Compliance: understanding AI Act interactions with MDR/IVDR held by TUV Sud on the relationship between the AIA effect on the MDR compliance last 11 June 2024.

safety regulation at its core,[88] as the MDR is. In addition, the AIA also embeds the protection of fundamental rights and the right to health as part of its goals.[89] This fundamental rights approach is a relevant point of difference between the two legislations. The MDR does not have one general article dedicated to the protection of health principle. Certainly, it is mentioned in recitals[90] and several articles,[91] but this only shows how the MDR is mainly a product safety regulation as the right to health is a target that is mentioned in those specific cases and not as an overarching principle.

The main questions a manufacturer will likely have in mind concerning the AIA and MDR compliance coordination will vary according to the features of the SaMD, which can be standalone or driving/influencing hardware. More specifically a SaMD manufacturer will need to understand whether and how the AIA and MDR compliance rules exclude one another in some respects, and/or they need to be combined. First, given that also the AIA is a regulation founded on risk management and product safety analysis, it is important to frame what kind of risk an AI- or foundation model-based SaMD might entail according to the AIA lens. The AIA divides the different kinds of AI systems in four categories: prohibited practices, which are never allowed;[92] high-risk AI systems,[93] which are allowed but with safety and compliance obligations; General Purpose AI models (GPAIs, read foundation models), which are in turn divided into GPAIs with or without systemic risk,[94] and, finally, the residual category of AI systems which are not included in the previously mentioned categories and have a low or almost non-existent level of risk.[95]

Leaving aside the prohibited AI practices of Article 5 AIA and the other kinds of AI systems not regulated (directly or not) by the AIA, let us check the relationship between high-risk AI systems and SaMD compliance starting by explaining what the MDR's manufacturer, meaning the AI provider according to the AIA, needs doing. High-risk AI systems have a complex application and are dealt with in Article 6 AIA mainly, complemented by Articles 7 to 9 AIA. If we focus on Article 6(1) AIA the case of medical SaMD is already envisaged. There is a non-rebuttable presumption[96] that the AI system is

[88] Article 17 AIA makes it indispensable for high-risk AI systems providers to implement an AI quality management system and the product safety rules are much more than the protection of fundamental rights ones which are contained in Article 1 and 4 and Section 2 Chapter 2 concerning the general requirements for high-risk AI systems. This was also reinforced during the first public seminar held by the newly created AI office on 30 May 2023. European Commission, 1st European AI Office webinar on Risk management logic of Ai Act and related standards, https://digital-strategy.ec.europa.eu/en/events/1st-european-ai-office-webinar-risk-management-logic-ai-act-and-related-standards (last access 23/09/2024).

[89] Article 1(1) AIA.

[90] Recital 37 MDR.

[91] Such as, as an example, Article 52, 59, 61,62,66,68, 75,80,87,88,89,91,94,95,97,98,99,100, 106 MDR Annex I, 1, 6,9; Annex XV 4.1.

[92] Article 5 AIA

[93] Article 6 and 7 AIA.

[94] Articles from 50-52 AIA.

[95] This category will need to apply some principles such as the AI literacy one at Article 4 AIA and, because of the reference of Recital 166, conformity requirements will be the ones that are described in the GPSR alongside the non-mandatory AIA requirement to draft a code of conduct.

[96] Now that the AIA's text has been published there is no room left for interpretation and it appears that if an AI system falls into the list of the harmonized subjects of Annex I mentioned in Article 6(1) AIA, it will always be a high-risk system, with no exception. This means that all AI-based SaMD will be considered high-risk no matter their way of working and concrete risks to people. Luckily, as already explained in Section 2, the SaMD label is

high risk if two conditions are met "(a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I; (b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I."[97] If we check Annex I, at point 11 we can find the MDR among the list of the New Legislative framework procedures that will need to be considered high-risk.[98] Reading more carefully, it is unlikely that the AI system in this context is an MD and a safety component at the same time, as it would lack both the exclusive medical function and the intended purpose of being an MD. It is more likely that in this case, the AI system is an AI-based SaMD according to figure 1 section 3[99]. As well as MDR's SaMDs, also AIA's high-risk systems are admitted if they pass a conformity assessment which is granted using AI-specialised NBs. This will be one of the most interesting points that needs further clarification from the AI Office and the MDCG. Both the MDR and the AIA create SaMD conformity procedures and set up a system based on NBs which will determine the possibility for the AI system to circulate in the (Digital) Single Market.

To answer the main research question of this article, which is how to ensure compliance for AI-based and foundation model-based SaMD, I will use the complementarity principle. I argue that the complementarity principle will be the main principle through which the MDR and AIA compliance procedures will be combined. This is not a general principle of the EU legal order, but a derived one after the EU exercised its full competence or decided to use the subsidiarity principle.[100] In this case, complementarity does neither refer to the non-written sources of EU law, nor does it mean the relationship between the Commission and a MS. Rather, it is an ordaining criterion among subjects in which the EU has already exercised its competence the medical devices harmonization and the AI systems harmonization. This principle is explicit in the AIA and introduces a new ordaining and simplification criterion that generally applies to the selected and previously existing product safety laws (such as the MDR) and recent ones (such as the AIA). The quite clear drafting of Article 8(2) AIA supports this view. This latter article ensures that for all those disciplines that are harmonized under EU law and that are part of Section A of Annex I (to which the MDR belongs[101]), AI providers (it is worth remembering that they are the SaMD manufacturers in the MDR lexicon) must ensure all the compliance needed for the harmonization legislation (in this case the MDR). In order "to ensure consistency, avoid duplications and minimise additional burdens, providers shall have a choice of integrating**,** *as*

not given away easily. However, MD manufacturers must receive complete training on the AIA before putting into the market new standalone or driving or influencing hardware SaMD.

