ARTIFICIAL INTELLIGENCE IN EU MEDICAL DEVICE LEGISLATION

May 2021

COCIR, the European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry

EXECUTIVE SUMMARY

The European Medical Devices Regulation (EU) 2017/745 (EU MDR) and In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (EU IVDR) in combination with the General Data Protection Regulation (EU) 2016/679 (GDPR) contain requirements for artificial intelligence in healthcare to be safe and performant. These requirements, both ex ante and ex poste requirements, ensure medical devices based on artificial intelligence are safe and performant throughout their entire lifecycle (Chapter 7).

This document provides an analysis of the legal requirements and concludes AI can be deployed in a way that is consistent with EU MDR and EU IVDR (Chapter 6.3). To facilitate the practical implementation of the legal requirements in the EU MDR, EU IVDR and GDPR, COCIR recommends the adoption of practical guidance, supported by the development of international standards. COCIR makes concrete proposals for such guidance throughout this analysis, and recommendations summarized in Chapter 11.

The analysis explains the characteristics of AI relevant for regulatory discussions, including possible approaches to the management of changes in software. Then, the crucial topic of ethics is addressed – especially the distribution of responsibilities between software developer and user needs to be clearly defined. The concept of trust is explored in its different dimensions, offering tools to increase trust in AI. The document also delves in more detail into the conformity assessment process under the EU Medical Device Regulations. The analysis presents how the existing risk management, life-cycle approach and testing requirements are fitted to AI-based medical devices. International standards are an essential building block of the medical device regulatory system. An overview of on-going standards development activities relevant for AI is provided.

The European Commission has shown its ambition in the area of artificial intelligence (AI) in its recent White Paper on Artificial Intelligence – a European approach to excellence and trust[1]. This White Paper is at the same time a precursor of possible legislation of AI in products and services in the European Union. However, COCIR sees no need for novel regulatory frameworks for AI-based devices in Healthcare, because the requirements of EU MDR and EU IVDR in combination with GDPR are adequate to ensure that same excellence and trust (Chapter 5 & 6).

[1] *White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65, published 2020.02.19*

CONTENTS

1. INTRODUCTION

Although different people may understand the term artificial intelligence differently, it is a reality in healthcare since decades. COCIR has identified numerous applications[2]. AI technology has been adopted in medical devices, workflows, and decision-making processes. Rather than replacing the human component of health care delivery, artificial intelligence has become a vital tool – a companion - to help improve patient outcomes.

The very fact that AI has been present for so long in medical devices, safely and effectively, demonstrates that the medical device legislation in the EU is an adequate legislative framework for its placing on the market. An in-depth analysis is necessary of how existing legislation affects AI-based devices in healthcare. This paper provides that analysis and outlines how Artificial Intelligence, including the aspects of trust and excellence raised in the EU White Paper, are addressed in the EU MDR, EU IVDR and GDPR. As such, COCIR intends to contribute to a better understanding and reassurance of AI in healthcare.

2. SCOPE OF THIS ANALYSIS

This analysis focusses on AI-based devices in scope of the EU MDR and EU IVDR, i.e. medical device software[3], parts or components of or accessories for medical devices or in vitro diagnostic medical devices that are or comprise AI, including AI sold as a service or as part of a hardware device (a.k.a. embodied AI, i.e. able to interact with the physical world).

Artificial intelligence refers to a wide variety of techniques[4]. Whereas today neural networks are in the spotlights, this chapter covers all forms of AI, including 'classical AI' (e.g., search and optimization techniques, expert systems[5], Hidden Markov Models[6] and older forms of computer vision), 'symbolic AI'[7] (e.g., logical reasoning[8] and decision making, Abstract Syntax Tree[9] (AST) modifying code), probabilistic reasoning[10], machine learning[11], knowledge representation[12], planning and navigation, natural language processing[13] and perception[14].

As we do not anticipate Artificial General Intelligence (AGI can learn incrementally, reason abstractly and act effectively over a wide range of domains), to appear on the market in the near- or medium-term future, this paper focusses on so-called 'narrow AI', i.e. artificial intelligence with a specific, rather than a general purpose.

This analysis does not cover liability in healthcare. For an evaluation of the adequacy and completeness of liability regimes see the European Commission report "Liability for Artificial Intelligence and other emerging technologies"[15] by the Expert Group on Liability and New Technologies and the "Report from the Commission to the European parliament, the Council and the European Economic and Social Committee".[16]

[2] *COCIR Use Cases – Artificial Intelligence in Healthcare*

[3] *Medical device software is software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a "medical device" in the medical devices regulation or in vitro diagnostic medical devices regulation. See MDCG guidance 2019-11 on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.*

[4] *AI HLEG A definition of Artificial Intelligence: main capabilities and scientific disciplines. 8 April 2019, accessed 2020-02-19*

[5] *Wikipedia. An expert system is a computer system emulating the decision-making ability of a human expert. Expert systems are designed to solve complex problems by reasoning through bodies of knowledge, represented mainly as if–then rules rather than through conventional procedural code. https://en.wikipedia.org/wiki/Expert_system. Accessed 26 January 2021.*

[6] *Hidden Markov Model is a statistical Markov model in which the system being modeled is assumed to be a Markov process with unobservable ('hidden') states. https://en.wikipedia.org/wiki/Hidden_Markov_model. Accessed 26 January 2021.*

[7] *Symbolic AI: AI system that encodes knowledge using symbols and structures. CD2 ISO-IEC 22989, 3 September 2020. Symbolic AI performs manipulations of abstract objects/concepts for logic deduction. Symbolic AI focusses much less on (mathematical/numerical) calculation and much more on composition and manipulation.*

[8] *Logical reasoning is a form of thinking in which premises and relations between premises are used in a rigorous manner to infer conclusions that are entailed (or implied) by the premises and the relations. Springer. https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-1428-6_790#:~:text=Logical%20reasoning%20is%20a%20form,of%20science%20and%20artificial%20intelligence. Accessed 21 January 2021.*

[9] *Wikipedia. Abstract Syntax Tree is a tree representation of the abstract syntactic structure of source code written in a programming language. https://en.wikipedia.org/wiki/Abstract_syntax_tree . Accessed 20 January 2021.*

[10] *Probabilistic reasoning combines probability theory with logic to handle uncertainty of knowledge. Javatpoint.com. Accessed 20 January 2021.*

[11] *Machine learning: process using computational techniques to enable systems to learn from data or experience. Source: IEC 23053, 3.16*

[12] *Knowledge representation is the field of artificial intelligence dedicated to representing information about the world in a form that a computer system can utilize to solve complex tasks such as diagnosing a medical condition or having a dialog in a natural language. Wikipedia. Accessed 21 January 2021*

[13] *Natural language processing: <system> information processing based upon natural-language understanding and natural-language generation. CD2 ISO-IEC 22989, 3 September 2020*

[14] *Artificial Intelligence: A Modern Approach (3rd Edition), Stuart Russell and Peter Norvig, 2009, Pearson*

[15] *Expert Group on Liability and New Technologies, Liability for Artificial Intelligence.. 21 November 2019.*