[97] Article 6(1) AIA.

[98] Annex I, Section A, 11.

[99] Compared to the specific high-risk AI systems mentioned in Article 6(2) and (3) and connected to Annex II and III, the high-risk AI systems compliance of Article 6(1)AIA in connection with Annex I (the SaMD case, to be clearer) is relatively simpler. Ms Irina CARNAT conducted an extensive analysis of the structure of Article 6 AIA and the problematic implications of its (2) and (3) paragraphs especially regarding judicial procedures. See I. CARNAT, *Addressing the Risks of Generative AI for the Judiciary: the Accountability Framework(s)* submitted to *Computer Law and Security Review*, pending revisions, 2024-2025.

[100] Article 5(3) TEU.

[101] Annex I point 11 MDR.

appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under the Union harmonisation legislation listed in Section A of Annex I."[102] This means that the MDR will stay in any case the basis for AI/foundation model-based SaDM compliance but there will be a choice as to how and when to integrate the AIA requirements that did not exist in the MDR or that are utterly new. From this first preliminary rule and by using an exclusion logic, I can derive at least three operational rules

i) if a rule/process/ requirement/duty is present in the AIA and not in the MDR, the AIA requirement will be added to the MDR conformity procedure;
ii) if there is a rule /process/ requirement/duty that is present in both the AIA and the MDR but still adds a new element in terms of AI, one will have to evaluate how to integrate the AIA requirement in the MDR on a case-by-case basis;
iii) if a rule /process/ requirement/duty is present in the MDR and not in the AIA, it will continue to exist.

In my opinion, this is easier said than done. In Article 8(2) AIA indent, the "as appropriate" part, could lead to a variety of practices which in principle could be understandable given also the general character of the MDR and the variety of MDs to which it applies. However, not knowing especially when to carry out the AIA compliance while starting the proceedings with a NB for an AI-based or foundation-model-based SaMD could have huge repercussions in terms of the damages that SaMD could cause and that were explained in section 2 while discussing of rule 11 in Annex VIII MDR. What if, for instance, a patient was misdiagnosed because the design of the AI system powering the SaMD was designed in a way that considers the AIA duties of transparency and data governance at the end of the certification process? The manufacturer (as the NB is still not liable according to the MDR) will need to justify the appropriateness of when they decided to integrate the AIA compliance requirement and whether that was justified.

To find out at least which blocks of the AIA are going to be included in the MDR certification process it might be useful to divide the most relevant groups of articles for AI-based and foundation model-based SaMD:

a) articles concerning overarching principles applicable to all AI systems: Articles 1- 4 AIA ;
b) general requirements for high-risk systems: Articles 8- 15 AIA
c) requirements for providers and deployers[103] of high-risk AI-systems and other parties: Articles 16 -27 AIA + 50 AIA (specific requirements on transparency, applicable in part to foundation model-based SaMDs)
d) standards and common specifications: AIA Articles 40-42;
e) NBs: Articles 28-39
f) Conformity procedures: 43, 47, 48.

[102] Article 8(2) AIA. Emphasis Added.
[103] AI deployer does not have a direct equivalent in the MDR and is defined as a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. Article 3(4) AIA.

g) If the SaMD is foundation model-based, meaning a GPAI model or system further obligations to be added to a), b) c) e) f) rules: Articles 52-56 AIA .
h) Governance: Articles 64-70 AIA
i) Post Market surveillance: 71- 73 AIA
j) Enforcement: 74 -84 and 88-94 AIA

Here follows a table that tries to compare and contrast whether the AIA duties do have or not a direct equivalent in the MDR. We will cross the two criteria highlighted, the complementarity one and the AIA disposition applicable to SaMD

Colour coding

rule/process/ requirement/duty is present in the AIA and not in the MDR

there is a rule /process/ requirement/duty that is present in both the AIA and the MDR but still adds a new element in terms of AI

a rule /process/ requirement/duty is present in the MDR and not in the AIA

AIA groups of Articles Applicable to SaMD	AIA Articles applicable AI and foundation model-based SaMD (high-risk 6(1) AIA and GPAI)	Corresponding Articles in the MDR for AI and foundation model-based SaMD
A) articles concerning overarching principles applicable to all AI systems	**1. Protection of health and fundamental rights**	**Protection of health**: recital 37 and articles but not as a separate article in the main text
	4: AI literacy principle. The AI provider and deployer must ensure that their staff and users are aware of the risks and intended purpose of the SaMD	**AI literacy:** Not present
B) general requirements for high-risk systems	**8(2) Complementarity**: Compliance with requirements; principle of complementarity	**Complementarity:** Only when referring to standards that are not harmonized and reference to the General Product Safety Directive

		(now GPSR regulation)
	9: Risk management system. Objectiveà Identification of the known and reasonably foreseeable risks that high-risk AI systems can pose to health safety and fundamental rights. Limitation to the reasonably mitigable or eliminable risks through development of the design of the AI	**Risk management system:** Article 10(1) combined with Annex I section 3. Similar in the sense that is an iterative and continuous process but there is no AI reference
	10: Data and data governance. Main principle at para (2) *Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system.* Moreover data shall be representative (3) datasets must take into account the contextual setting of the SaMD (4); authorization to process special categories of data(5)	**Data and data governance:** Only mention of clinical data and data for devices for clinical evidence. Among many Annex XIV, clinical evaluation and post-market follow up. Not AI data training.
	11: Technical documentation 11(1): must demonstrate compliance with the general requirements for high risk systems (**more in Annex IV**) 11(2): Applicable to 6(1):	**Technical documentation:** Article 10(4) in combination with Annexes II and III but it does not mention AI

	only a **single set** f technical documentation shall be drawn up containing all the information set out in paragraph 1 **as well as the information required under those legal acts.**	
	12: Record keeping (1) High-risk AI systems shall technically allow for the automatic recording of events ('logs') over their lifetime. (2) logging capabilities must record events relevant for identifying risk relevant for market surveillance; facilitate post-marketing, monitoring; conservation for at least six months by AI deployers	**Record keeping.** Not a separate article but a frequent requirement throughout Chapter VI on clinical evaluations and investigations In combination with Annex XIV and in connection with the preservation of documents by the manufacturer Article 10(8) functional to show documents to NBs and MS authorities.
	13: Transparency and provision of information to deployers (1) principle of sufficient transparency to interpret the system's output (3) list of minimum requirements for transparency written in coincise complete correct manner (2) such as the characteristics, capabilities and limitations of performance of the high-risk AI system, including: (i) its intended purpose;	**Transparency.** Recitals 4, 43, 44, 53, 74, 88 might have an equivalent effect function. Not specific for AI

	50: Transparency obligations for providers and users of certain AI systems (1) applicability to AI systems intended to interact directly with natural persons. Duty to inform the natural person that they are interacting with an AI/foundation model based SaMD *unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use*. (2) Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. This is relevant in case a foundation model based SaMD is integrated and used such as a conversational agent in a healthcare robot.	**Transparency.** Article 10(14),(15). Duties of the manufacturer towards authorities Annex I, 4, duties to alert users of residual risks Annex XV duty of the sponsor/manufacturer to alert on adverse effect (4.5) or reaction 25(c). Not specific for AI based SaMD.

	14 Human oversight (1) *High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use* (2) The objective is to minimise the risks to health and safety or fundamental rights which might emerge while using AI-based SaMDs (3) *The oversight measures shall be commensurate to the risks, level of autonomy and context of use of the high-risk AI system* (4) at least two people charged with the oversight which must be aware of the automation bias, meaning *the tendency of automatically relying or over-relying on the output produced by a high-risk AI system*	**Human oversight:** not present in its AIA meaning. There are Just recitals 51 and 53 which mention oversight as applicable to NB
	15: Accuracy (2) The EU Commission will *in cooperation with relevant stakeholder and organisations such as metrology and benchmarking authorities, en-*	**Accuracy:** Article 31(5); Annex I 14.2(g), 15(1), 19(1)(c), 23.4; Annex II 6.2(f). Not as a principle but as a characteristic to ensure in specific circumstances such as

	courage, as appropriate, the development of benchmarks and measurement methodologies. (3) Accuracy metrics must be declared in the instruction for use (4) technical and organizational measures must be taken in order to avoid errors, faults and inconsistencies *…and to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loop)*	general safety and health requirements and technical documentation
	15: Robustness Idem 15(2) (4) robustness must be achieved through *technical redundancy solutions, which may include backup or fail-safe plans*	**Robustness :** Article 71 (3)(d); Article 75(1) Article 78(8) (C) Annex XV, 3.6. Requirement connected to data during clinical investigations
	15: Cybersecurity (5) mandatory to ensure resilience against unauthorized third party attacks. The solutions aiming to ensure cybersecurity must be proportionate to the risks. Examples of solutions: *measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set ('data poisoning') pretrained components*	**Cybersecurity**: Not present per se but often recalls to the state of the art, harmonized standards and common specifications which also include cybersecurity good practices

	used in training ('model poisoning'), inputs designed to cause the AI model to make a mistake ('adversarial examples' or 'model evasion'), confidentiality attacks or model flaws.	
C) requirements for providers and deployers	**16, + 22- 26 Obligations of providers of high-risk AI systems, deployers and other actors on** NB Quite similar in structure to the MDR. The list of subjects involved are high-risk AI providers (16) authorised representatives (22);importers (23); distributors (24); deployers of AI systems (26). Very important is Article 25 which allocates responsibilities along the AI value chain. If any actor, including the third party put their name or trademark or substantially modify the AI system. They will be considered as AI providers. (3) in case the high-risk AI system is a safety component of products covered by Article 6(1), Annex I, list A (MDR), the product manufacturter will be considered the provider of the high risk system if the high risk system is put into	**Obligations of manufacturers (and other economic operators)** 10-16 MDR. Similar overall except for the fact that in the MDR there is not the definition of AI provider or AI deployer, although in the first case it can easily coincide with the MD manufacturer. It is Important Article 16 in which there are rules as to when obligations of manufacturers shift on importers , distributors or other persons. However, MDR has a person in charge for MDR compliance (15). All these articles lack AI-specific references