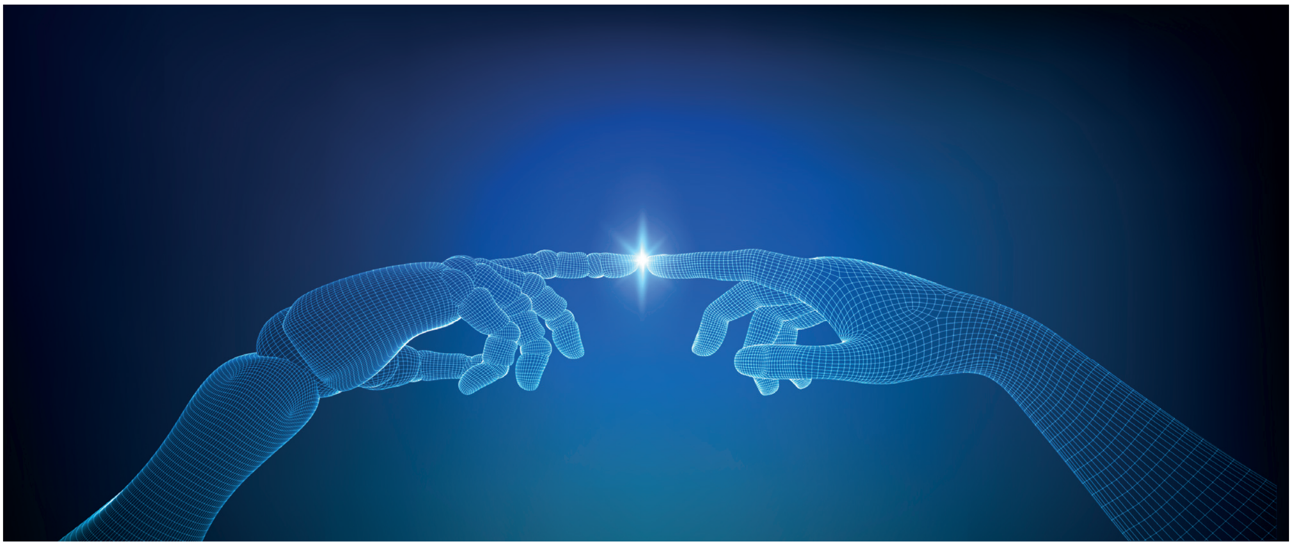
[16] *Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics - Report from the Commission to the European parliament, the Council and the European Economic and Social Committee. 19 February 2020. European Commission.*

3. DEFINITION OF ARTIFICIAL INTELLIGENCE

Having one common internationally accepted definition for AI would be useful to compare AI investments and regulations across the world. There are several definitions[17], each with different flavours. In trying to capture the essence of AI, the definitions tend to focus on AI's learning ability and/or its intelligent nature; two aspects that pose significant interpretation issues in a legal context[18].

With regards to AI's intelligent nature science has no consensus on what "intelligence" is[19]. As society tends to strip older AI techniques of their "intelligent" status, the term poses a large moving edge. Regarding its learning ability, generally, learning is understood as "acquiring knowledge or new skills". If learning knowledge is sufficient, many digital products will qualify as AI as soon as they acquire input data. If learning a new skill is necessary, then the meaning of the term narrows significantly.

Due to the uncertainty of what is and what is not covered by the term, **this paper focusses on software[20] in general and considers abstract attributes of certain types of software that are commonly associated with AI**. COCIR recognizes that these attributes can also be present in other technologies and that other attributes may require attention as the technology evolves.



[17] *Samoili, S., López Cobo, M., Gómez, E., De Prato, G., Martínez-Plumed, F., and Delipetrev, B., AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence, EUR 30117 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-17045-7, doi:10.2760/382730, JRC118163. This study assessed a large set of AI literature from three complementary perspectives: policy, research and market. The paper contains a collection of 46 definitions. Most notable definitions:*
The High Level Expert Group (an independent expert group established by the European Commission in June 2018) in the context of the European AI strategy (See AI HLEG "A definition of AI – Main Capabilities and Disciplines", 8 April 2019, accessed 2020-02-19) provides the following definition: "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. […]"
Draft IEC 22989 - Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, published 2019-10-31, defines artificial intelligence as the capability of an engineered system to acquire, process and apply knowledge and skills. Note: knowledge are facts, information, and skills acquired through experience or education.

[18] *Matthew U. Scherer, 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies,' [2016] Harvard Journal of Law & Technology; and Miriam C. Buiten, 'Towards Intelligent Regulation of Artificial Intelligence', [2019] European Journal of Risk Regulation.*

[19] *One way of defining intelligence is provided by Steven Pinker. He defines intelligence as the ability to deploy novel means to attain a goal; whereby the goals are extraneous to the intelligence itself. It should also be noted that Intelligence is a multi-dimensional variable, i.e. there are lots of facets to it (e.g. visual, motor, maths, language), hence, just like humans an AI can be intelligent on one facet, but not on another.*

[20] *Guidance on the Qualification and Classification of Software in Regulation (EU) 2017/745 and Regulation (EU) 2017/746 - IVDR defines software as "a set of instructions that processes input data and creates output data". Supplementing "a set of instructions" with "or computing logic" to accommodate neural networks, may not be needed as neural networks can also be considered to operate by "a set of instructions".*

4. ATTRIBUTES OF ARTIFICIAL INTELLIGENCE

COCIR advises manufacturers to describe the attributes of their AI-based devices in user-facing documentation to inform, gain trust and be commercially successful. Manufacturers have flexibility to describe these attributes in documentation either directed at an organisational level (if the software is business to business) or at an end-user level, or both (if appropriate).

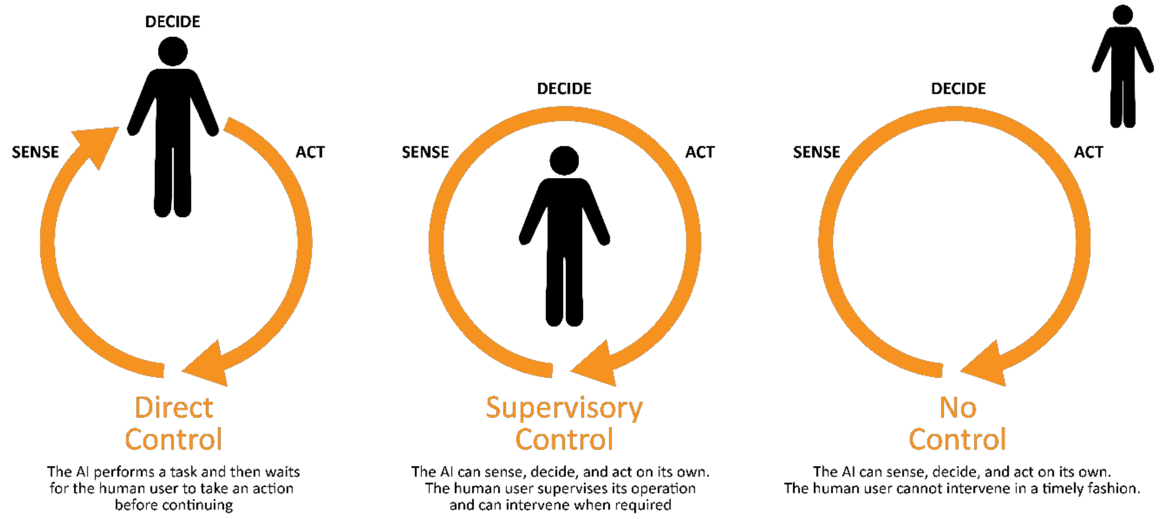
- **COCIR recommends** updating IEC 82304-1[21] requiring manufacturers to describe AI attributes in user-facing documentation:
    1. If, for what aspects and how the AI-based device provides human oversight or control
    2. If, for what aspects and how the AI-based device changes
        - Define if AI is locked or changes through learning during runtime
        - Provide a description of change dynamics and change boundaries
        - Define if and how humans can control change
- **COCIR recommends** updating IEC 62304[22] by requiring among others that manufacturer define an Algorithm Change Protocol (ACP) for AI-based devices that change through learning during runtime
- **COCIR recommends** that manufacturers of AI-based devices that change through learning during runtime add a pre-determined Algorithm Change Protocol to the technical documentation of their device for evaluation during conformity assessment. Manufacturers that make significant changes to the pre-determined Algorithm Change Protocol need to update the technical documentation, including the clinical evaluation and perform a new conformity assessment.