	commerce together with the product under the name or trademark of the manufacturer, or he high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.	
	17:Quality management system 17(3) (3) *Providers of high-risk AI systems that are subject to obligations regarding quality management systems or an equivalent function under relevant sectorial Union law may include the aspects listed in paragraph 1 as part of the quality management systems pursuant to that law* (complementarity)	**Quality Management System** 10(9), in combination with Annex IX more complex than AIA but also lacks any AI reference
	18: Documentation keeping 10 years after the SaMD has been put on the market together the AI provider must be able to provide to competent authorities *(a) the technical documentation referred to in Article 11; (b) the documentation concerning the quality management system referred to in Article 17; (c) the docu-*	**Documentation keeping** Not a single provision but Article 10(8) on the manufacturer's obligation to keep the technical documentation in combination with Annexes II and III have on technical documentation pre and post marketing the medical device. The contents are quite similar and specific for the generality of the different MDs but do

	mentation concerning the changes approved by notified bodies, where applicable; (d) the decisions and other documents issued by the notified bodies, where applicable; (e) the EU declaration of conformity referred to in Article 47.	lack AI mentions
	19: Automatically Generated Logs Logs will be kept for a period of 6 months	**Automatically generated logs**. Not present
	20: Corrective action and duty of information. If the SaMd alreadyon the market or put into service, the provider must *immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate*. In case of the risk that the product or service could cause to health and safety according to the Market Surveillance regulation and the provider is aware of that, they must immediately inform *the market surveillance authorities of the Member State or Member States in which they made the high-risk AI system available on the market and, where*	**Corrective actions and duty of information** referred to specific fields: Placing on the market Article 5(5), (h) General obligations of manufacturers Article 10(9)(k) and (13) Unique Device Identification system Article 27 Post market surveillance by the manufacturer Article 83(2), 85(1); Annex III 1.1 (a), (b) Vigilance Articles 87,89, 90, 91,92 Market surveillance Article 93(6) Requirements to be met by NB Annex VII, 4.10 Procedure for custom-made devices Annex XIII (5) Clinical investigations Annex XV 2.4, 7

	applicable, the notified body that issued a certificate for that high-risk AI system in accordance with Article 44, in particular, of the nature of the non-compliance and of any relevant corrective action taken.	
	21: Cooperation with competent authorities Duty of loyal cooperation with EU and national authorities	**Cooperation with competent authorities** See supra but not AI specific
	27: Fundamental rights impact assessment – not applicable for high risk systems Article 6(1) AIA Annex I.	**Fundamental rights impact assessment**. Not applicable
D) standards and common specifications	Article 40(1) discipline of harmonised stanadards (general) Article 41:Common Specifications (5) Article 42(2) presumption of cybersecurity compliance	Article 2(70) and Article 8 (MDR) Article 2(71) MDR and one main Article 9 MDR for common specifications although it appears many other times in the document).
E) NBs	**28-39: Notified bodies take Article** 29 AIA (4) case for already harmonised discipline. NB can submit the application for the notification procedure under the AIA. submission possible so also existing MDR NB might apply to have this further capacity Articles 31- 39+45 Focus on Article 31: (3) obligation	**Notified bodies:** Articles 35-50 MDR + Annex VII Most of their obligations are the same of AI NB, meaning impartiality, no conflict of interest and proven expertise in the field. Only they do not as an object AI-based SaMD

	to satisfy quality management, organisational and cybersecurity requirements (4) independence (5) no conflict of interest Article 32 presumption of conformity if NB shows conformity with the relevant harmonised standards Article 33(3) subsidiaries list made public	
F) Conformity procedures and declaration, 43, 47, 48.	**43: conformity assessment.** For high- risk Article 6(1) AI-based SaMD focus on (3) requires the relevant harmonized procedure + Points 4.3. 4.4., 4.5. and the fifth paragraph 4.6 of Annex VII shall also apply. + Annex V; Art 47: objective certify that AI system meets requirement section II (principles) Article 48 CE Marking, focus (5)	**conformity assessment** Article 19 and 20 MDR and Annex IV and V MDR
G) GPAI= foundation model based SaMD	Articles 50-56 Articles must be added as well as Article 61 on the AI office and 68 on the scientific panel of independent experts	None
H) Governance	Creation of **64: AI office**à relevant if GPAI (foundation-model based SaMD) has systemic risk (64 AIA)	Not a dedicated section per se but there are several groups of articles involving the relevant actors a part from economic operators

	65: European Artificial Intelligence Board à relevant for AI and foundation model based SaMDs as as it collaborates with national authorities for market surveillance and gives inputs on the **implementation of the AIA vis-à-vis GPAIs** (foundation-model based SaMDs) (65, c) + inputs for **codes of practice, common specifications, harmonised and not harmonised standards** (65,e, I,iii, iv) and **creation of benchmarks** (g) **68: Scientific Panel of Independent experts à** experts in 'all things AI' appointed by the EU commission. It will support and advise AI office (68, 3) **70: National competent authorities à** obligation of a single point of contact for each Member State for this regulation. It could be a *1) notifying authority, and 2) market surveillance authority*	**Vigilance** Articles 87,89, 90, 91,92 **Market surveillance** 93 and ff **Requirements to be met by NB** Annex VII **104 :support by the EU Commission** **105- 107: MDCG**, role and functions **101 Competent Authorities** **106 Expert panels and expert laboratories**
I) Post-market surveillance	**72: Post-market monitoring**. Providers shall establish a post-market monitoring system in a manner that is proportionate to the nature of	**83 Post-market surveillance system of the manufacturer.** More detail in the duties here than in the AIA see art 84, 85, 86

	the AI technologies and the risks of the high-risk AI system.It can rely on the **collaboration of AI deployers** and could include **and analysis of the interaction with other AI systems.** It means also that the MD manufacturer **must have a post-marketing plan;** **73: Reporting serious incidentsà** to the market surveillance authority designated	**Vigilance Article**s 87,89, 90, 91,92 **Market surveillance** 93 and ff.
J) Enforcement	**74-84:** Application of market surveillance regulation 2019/1020 (article 74) ; mutual assistance and market surveillance for control of GPAI(75); real-world testing (76) powers to protect fundamental rights (77); procedure at national level for dealing with AI systems presenting a risk (79); **Compliant AI systems which present a risk (82)** Formal non compliance (83); Union AI testing support structures (84) **88-94: specific rules pertaining to GPAIs, applicable to foundation-model SaMD**	**Market surveillance** 93 and ff - Evaluation of devices suspected of presenting an unacceptable risk or other non-compliance (94) - Procedure for dealing with devices presenting an unacceptable risk to health and safety (95) - Procedure for evaluating national measures at Union level (96) - Other non compliance (97) - Preventive health protection measures98 - Good administrative practices 99 - electronic system on market surveillance 100 - Device registers and databanks 108

	99-101: penalties	CHAPTER VIII cooperation between Member State, Medical Device Coordination Group, Expert laboratories, expert panels and device registers CHAPTER IX: penalties

Table 2. Comparison between the AIA and MDR compliance for SaMD

5. Open issues and operative suggestions

As one could have foreseen, quantitatively the number of rules and principles that are brand new in the articles analysed is not high. However, as far as governance is concerned there are new elements, especially when referring to GPAI models, which, for the purposes of this article, coincide with foundation model-based SaMD.[104] What I believe is going to be the problem is that it will not be easy to assess when and where to add an AIA duty that has a *quid pluris* compared to an existing similar MDR requirement that, in turn, does not consider AI. In this part of the Article, I will try to be more operational and focus mainly on i) the new or almost new duties for MD manufacturers; ii) the difficulty of translating everything into standards and common specifications in the AIA; iii) the complementarity applied in the conformity procedure and what it means for the AI and foundation model-based SaMD.

As far as the first issue, the first and second group of articles that deal with overarching principles for high-risk AI systems and the one concerning general requirements for high-risk systems both introduce completely new elements and profoundly renewed concepts in the SaMD-MDR compliance. In either case, even if one can read a disposition as a principle, it will most likely contain many duties and obligations that AI or foundation model-based SaMDs providers/manufacturers must implement. The first example is the brand-new AI literacy principle in Article 4. This principle states that AI providers (in our case AI-based SaMD manufacturers) must ensure that their staff and the people who will implement their AI systems (AI deployers, which might be doctors and hospitals/private clinics management in our case) are AI literate. What does this mean practically? It might be considered already the most important Article in the AIA[105] but it seems hard to define as its precise contents vary

[104] See for instance the specifications of the AI office about GPAIs (foundation model SaMD) with systemic risk at Article 52 AIA. There will be also new governance structures such as the European Artificial Intelligence Board (Article 65 AIA) and the scientific panel of independent experts (Article 68) and the AI-based or foundation model-based SaMD manufacturers will need to monitor their actions in defining their inputs on codes of practice and common specifications.

[105] I. CARNAT, *Compliance impossible?*, Forthcoming, 2024-2025

on the characteristics of the AI system- and, in our case, of the SaMD- involved. AI literacy is better defined in Recital 56 AIA which describes it as "skills, knowledge and understanding that allows providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause"; Recital 20 AIA further clarifies it in this following way: it "should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement" as well as "follow up actions" and attention to "vulnerable persons".[106] Article 4 AIA makes it mandatory for both AI providers and deployers to sufficiently train their staff working with AI systems as well as whoever will need to use AI systems. It will be necessary to provide this AI literacy training by taking into account several factors among which there will be "their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used".[107] But how can one quantify enough training? Maybe, the MDR can be helpful especially if we remind ourselves of the damage examples that software might cause, set in rule 11 Annex VIII MDR. If the level of damage is low to medium low, there will not be as much training as per an AI-based SaMD whose class of risk is IIb and or III. Another important set of duties is the data governance ones at Article 10 AIA or human oversight at Article 14. Article 9 gives precise indication concerning how to train and validate data. In theory, these principles were already applicable, as the 2020 Guidance (see *supra* 2) detailed some research good practices focussing on clinical data to get an evaluation of the clinical performance of SaMDs. With the data governance duties set at Article 9 AIA, the 2020 Guidance good practices become now enforceable although they were not primarily designed for AI systems design and functioning. For AI and foundation model-based SaMDs, these preliminary operations on the training of their AI functioning system will become horizontal/general obligations. One can reasonably expect that the level of safety and the efficiency of functioning of the new AI and foundation model-based SaMD will increase after the AIA entry into force which was on 1st August 2024. There are also complementary rules to these and it is worth focussing on Article 15 AIA, which concerns the level of accuracy, robustness and cybersecurity of high-risk AI systems. Article 15 AIA touches upon issues that were already important for the application of the MDR, but it adds new and more specific elements. For instance, the EU Commission must involve actors to provide benchmarks to measure the accuracy of the AI system outcome. This is extremely important for SaMD as accuracy in AI-based diagnostic applications is essential, as well as an adequate level of device cybersecurity given the sensitive nature of the data processed by AI-based SaMD. Even if cybersecurity is not cited directly in the MDR, the reference to harmonized standards, common specifications, and international standards in the MDR hints at the specificity of these standards for MDs. That is why the MDR is excluded by the application field of the newly approved cyber-resilience act, which, on the contrary, sets horizontal and general standards for the generality of connected devices.[108] Nevertheless, it is arguable how such a