[21] *IEC 82304-1:2016 Health Software – Part 1: General requirements for product safety.*

[22] *IEC 62304:2006/A1:2015 Medical Device Software – Software lifecycle processes. Meanwhile COCIR's recommendation has been accommodated for in the text of the third edition of the standard, out for ballot later this year.*

4.1. CONTROLLABILITY – HUMAN OVERSIGHT

Controllability refers to the ability of an external operator to intervene or deactivate an AI-based device in a timely manner[23]. Figure 1 illustrates the types of controllability[24]. **Having a human in the loop leverages the user's situational awareness and judgement, which may be beneficial for the performance and safety of the AI-based devices.**



The AI performs a task and then waits for the human user to take an action before continuing

The AI can sense, decide, and act on its own. The human user supervises its operation and can intervene when required

The AI can sense, decide, and act on its own. The human user cannot intervene in a timely fashion.

Figure 1 *Types of controllability. Devices that are controlled or supervised by humans are also known as heteronomous devices. Devices that do not provide a means to intervene in a timely fashion are also known as autonomous devices. Hybrid devices provide direct control or supervisory control on certain functions and no control on other functions.*

Having a human in the loop requires situational awareness, enough time to intervene and a mechanism through which to intervene (a communication link or physical controls) in order to take control or to deactivate the device should circumstances require.

From a risk management and performance point of view, it may sometimes be required to take the human out of the loop, to reduce the risk as far as possible by avoiding human-machine interaction problems[25], such as lack of operator situational awareness (sensing uncertainties/limited situational awareness): the operator having insufficient knowledge of the state of the device at the time of intervention.

When specific actions require high speed or accuracy in order to be performed safely, it may be safer to circumvent the limitations of immediate, real-time human control. For example, an AI-based robot for eye surgery[26] may require the human to be taken out of the loop because of the user's limited decision making-capacity[27], limited situational awareness and sensing uncertainties. In this case, the most effective human supervision will be based on continuous oversight and retrospective periodic review of the performance for individual patients or for cohorts of patients, for example as part of Post-Market Clinical Follow-Up (PMCF).

[23] *Draft IEC 22989 - Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, published 2019-10-31.*

[24] *The High-Level Expert Group on AI in its Assessment List for Trustworthy AI (17 July 2020) distinguishes human-in-the-loop (HITL; i.e. direct control), human-on-the-loop (HOTL, i.e. supervisory control) and human-in-command (HIC). Human-in-command refers to the capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the AI system in any particular situation. The latter can include the decision not to use an AI system in a particular situation to establish levels of human discretion during the use of the system, or to ensure the ability to override a decision made by an AI system.*

[25] *Autonomy, artificial intelligence and robotics: Technical aspects of human control, ICRC, August 2019.*

[26] *For a discussion on the role and limitations of AI in eye surgery, see Urias, M.G., Patel, N., He, C. et al. Artificial intelligence, robotics and eye surgery: are we overfitted? Int J Retin Vitr 5, 52 (2019).*

[27] *High throughput computing can handle situations much faster than the human brain can let a signal pass from eye to brain to hands. Any device that ultimately relies solely or primarily on human attention and oversight cannot possibly keep up with the volume and velocity of algorithmic decision-making or will necessarily be outmatched by the scale of the problem and hence be insufficient.*

Automation is of course not a panacea. Manufacturers and health institutions must be aware that in some circumstances automation leads to deskilling, or may require more user training and higher skilled individuals than if there is no automation.[28] In that respect AI training initiatives by professional organizations such as EFOMP[29] are highly valuable and should be further encouraged.

4.2. CHANGE THROUGH MACHINE LEARNING

Some AI, such as neural networks, **learns on the basis of training data** (samples to fit a machine learning model), whereas **other forms of AI learn without training samples**, such as through genetic programming[30] or reasoning. For example, semantic computing learns through semantic networks (a knowledge base that represents semantic relations between concepts in a network) which through reasoning, deduction and inference may grow or adapt over time during its operation. Consequently, the reader must be aware that aspects related to training data as described in this paper and in the EU Whitepaper on AI are not applicable to certain types of AI. Also, hybrid approaches exist, using a combination of both, e.g. neural networks and symbolic AI. It is likely that the influence of the latter will increase in the future[31].

Where AI learns by means of training data, the manufacturer may obtain the data for processing, or instead, may use techniques such as federated learning to train the AI without obtaining the data, i.e. the data remains safely in health institutions behind differential privacy and secure aggregation shields. Only machine learning parameters are exchanged, usually encrypted (see Figure 2). The EU health data dataspace is set to enable federated learning.

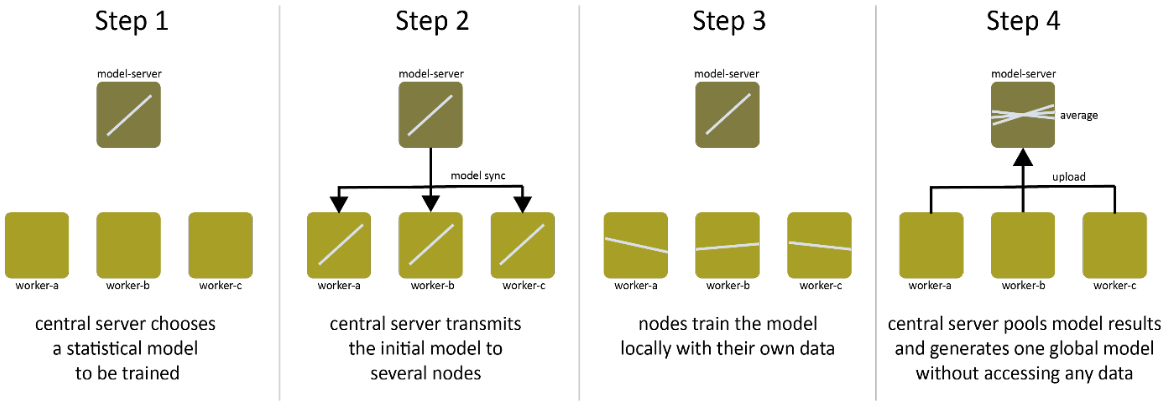

Step 1
model-server
worker-a
worker-b
worker-c
central server chooses a statistical model to be trained
Step 2
model-server
model sync
worker-a
worker-b
worker-c
central server transmits the initial model to several nodes
Step 3
model-server
worker-a
worker-b
worker-c
nodes train the model locally with their own data
Step 4
model-server
average
upload
worker-a
worker-b
worker-c
central server pools model results and generates one global model without accessing any data

Figure 2 *Federated learning is a machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging them. This approach stands in contrast to traditional centralized machine learning techniques where all the local datasets are uploaded to one server, as well as to more classical decentralized approaches which often assume that local data samples are identically distributed. The main advantage of using federated approaches is to ensure data privacy or data secrecy. Indeed, no local data is uploaded externally, concatenated or exchanged. Since the entire database is segmented into local bits, this makes it more difficult to hack into it. With federated learning, only machine learning parameters are exchanged. In addition, such parameters can be encrypted before sharing between learning rounds to extend privacy and homomorphic encryption schemes can be used to directly make computations on the encrypted data without decrypting them beforehand.*

Standardization bodies worldwide are currently developing standards to characterize data sets. Manufacturers can use these standards to establish the quality of AI training or evaluation data. They can use these characteristics to establish bias and determine whether the AI is suitable for a specific target population. **However, mandatory certification of training data against these standards is not an effective mechanism to assure the AI is safe and effective for the target population or that bias is minimized.** As explained above, some forms of AI do not rely on training data. If it does, manufacturers do not always have access to the training data. And foremost, because bias can enter the AI development chain at different points (see Figure 6), the training data being only one of those entry points. Manufacturers can make a

[28] *Ironies of automation, Bainbridge Automatica, Vol. 19, No. 6, 1983*

[29] *EFOMP is the European Federation of Organisations for Medical Physics. EFOMP is currently creating an AI curriculum for medical physicists, radiology professionals and computer scientists.*

[30] *Genetic programming is a technique to create algorithms that can program themselves by simulating biological breeding and Darwinian evolution. Instead of programming a model that can solve a particular problem, genetic programming only provides a general objective and lets the model figure out the details itself.*

[31] *Today, in the world of AI there are two school of thoughts: (1) that of Yann LeCun who thinks we can reach Artificial General Intelligence via Deep Learning alone and (2) that of Gary Marcus who thinks other forms of AI are needed, notably symbolic AI or hybrid forms. See Deep learning: A critical appraisal. arXiv 2018 G Marcus - arXiv preprint arXiv:1801.00631, 2019.*

more comprehensive assessment through the use of qualitative evaluation data.

Often training cannot be done directly online, and therefore learning takes place offline. In other cases, AI may change its model during runtime[32] through self-learning, for example by adjusting weights and parameters of the model, changing the models' architecture, switching to an earlier model, etc.

4.2.1. PRE-DETERMINED CHANGE

Pre-determined change during runtime refers to an adaptation, refinement or calibration of a device within set boundaries to the characteristics of a specific patient or healthcare setting and within the intended purpose of the device as determined by the manufacturer before placement on the market.

Pre-determined change is not unique to AI-based devices. Many medical devices adapt to the patient or their environment or compensate for wear and tear by reconfiguring or self-healing their design. For example:

- A CT machine undergoes regular calibration cycles to adjust for wear and tear. The calibration re-configures the CT software to compensate for and adapt to hardware changes.
- An APAP device (Automatic Positive Airway Pressure for patients with obstructive apnea) automatically increases pressure just enough to return breathing to normal. The air pressure from the machine rises and falls throughout the night as needed to keep the airways open. The feedback loop continuously adapts the machine performance.
- Self-healing polymers used in medical-grade seals and self-healing hydrogels and tissues used in biomaterials adapt themselves to degradation or changes in the human body.
- DNA hydrogel. The gel contains small pieces of DNA that activate when gene x of ebola or gene y for cancer is encountered, making the hydrogel change shape and administer the medicine.

Pre-determined changes through machine learning enable personalized healthcare, including e.g. a modification of the "working point" of the AI based on the local/patient environment; it allows AI to maximize performance for a given patient or situation. It allows the device to adapt to the patient, rather than force the patient to adapt to the device. E.g.

- AI used in the joints of bionic limbs allows the kinetics to be adapted to the patient, rather than let the patient adapt its gate to the kinetics of the prosthesis.
- AI for the prediction of headaches learns from environmental conditions, patient behavior and patient feedback to make predictions with higher sensitivity and specificity than if using the settings for the population average.
- AI for precision medicine enables more precise calculation of medication dose, e.g. an AI-based device for patients with Parkinson's disease learns from information regarding disease progression, symptom manifestation, drug intake and other patient characteristics to calculate the optimal dose while avoiding side effects of the drug. Rather than performance averaging out on the population's mean (e.g. 90% precision), it maximizes performance for a specific patient (e.g. 99% precision).

4.2.2. CHANGE DYNAMICS - HUMAN CONTROL OF CHANGE

Figure 3 illustrates four scenarios of how the manufacturer and the user exercise control over the learning in relation to how the device is placed on the market.

In the first scenario, the AI is locked and the manufacturer controls the learning. '**Locked AI**', is not changing its design

[32] *Runtime: the period in the software lifecycle during which a computer program is executing*

during runtime. Examples of locked AI are static look-up tables, decision trees, and complex classifiers[33]. Locked AI generally provides the same result each time the same input is applied to it, although there are some exemptions to this, for example, in case the AI contains non-deterministic[34] algorithms or when the user is able to change the working point on the operating curve. A 'locked' AI may nevertheless still change. Consider an algorithm to screen for tuberculosis at airports. Whereas the algorithm's design is locked, the user may still choose a point on the operating curve different from the factory default. For example, to trade-off increased sensitivity with reduced specificity.

AI can change during runtime in various other ways. In the second scenario (continuous change), the model continuous to learn within the boundaries set by the manufacturer. Consider for example an AI for precision medicine that calculates the optimal medication dose to reduce the tremor of a patient with Parkinson's disease, while limiting the side effects of the drug. . As the disease progresses over months or years, symptoms change. The algorithm continues to evolve together with the patient's disease state, just like 'locked AI'. In this scenario, the user may change the working point on the operating curve. A patient may, for example, on a particular day, decide to pick a point on the operating curve that lowers the dose, allowing for more tremor, but improving his cognitive performance. A patient may prefer a different operating point because the medication causes mild cognitive impairments, such as distraction, disorganization, difficulty planning, and accomplishing tasks.

In the third scenario (discrete changes) the learning initially occurs under the manufacturer's control. The model is then handed over to the user (or another party) for further calibration or adjustment to the local context or to a specific patient. The change occurs within the intended use, within the change boundaries and according to the manufacturer's algorithm change protocol (see next section for a description of change boundaries and algorithm change protocol). The manufacturer remains responsible for the device. Consider, for example, an AI for the prediction of sepsis. The hospital makes a change in its local practices, now also encoding blood parameters procalcitonin and IL-6 and making these available for the AI. The manufacturer has proved these blood parameters to work as valid inputs, described in the algorithm change protocol. The user can now further improve the local model's performance by training the AI on these extra blood parameters, following the algorithm change protocol defined by the manufacturer.

In the fourth scenario, the manufacturer places the device on the market, but then the user intentionally changes the local model in a way not allowed by the manufacturer's change control plan, either by making a change

a. beyond the manufacturer's pre-determined change envelope (a.k.a. change boundaries or pre-specifications), for example for purpose not covered by the intended use or for more specific purposes than claimed by the manufacturer
b. While not complying with the manufacturer's Algorithm Change Protocol

In the fourth scenario the device is intentionally changed by the user in a significant way. The user is misusing the device. Consider, for example, an AI to read quantitative Polymerase Chain Reaction (qPCR) assays. The AI can handle qPCR curves generated for assays for plant, animal, or human specimens. Assume a second manufacturer or a health institution produces an assay for the detection of SARS-COV-2. By continuing the AI training, it becomes especially good at reading qPCR curves associated with a SARS-COV-2 assay. 'Reading qPCR curves for SARS-COV-2' is a more specific claim and requires a higher level of performance before it is considered state-of-the-art than is 'reading qPCR curves for assays for plant, animal or human specimen'.