[106] 165 recital AIA.
[107] Article 4 AIA.
[108] Article 2(2)(a), Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

vague reference to state-of-the-art cybersecurity standards can have better results than excluding any harmonized cybersecurity standards. Because of this, the AIA is an important occasion to specify that compliance with the Cybersecurity act,[109] and, specifically with the cybersecurity certification schemes, leads to a (rebuttable) AIA conformity presumption. These three last elements likely need to be thought of since the design of the SaMD is in connection with its intended purpose.[110]

This leads us to another debated issue which concerns the role of standards and common specifications both in the MDR and in the AIA. MDR has only two articles that give the definitions of harmonized standards and common specifications.[111] Standards are mentioned throughout the MDR but this word not only refers to harmonized standards but also standards intended as state of the art and practice, especially as far as specific procedures are concerned.[112] Article 8 MDR on harmonized standards sets a conformity presumption of the MD if it uses and implements EU harmonized standards. Article 8(2) also specifies that harmonized standards will apply to system and process requirements. For common specifications, it is almost the same as with harmonized standards. Article 9 MDR states that common specifications (CS) are defined by the EU Commission in the eventuality that there are no harmonized standards at the moment of the deadline laid by the MDR provisions for harmonized standards. The AIA takes inspiration from this approach as it also defines harmonized standards[113] and common specifications.[114] The main difference relies on Article 40(2) AIA in which it is explained that the EU commission will issue standardization requests for all the requirements concerning the high-risk systems' general principles such as the one of human oversight and the trans-

COM/2022/122 final. Approved on 12 March 2024 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html#title2 (last access 23/09/2024).

[109] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) PE/86/2018/REV/1 OJ L 151, 7.6.2019, p. 15–69. See also F. CASAROSA, *Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act*, in *International Cybersecurity Law Review*, 3, 2022, 115-130.

[110] More on the connection between AI and cybersecurity from a health point of view, see E. BIASIN, E. KAMENJAŠEVIĆ, *Regulatory Approaches Towards AI-Based Medical Device Cybersecurity: A Transatlantic Perspective* in *European Journal of Risk Regulation*, 2024, 1- 11. If interested also with the connection between cybersecurity and the European Health Data Space (EHDS) see F. CASAROSA, *European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats?*, in *European Journal of Risk* Regulation, 2024, 1-11.

[111] Article 2(70) and Article 8 MDR for harmonized standards, which are specific ones, drawn up by the EU standardization bodies, meaning CEN, CENELEC and ETSI by delegation of the EU Commission. They are regulated by the Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance OJ L 316, 14.11.2012, p. 12–33. Article 2(71) and Article 9 MDR instead explain the meaning and conformity presumption of common specifications. Common specification, abbreviated often in CS, appears 111 times in the MDR document; harmonized standard(s) instead appears 48 times.

[112] For instance, see Article 106(8) (c) MDR on the provision of scientific technical opinion and advice states that expert laboratories shall "*have the necessary knowledge of international standards and best practices*".

[113] The MDR defines harmonised standards is defined in the same way than in the MDR, see Article 3(27) AIA.

[114] Common specification is defined in the same way than in the MDR, see Article 3(28) AIA.

parency obligations for providers and deployers of certain GPAI systems, hence including the foundation-model based SaMD. Scholars[115] have criticised the over-reliance on standardisation also to protect fundamental rights since the AIA was a proposal. Despite this intrinsic difficulty in standardizing principles, this view has not changed with the AIA's final approval and a product-specific logic (the one involving standards) is going to be applied also to fundamental rights that are difficult, if not impossible, to measure. For AI-based and foundation model-based SaMD, this means simply that the new sets of harmonized standards involving the respect of fundamental rights will need to be integrated within the design of the SaMD together with the more specific ones investing medical software, and that can also correspond to state of the art practice. The same *rationale* goes for the common specifications in Article 41 AIA. In both circumstances, however, the conformity to harmonized standards and common specifications does not exempt the AI/ foundation model-based SaMD manufacturer from liability in case damage arises.[116]

Another block on which the compliance between AIA and MDR concerning SaMD needs harmonization and we see the principle of complementarity applied is the relationship between MDR NBs and AIA NBs. As already specified *supra* in Section 2, because of previous health scandals, NBs requirements in the MDR are more specific, and count more provisions than the AIA.[117] What is interesting is that specialised MDR-NBs could apply to require new competencies and evaluate the AI and foundation model-based SaMD by filling in the application for the notification procedure under Article 29 AIA. Article 29(4) AIA details the case of NBs who are already appointed under any other Union harmonization legislation (MDR included). In this case, MDR-NBs can apply to become AIA-NBs as well by using the documentation employed to obtain the previous (MDR) notification and by adding the documents listed in (2) and (3) of the same article. Among these documents, the MDR-specialised NB will need to add "the conformity assessment module or modules and the types of AI systems for which the conformity assessment body claims to be competent, as well as by an accreditation certificate",[118] together with "any valid document related to existing designations".[119] In case the NB cannot provide an accreditation certificate, the NB will provide the notifying authority "all the documentary evidence necessary for the verification, recognition and regular monitoring of the compliance".[120] If MDR-NBs apply specifically to certify AI-based or foundation model-based SaMD, the complementarity principle would be respected. Not to mention, it would save time and resources for

[115] M. EBERS, *Standardizing AI, The Case of the European Commission's Proposal for an 'Artificial Intelligence Act* in L.A. DIMATTEO, C. PONCIBÒ, M. CANNARSA (eds.), *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics*, Cambridge, 2022, 321-344.