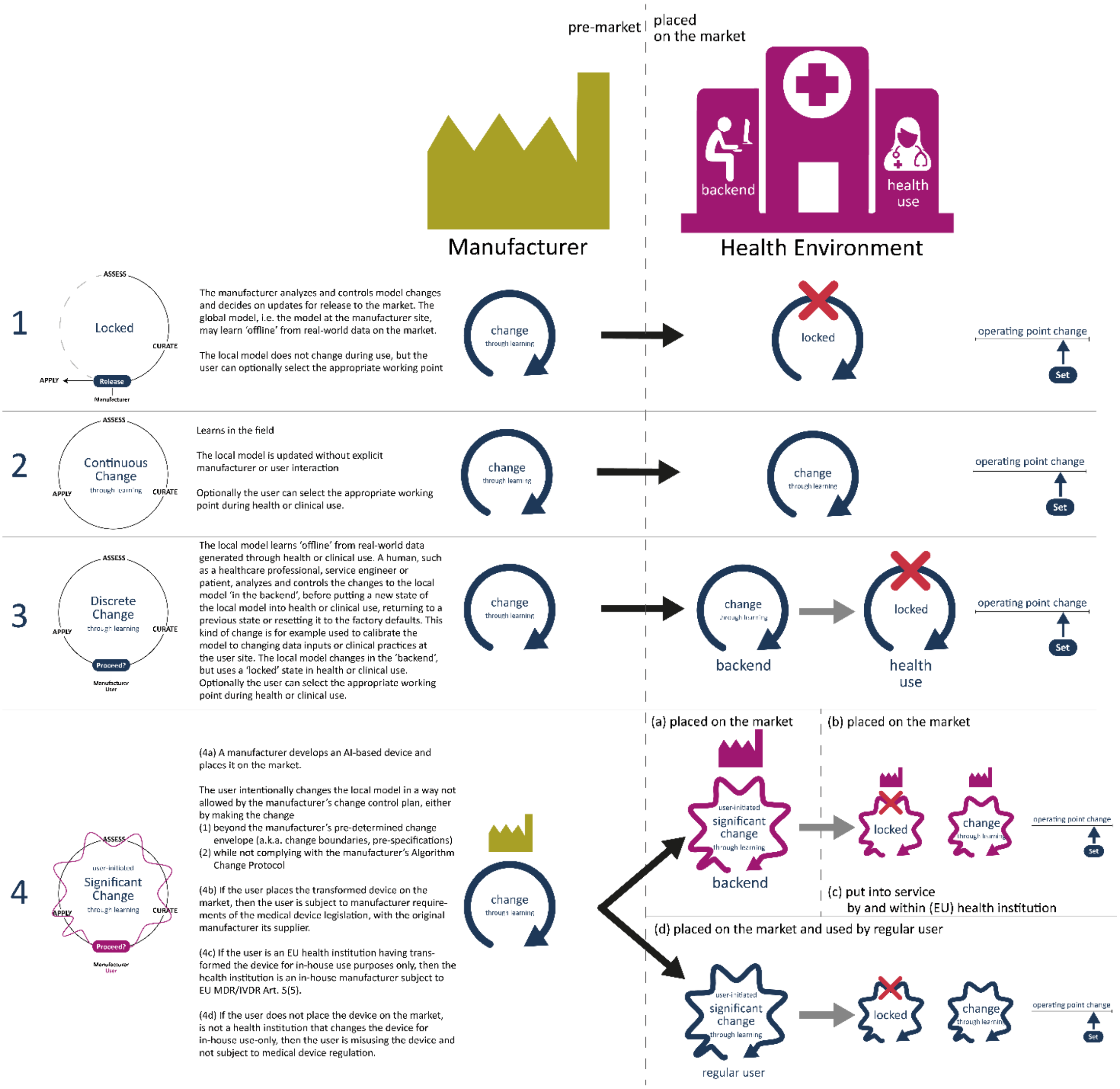
Consequently, the more specific claim is considered a significant change. A manufacturer or Eu-based health institution (following EU MDR Art. 5(5) on in-house manufacturing) performing such change carries the manufacturer responsibilities under medical device regulations. Suppose the second manufacturer can prove safety and performance without having the technical documentation of the original device. In that case, the original manufacturer's intellectual property remains protected if the Notified Body or competent authority accepts the 'new' device's technical documentation containing just a reference to the master file of the original device. That master file then has to be made available by the original manufacturer to the Notified Body. Note that also the FDA provides the possibility to use master files.

[33] *Discussion Paper "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)", published by US Food and Drug Administration on 2019-04-02.*

[34] *Whereas computer programs generally excel at repetitive behavior, certain AI (e.g. probabilistic AI, soft computing and fuzzy logic), in order to cope with very noisy input data, will employ an execution flow that is very un-deterministic, but will nevertheless each time reach a deterministic answer, within certain margins of tolerance. For example, you can run the program a hundred times, it will never run the same way twice, but it will (should) consistently produce the same result, within the margins specified by the manufacturer. It has inherent variability to tolerate imprecision, uncertainty and partial truth in real world data to solve complex problems while achieving tractability, robustness and low cost. Also, AI may use differential privacy, a technique that carefully injects random noise to protect individual privacy. The goal of such systems is to protect privacy by making it impossible to reverse engineer the precise inputs used, while still delivering an output that's close enough to the accurate answer.*

Also hybrid scenarios may exist, whereby the model continuous to evolve, but the user has the ability to revert back to an earlier state of the model or to the factory default.

Note that having a human in the loop during learning to control what model state is put into clinical use, is different from having a human in the loop to control the device during clinical use, i.e. a continuously changing AI does not have a human in the loop to control the learning, but can nevertheless have a human in the loop to take control of device functions during clinical use, for example through a device override or emergency stop.



The manufacturer analyzes and controls model changes and decides on updates for release to the market. The global model, i.e. the model at the manufacturer site, may learn 'offline' from real-world data on the market.

The local model does not change during use, but the user can optionally select the appropriate working point

Learns in the field

The local model is updated without explicit manufacturer or user interaction

Optionally the user can select the appropriate working point during health or clinical use.

The local model learns 'offline' from real-world data generated through health or clinical use. A human, such as a healthcare professional, service engineer or patient, analyzes and controls the changes to the local model 'in the backend', before putting a new state of the local model into health or clinical use, returning to a previous state or resetting it to the factory defaults. This kind of change is for example used to calibrate the model to changing data inputs or clinical practices at the user site. The local model changes in the 'backend', but uses a 'locked' state in health or clinical use. Optionally the user can select the appropriate working point during health or clinical use.

(4a) A manufacturer develops an AI-based device and places it on the market.

The user intentionally changes the local model in a way not allowed by the manufacturer's change control plan, either by making the change
(1) beyond the manufacturer's pre-determined change envelope (a.k.a. change boundaries, pre-specifications)
(2) while not complying with the manufacturer's Algorithm Change Protocol

(4b) If the user places the transformed device on the market, then the user is subject to manufacturer requirements of the medical device legislation, with the original manufacturer its supplier.

(4c) If the user is an EU health institution having transformed the device for in-house use purposes only, then the health institution is an in-house manufacturer subject to EU MDR/IVDR Art. 5(5).

(4d) If the user does not place the device on the market, is not a health institution that changes the device for in-house use-only, then the user is misusing the device and not subject to medical device regulation.

Figure 3 *Four change scenarios for AI-based medical devices. If such novel change were made by another legal entity for placement on the market, than that other legal entity is considered to perform re-manufacturing and takes on the manufacturer responsibilities. If such novel change were made by another legal entity for placement on the market, than that other legal entity is considered to perform re-manufacturing and takes on the manufacturer responsibilities.manuf*

4.2.3. CHANGE BOUNDARIES AND ALGORITHM CHANGE PROTOCOL

The manufacturer must specify a change envelope or change boundaries and an Algorithm Change Protocol. As long as the device operates within the related change boundaries, its safety and performance are guaranteed (e.g. with a minimum specificity and sensitivity). The manufacturer can ensure this through procedural (e.g. acceptance testing) and/or technical measures. How change envelopes can be defined depends on the technology used. The manufacturer should be able to demonstrate why the chosen parameters and threshold values are valid in consideration of clinical state of the art and the intended purpose of the device.

4.2.4. CHANGE ACCORDING TO EU MDR AND EU IVDR

Before a device can be placed on the market, the Medical Device Regulations require a manufacturer to perform a conformity assessment to demonstrate the requirements of the regulation relating to the device have been fulfilled.[35] Devices can change in terms of design and characteristics after conformity assessment, but only if manufacturers have a quality management system in place to address these changes in a timely manner with regards to regulatory compliance, including compliance with conformity assessment procedures.[36] Manufacturers are prohibited to suggest uses for the device other than those stated in the intended use for which the conformity assessment was carried out.[37]

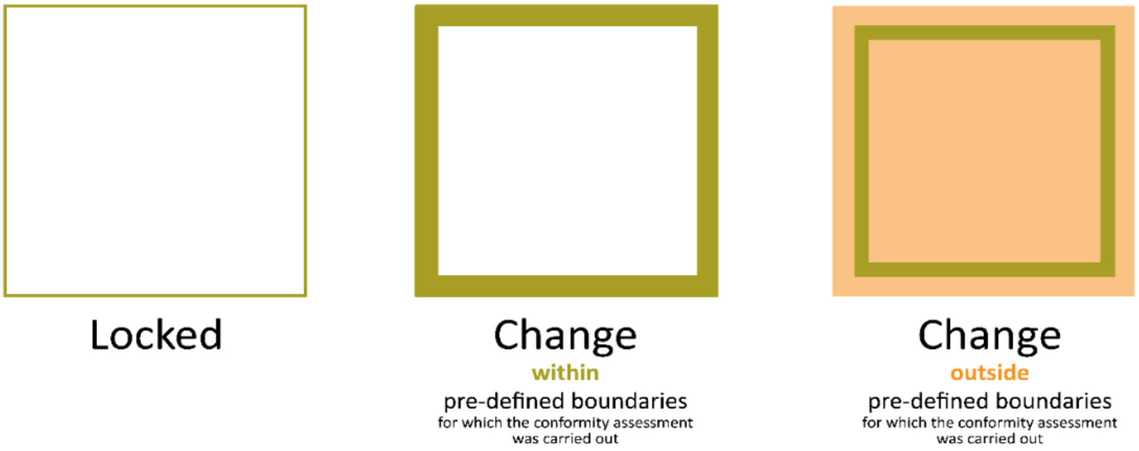

Locked
Change
within
pre-defined boundaries
for which the conformity assessment was carried out
Change
outside
pre-defined boundaries
for which the conformity assessment was carried out

Figure 4 *Illustration of AI change types. EU MDR and EU IVDR allow hardware devices to be placed on the market that recalibrate or reconfigure themselves within certain boundaries for which a conformity assessment was carried out. Similarly, manufacturers can place devices on the market comprising AI that changes within pre-defined boundaries for which a conformity assessment was carried out. Currently the EU MDR and EU IVDR do not allow manufacturers to place devices on the market comprising AI that changes outside of pre-defined boundaries.*

Notified Bodies must have documented procedures and contractual arrangements in place with the manufacturer relating to the assessment of changes to the approved design of a device and the intended use of or claims made for the device. Manufacturers must submit plans for such changes for prior approval where such changes may affect conformity with the general safety and performance requirements or with the conditions prescribed for use of the product, including for changes related to limitations of the intended purpose or conditions of use. The Notified Body must assess the proposed changes and verify whether, after these changes, the design of a device or type of a device still meets the requirements of the regulation and notify the manufacturer of its decision and provide a report or as applicable a supplementary report to the EU technical documentation assessment certificate containing the justified conclusions of its assessment.[38]

This implies that **a manufacturer can place a device on the market that is able to change within a pre-defined change envelope or tolerances for which a conformity assessment was carried out**, in consideration of contractual agreements between notified body and manufacturer with regards to the assessment of design changes.

[35] *EU MDR Art. 2 (40) and Art. 52(1) and EU IVDR Art. 2 (32) and Art. 48(1)*
[36] *EU MDR Art. 10(9) and EU IVDR Art. 10(8)*
[37] *EU MDR and EU IVDR Art. 7(d)*
[38] *Annex VII Requirements to be met by Notified Bodies Section 4.9, Annex IX Conformity Assessment based on a quality management system and on assessment of technical documentation - Chapter II Assessment of the technical documentation Section 4.10 and Annex X Conformity Assessment based on Type-Examination Section 5 Changes to the type*

In contrast to that, **the EU MDR and EU IVDR currently do not allow manufacturers to place AI-based devices on the market intended to change outside of the change envelope or to suggest claims, intended uses or use conditions to the device for which no conformity assessment was carried out** (see Figure 3), for example:

device that learns from real-world data to document safety and performance for extended patient cohorts which it was not validated on before being placed on the market. This is considered a significant change in safety and performance characteristics and requires a new conformity assessment.

Changes outside of the change envelope or assigning new claims or use conditions require an update of the technical documentation, including the clinical evaluation and a new conformity assessment to be carried out.[39] Significant changes to the pre-determined Algorithm Change Protocol require an update of the technical documentation, including the clinical evaluation and a new conformity assessment to be carried out.

If a natural or legal person (1) changes the intended purpose or (2) modifies a device already placed on the market or put into service in such a way that compliance with the applicable requirements may be affected, then that person shall assume the obligations incumbent on manufacturers, except if that person changes the device without changing its intended purpose to adapt it for an individual patient.[40] This implies that a health institution can for example, adapt an AI-based bionic eye to restore a patient's eyesight if the eye is intended for that purpose, even if this involves a modification in such a way that compliance may be affected.

A health institution can (1) change the intended purpose or (2) modify a device in such a way that compliance with the applicable requirements are affected so that it can be used on multiple patients, but only if the health institution meets the conditions for in-house manufacturing[41], i.e. (a) the device is not transferred to another legal entity, (b) it has an appropriate quality management system in place, (c) justifies that the target patient group's specific needs cannot be met, or cannot be met at the appropriate level of performance by an equivalent device available on the market, (d) provides information on the manufacturing, modification and use to its competent authority upon request and draws up a declaration which it shall make publicly available.[42] The exception to this rule is when a health institution adapts a device for a purpose not in scope of the medical device definition, e.g. adapt a bionic limb for superhuman purposes rather than to alleviate or compensate for a disability, then the conditions for in-house manufacturing must not be met.

[39] *EU MDR Art. 27(3) and EU IVDR Art. 24(3)*
[40] *EU MDR and EU IVDR Art. 16*
[41] *EU MDR and EU IVDR Art. 5(5)*
[42] *EU MDR and EU IVDR Art. 5(5)*

5. ETHICS

Ethics is used in the meaning of respecting human values, including safety, transparency, accountability, and morality, but also in the meaning of confidentiality, data protection and fairness. Many of these aspects are already covered by EU MDR and GDPR as discussed elsewhere in this document. They are not new as philosophers have been debating ethics for millennia.

On the other hand, the science behind creating ethical algorithms is relatively new. Computer scientists have a responsibility to think about these aspects of technologies they are involved in and mitigate or resolve these issues. Of these ethical aspects, fairness is probably the most complicated because fairness can mean different things in different contexts and to different people[43].

To consider the ethical aspects of software that changes itself, the European Parliamentary Research Service[44] **frames it as a real-world experiment**. In doing so, it shifts the question of evaluating the moral acceptability of AI in general to the question of **'under what conditions is it acceptable to experiment with AI in society?'** It makes the **analogy to healthcare** where medical experimentation requires manufacturers to be explicit about the experimental nature of healthcare technologies by following the rigorous procedures of a **clinical investigation**, subject to ethics committee approval, patient consent and **careful monitoring** in order to protect the subjects involved or impacted.

Under the EU Medical Device Regulations (EU MDR & EU IVDR) a manufacturer can only place medical devices, including AI-based devices, on the market for use on patients or their data when these are safe and effective. Once the device is on the market, the manufacturer must perform clinical **evaluations throughout the entire lifetime of the device**, including post-market clinical follow-up, to prove the assumptions remain valid and no risks emerge that are unacceptable. Devices that change during use can do so only within predefined boundaries considered during the conformity assessment procedure. For the majority of medical software, a third party, a so-called 'notified body', performs the conformity assessment, both premarket (ex-ante) and post market (ex-post).