[116] This was also the outcome of the James Elliott CJEU judgment. *James Elliott Construction Limited v Irish Asphalt Limited*, C-613/14, ECLI:EU:C:2016:821. K. P. PURNHAGHEN, *Voluntary "New Approach" Technical Standards are Subject to Judicial Scrutiny by the CJEU! – The Remarkable CJEU judgment "Elliott" On Private Standards* in *European Journal of Risk Regulation*, 8,3, 2017, 586-598; A. VOLPATO, *The harmonized standards before the ECJ: James Elliott Construction* in *Common Market Law Review*, 54, 2, 2017, 591-603.

[117] In the MDR, Articles 35-50 and Annex VII are exclusively dedicated to the NB and are recalled in many other articles. In the AIA, NB's duties and characteristics are at Articles 29-39 and 45 but they are cited throughout the AIA several times.

[118] Article 29(2) AIA.

[119] *Ibid*.

[120] Article 29(3) AIA.

AI and foundation-model-based SaMD for the conformity procedure. One peculiar thing is how cybersecurity is a new AIA element that will indirectly change the AIA. An MDR-specialized NB would need to meet cybersecurity requirements to apply and to become a AI- specialised NB.[121] This adds to the MDR- NBs requirements of being impartial, competent and with no conflict of interest. However, the complementarity principle here can be applied quite clearly with the addition of the AIA peculiarities to the MDR-NB appointment compliance.

The final block of rules in which the principle of complementarity appears as an addition to an existing procedure concerns the integration between the two sets of conformity procedures: the ones set in the MDR and its Annexes and the ones in the AIA. Article 43 AIA is the main rule for the conformity assessment. For high-risk Article 6(1) AI-based SaMD focuses on paragraph (3). The paragraph requires the respect of the relevant harmonized procedure, which, in this case, would be the MDR one, chosen according to the device's risk level as already explained.[122] However, there will be the need of an integration of Annex VII AIA. In particular, the NB will need to have "full access to the technical documentation and full access to the training, validation and testing data sets used, including, where appropriate and subject to safety safeguards through API or other relevant technical means and tools enabling remote access".[123] Moreover, the NB can require the provider (the SaMD manufacturer) to provide more evidence or conduct further tests.[124] Furthermore, if the NB deems it necessary and there are no other means to assess the conformity requirements, and submits a reasoned request on this matter, the AI provider shall grant access to "the training and trained models of the AI systems, including its relevant parameters".[125] This operation will happen in compliance with the EU intellectual property and trade secrets disciplines.[126] Finally, the NB must motivate its refusal to grant conformity to a specific AI system especially when the grounds for its refusal concern the data quality.[127] The AI provider who does not meet the AIA requirements will need to re-train the model and resubmit a request for a compliance assessment by the NB.[128] Concerning the final CE marking, Article 47 AIA adds further requirements to add the analogue MDR CE marking discipline.[129] First, the AIA conformity declaration must be in a machine-readable format and physically or electronically signed.[130] It is important to mention that the criteria to evaluate conformity are the ones of the general requirements for high-risk systems, such as the principle of human oversight and assurance of transparency and data governance.[131] Regarding the CE marking, it is important to mention that whenever high-risk AI systems (including the SaMD) "are subject to other Union law which also provides for the affixing of the CE marking, the CE marking shall indicate that the high-risk AI system also

[121] Article 31(2) AIA.
[122] In this case it will be one of the procedures that can be chosen for each MD by combining Article 52 and Annexes from IX to XI MDR.
[123] 4.3, Annex VII, AIA.
[124] 4.4, Annex VII, AIA.
[125] 4.5, Annex VII, AIA.
[126] Ibid.
[127] 4.6, 5 para. Annex VII, AIA.
[128] *Ibidem*.
[129] Article 19 and 20 MDR and Annex IV and V MDR.
[130] Article 47(1) AIA.
[131] Article 47(2) AIA.

ISSN 2284-4503

fulfil the requirements of that other law."[132] It is easy to assume that the SaMD CE marking will need be just one and that it grants conformity both to the MDR and the AIA.

6. Preliminary conclusions

This work tries to be a bridge between two technical and distinct compliance requirements sources: the MDR and the AIA. However, the *trait d'union* between the two of them is easy to spot, and that is a software as a medical device, SaMD. Given the fast-paced development in embedding or using AI as an MD, it was particularly important to open the conversation about how to deal with the compliance of AI and foundation model-based SaMD. If other actors, including legal scholars, apart from technical experts, are aware of these technical disciplines and their specific problems with AI legal compliance is in any case a positive thing. It will be the first step to evaluate from more than one technical perspective the positive effects, as well as the drawbacks, of the incessant introduction of AI systems in our lives. This work could be a starting point of a reflection on how the MDR and AIA compliance requirements are going to influence liability rules and whether it is a useful thing to standardise ethical and legal principles. However, he main research objective of this early-stage research paper is to find a way to combine two sets of compliance rules (MDR and AIA) that are different because of the time in which they were written, because of the different levels of technological advancement and because one of them has a specific object, medical devices, and the other one instead deals with all the possible forms of AI systems.