The medical device regulations impose strict limitations with regards to the significance of changes allowed by the AI manufacturer before a new conformity assessment is required. Algorithms that change themselves during use can only do so within predefined boundaries taken into account during the conformity assessment (see chapter 4.2.4). To allow AI to be deployed that changes beyond those boundaries a change in regulation is required. To achieve the same level of control, requirements would need to be established for organizations that control the data pipelines for training such AI during use. In medical care the organizations that control the data pipelines are usually not the manufacturers, but the health institutions (e.g. hospitals), platform managers and healthcare authorities. To some extent such requirements are already in place for health institutions wish to train and operate such software for in-house use (see EU MDR & EU IVDR Article 5(5)), but these are not specific to AI. The European Parliamentary Research Service[45] proposes that such institutions obtain a data hygiene certificate, perform an ethical Technology Assessment (eTA) and complete an Accountability Report to deploy and operate such AI.
To deal with ethical aspects many AI ethics frameworks have appeared in recent years[46]. These differ based on the organization's goals and operating contexts. Such frameworks have limits, for example because **many AI systems comprise a tradeoff between algorithmic fairness and accuracy[47,48]**. A fair algorithm should provide the same benefits for the group you are trying to protect from discrimination. An accurate algorithm on the other hand should make a

[43] *There are many different interpretations of fairness. The European Parliament Panel for the Future Science and Technology (STOA) in its study Artificial intelligence: From ethics to policy (June 2020) defines fairness as the requirement to equally distribute goods, wealth, harms, and risks. The GDPR refers to substantive fairness (Recital 71): fairness of the content of an automated inference or decision, which, according to the STOA report The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (25 June 2020) can be summarized as (A) acceptability, i.e. the input data (the predictors) for the AI decision being normatively acceptable as a basis for the inferences concerning individuals (e.g., the exclusion of ethnicity if this does not impact disease determination), (B) Relevance: the inferred information (the target) should be relevant to the purpose of the decision and normatively acceptable in that connection, (C) Reliability: both input data, including the training set, and the methods to process them should be accurate and statistically reliable (which is an aspect that must be proven in the clinical evaluation or performance evaluation of a medical device). On the other hand the GDPR also informational fairness (Recital (60): that the subject must be informed be informed of the existence of the processing operation and its purposes. The High-Level Expert Group on Artificial Intelligence considers fairness to have both a substantive and a procedural dimension. The substantive dimension implies a commitment to: ensuring equal and just distribution of both benefits and costs, and ensuring that individuals and groups are free from unfair bias, discrimination and stigmatization. The procedural dimension of fairness entails the ability to contest and seek effective redress against decisions made by AI systems and by the humans operating them. Ethics Guidelines for Trustworthy AI, 8 April 2019. The European Parliament Panel for the Future Science and Technology (STOA) defines fairness as the requirement to equally distribute goods, wealth, harms, and risks. Artificial Intelligence: From Ethics to policy. 24 June 2020.*

[44] *Artificial intelligence: From ethics to policy, European Parliament Panel for the Future Science and Technology (STOA), (June 2020*

[45] *Artificial intelligence: From ethics to policy (June 2020), European Parliament Panel for the Future Science and Technology (STOA)*

[46] *The Ethics of Artificial Intelligence: Issues and initiatives. STOA Panel, 11 March 2020, Alan Winfield e.a., Science Communication Unit at the University of the West of England at the request of the Panel for the Future of Science and Technology (STOA).*

[47] *The Ethical Algorithm: The Science of Socially Aware Algorithm Design, Michael Kearns and Aaron Roth, 1 November 2019, Oxford University Press*

[48] *Artificial intelligence: From ethics to policy. European Parliamentary Research Service. Scientific Foresight Unit (STOA). June 2020.*

prediction that is as precise as possible for a certain subgroup, e.g. according to age, gender, smoking history, previous illnesses, etc. **Where an algorithm lies on the tradeoff curve between fairness and accuracy, often is a matter of public policy,** rather than for the organization to decide in isolation. Take for example the hypothetical example of an AI algorithm used during the COVID-19 pandemic to determine what patient should receive treatment. Certain countries or regions would prefer to allocate their scarce resources to patients that are predicted to have the highest chance of survival (accuracy prevails), whereas others may prefer to apply a fair allocation of resources and not take the patient's age and gender into consideration (fairness prevails). Such national and regional differences require a handshake between the company's ethics framework and that at policy level. To accommodate for national and regional differences algorithms can be designed so they can be adjusted by the ethics committees at hospitals or at regional level to the level of accuracy versus fairness desired.

- **COCIR recommends** updating IEC 82304-1 by requiring manufacturers to inform users on how to adjust the "knob" when fairness/accuracy trade-offs exist and can be adjusted by the user

Ethics committees emerged in healthcare in the 1970's at the very heart of hospitals. Initially they focused on **research ethics** for clinical investigations on human subjects. Such committees exist throughout Europe and are regulated by law. Nowadays many of these committees have organized themselves at regional or national level and also focus on **clinical ethics.** They have evolved into democratic platforms of public debate on medicine and human values. There is no single model, every country has created its own organizational landscape, in accordance with its moral and ideological preferences, adapted to the political structure of its health system, and to its method of financing health care.[49] This complex reality and the **lack of a unified European approach** make it challenging for companies to engage with ethics committees and find a single working point on the tradeoff curve between accuracy and fairness that is acceptable across the EU.

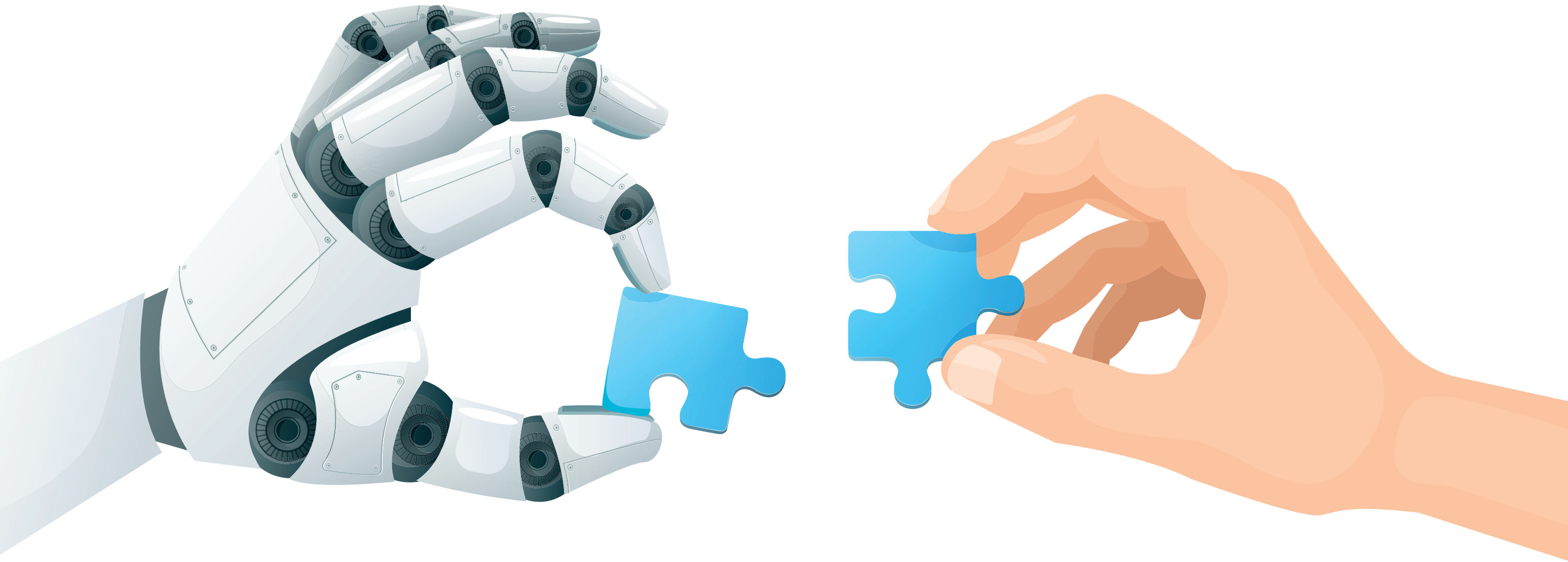
On a horizontal level **the General Data Protection Regulation offers** many options for effective **supervision and enforcement on fairness, transparency, individual rights and granting an individual control over their personal data. It does not affect algorithms that do not process personal data or that impact population rights (e.g. democracy).** In a letter to Member of the European Parliament Sophie in't Veld[50] the European Data Protection Board (EDPB) explains that the GDPR lays out the general principles, i.e. lawfulness, fairness and transparency, accuracy, data minimization and purpose limitation, that govern the processing of personal data, both when creating and using algorithms.[51] Controllers must ensure compliance with the GDPR and be able to demonstrate it. This means controllers are obliged to consider all the potential risks that the use or creation of the specific algorithm can potentially pose to the rights and freedoms of natural persons and, if necessary, take measures to address these risks. With regards to AI systems, the measures to be taken by controllers include controls over the adequacy and completeness of training sets, and over the existence of causes of bias and unfairness[52]. While GDPR Article 24 primarily concerns the rights to data protection and privacy, it may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, and the rights to liberty, conscience and religion.[53]