Methodologically, I started with the definition of SaMD and gave an idea of its fragmentary nature, divided between the generality of the MDR and the explicative value of the MDCG guidance documents. The objective of the first table in section 2 was to connect all these scattered definitions and rules in one place and to visualise which kind of risk class and which kind of procedure a SaMD might get today according to the MDR.

Secondly, after defining what an AI system was and what a SaMD was, it was easy to find that there could be new subsets of SaMD: the AI-based one and the foundation model-based one. Only after that I was able to select the most relevant articles about high-risk AI systems and compare them with the corresponding articles in the MDR (if there were any) in a second table.

The main results of this early-stage research are the following. The main principle to follow to carry out a correct MDR and AIA compliance is the complementarity principle set in Article 8(2) AIA, which establishes that the main procedure is the EU harmonized one, with which the product or service is put on the market. In our case, it is the MDR. Article 8(2) follows on explaining that novelties issued by the AIA must be integrated as appropriate. In practice, the AI/foundation model-based SaMD providers/manufacturers will need to apply three main logical rules to assess how and when to apply the AIA within the MDR compliance procedure:

i) if a rule/process/ requirement/duty is present in the AIA and not in the MDR, the AIA requirement will be added in the MDR conformity procedure;

[132] Article 48(5) AIA.

ii) if there is a rule /process/ requirement/duty that is present in both the AIA and the MDR but still adds a new element in terms of AI, one will have to evaluate how to integrate the AIA requirement in the MDR on a case-by-case basis;
iii) if a rule /process/ requirement/duty is present in the MDR and not in the AIA, it will continue to exist.

As it emerged from the second table in Section 4, the hypothesis under ii), is the most frequent one but also the most difficult of the three to implement for correct MDR and AIA compliance. Having the originally harmonized procedure as the main one, as explained by Article 8(2) AIA, is not easy in practice if the manufacturer does not know exactly when and where to add the new or partially new requirements to comply with the AIA and the MDR at the same time.

What appears from this first analysis is that the new requirements concerning overarching principles, such as the AI literacy principle, and the general high-risk systems requirements, such as the principles of data governance, will need to be integrated as early as from the design of the future SaMD also because of the new AIA governance system. These new principles follow the i) hypothesis. A case of a combination of rule i) and ii) concerns the AIA governance system: it will be composed of new actors such as the AI office but also (existing) national authorities, which will need to coordinate with the ones that were MDR-specialised (in Italy's case, the Health Ministry), especially when foundation model-based SaMDs are involved. SaMD manufacturers will need to care for both these groups of authorities especially if they develop a foundation model-based SaMD. Among the many examples sub ii) hypothesis, I decided to focus only on some for reasons of time and space. Despite the overarching AIA principles and general requirements for high-risk providers being sub i) hypothesis as they are new concepts per se, the fact that the Commission will issue requests for harmonized standards and common specifications which will make NBs presume compliance with those principles is partially déjà-vu for all harmonized EU legislations, MDR included. Standards and common specifications are not new, but the standardisation of principles is. What SaMD developers will need to do is to incorporate the available AIA harmonized standards and common specifications from the design of the SaMD, or, if there are not any available, to make choices to implement those principles since the SaMD early design phase. All these choices will need to be documented and inserted in the technical documentation of all the MDR conformity procedures which will integrate the specificity of the AIA conformity procedure set in Article 43 AIA. As, according to Annex VII AIA, the AI provider must give access to all the relevant material concerning the AI system to the NB, it will be important to insert this documentation as part of the quality management system of Annex IX MDR and, in general of Annex II and III, as well as in Annexes X and XI MDR whenever the quality management system or technical documentation is requested. Regarding NBs, there is also relevant news, which puts the NBs AIA discipline sub-rule ii), whenever AI or foundation model-based SaMD is concerned. The MDR-specialised NBs can apply to become experts in the evaluation of AI-based and foundation-model-based SaMD if they want to evaluate the SaMD compliance with the AIA correctly. Through the AIA notification procedure, which will be added to the MDR rules on NBs, MDR-specialised NB could acquire the competence to assess the risk of an AI-based or foundation model-based SaMD. This will be an addition to their consolidated and certified experience in medical devices. This could considerably reduce the expenses of a SaMD manufacturer that needs to certify their software both

under the AIA and the MDR. Nevertheless, these are just some examples of how the sub-ii) operational rule is the most common and most difficult to implement. It is unfair to think that manufacturers need also to take the responsibility to coordinate complex regulations such as the AIA and the MDR on their own, especially if they are not big companies. Article 113 AIA gives 36 months from the passing of the AIA for this kind of high-risk system such as the SaMD to comply with both legislations. As the AIA is formally applied from 1st August 2024, time is already running out. This deadline is not enough in terms of research and development but also to correct eventual AI or foundation model-based SaMD that might already be put in the market or into service and that are not fully compliant with the AIA. This reasoning is not only valid for the SaMD but also for all the EU harmonization legislation that is included in Annex I AIA. That is why what is expected as a minimum of legal certainty is a more precise guide drafted by the AI office in collaboration with the MDCG that can help SaMD manufacturers exit this impasse.