Furthermore, GDPR Article 22 prohibits any decision-making based solely on automatic processing of personal data, if such a decision "produces legal effects concerning [the data subject] or similarly affects [the data subject]".[54] This means that in practice it will often not be possible to rely solely on the outcome of an algorithm for sensitive decision-making. Furthermore, Article 22 requires the controller to implement suitable measures to safeguard the data subject's rights and freedoms and its legitimate interests, which has to include the right to obtain human intervention.[55] This human intervention has to be qualified, capable of discovering and recovering unfair outcomes or discriminations, as the European Data Protection Board (EDPB) has pointed out in its guidelines on data protection by design and by default.[56]

[49] *Ethical Function in Hospital Ethics Committees, Guy Lebeer, IOS Press, 2002.*
[50] *Response by the European Data Protection Board to MEP Sophie in't Veld, 29 January 2020. EDPB website.*
[51] *General Data Protection Regulation, Article 5, Official Journal of the European Union, 27 April 2016.*
[52] *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliamentary Research Service - Scientific Foresight Unit (EPRS - STOA). 25 June 2020*
[53] *Art. 24 and Art. 35 GDPR; Article 29 Working Party "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". WP 248 rev.01, 4 2017 - endorsed by the EDPB. https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.*
[54] *GDPR Art. 22(1). This prohibition has limited exceptions listed in Article 22(2) GDPR. See for more specific guidance on Article 22: Article 29 Working Party ''Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679'' WP 251 rev.01, as last Revised and Adopted on 6 February 2018 – endorsed by the EDPB.*
[55] *GDPR Art. 22(3)*
[56] *EDPB "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default". Version 1.0, 13 November 2019.*

COCIR recognizes that the adherence to ethical principles is a shared responsibility between manufacturers, deployers and operators of medical devices. Ensuring that AI systems follow and embody ethical principles cannot be done by manufacturers, deployers or operators independently on their own. Each party has to take appropriate and well-defined steps within their control.

Note that ethics principles are not requirements, but that requirements need to be derived from principles. A better understanding needs to be developed on how principles can be translated into design requirements.



6. TRUST

Only by gaining the user's trust will AI-based devices find their way into the care pathways. Trust has multiple dimensions; EU MDR and EU IVDR address several of these dimensions. This chapter first discusses dimensions of trust not covered by the Medical Device Regulations, followed by those required by the regulations.

6.1. TRANSPARENCY - EXPLICABILITY

Transparent AI presents core elements of decision-making in an open, comprehensive, accessible, clear, unambiguous, and interpretable way.[57] The first question that comes to mind when considering algorithmic interpretability is: 'interpretable to whom?' The very word 'interpretable' implies an observer or subjective recipient who will judge whether she can understand the algorithm's model or its behaviours. Another challenge is the question of what we want to be interpretable: the historical data used to train the model, the model, the performance of the model found by the algorithm on a population cohort, or the decisions made by the model for a particular case?

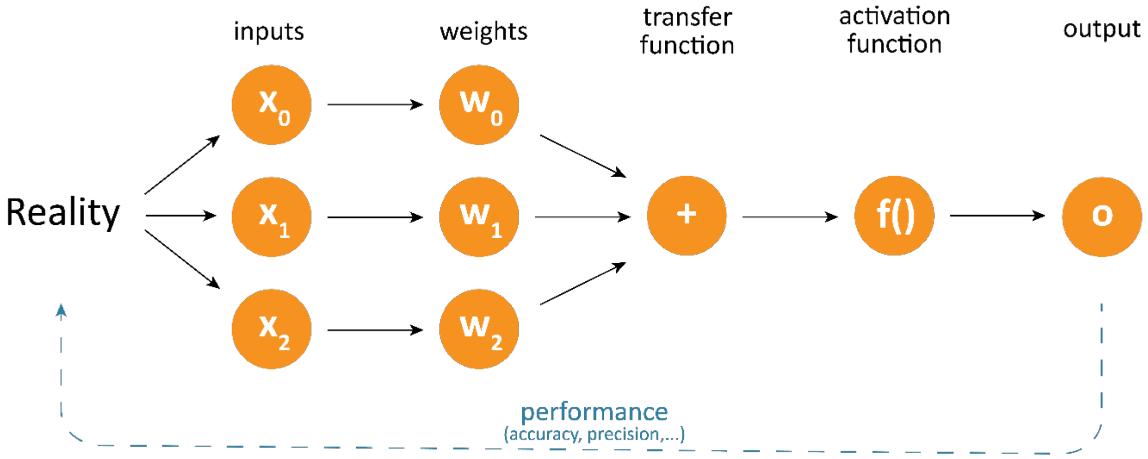


Figure 5 Neural networks comprise relatively simple models, with weights, transfer and activation function, but due to the vast amount of data, a person will not be able to process this information to the point of understanding it. AI being technically interpretable or transparent does not automatically imply that a doctor or a patient is able to interpret it, i.e. to understand cause and effect. A different level of abstraction is required to make the neural network interpretable to users.

Early well-known machine learning models are rather simple (see Figure 5), principled (maximizing a natural and clearly stated objective, such as accuracy), and thus are interpretable or understandable to some extent. However, the 'rules' used by such models can be extremely difficult to fully understand. They may capture complex and opaque relationships between the variables in what seemed to be a simple dataset. While radiologists may look for "a curved tube resembling a ram's horn, located in the inner region of the temporal lobe of the brain, to identify the hippocampus", AI may use features and patterns that are not articulable in human language. While this makes AI into an extremely powerful tool for clinical decision making, it also brings the risk of the AI reflecting spurious correlations in the data or overfitting to this particular dataset at the cost of transferability. Thus, simple algorithms applied to simple datasets can nevertheless lead to inscrutable models. But it is also entirely possible that even a model we cannot understand 'in the large' or that is hidden from the user can make specific decisions that we can understand or rationalize post hoc[58]. For example, a doctor can review the output of an algorithm that reports on the wound healing stage (hemostasis, inflammatory, proliferative or maturation) by looking at a wound picture to determine whether the algorithm identified the healing phase

[57] *Transparency is defined as open, comprehensive, accessible, clear and understandable presentation of information (ISO 20294:2018, 3.3.11) or as openness about activities and decisions that affect stakeholders and willingness to communicate about these in an open, comprehensive, accessible, clear and understandable manner (draft IEC 22989 - Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, published 2019-10-31.)*

[58] *This phenomenon is called emergence. Emergence occurs when an entity is observed to have properties its parts do not have on their own. Similar to how the function of a biological organism emerges from the interaction of its cells: properties emerge in the organism that are not present and understood when looking at the cellular level. Wikipedia, accessed 19 June 2020.*

correctly. Alternatively we can interrogate the model by having it tell us what it would do on any input. We can explore **counterfactuals** such as "***What would be the smallest change in input data that would change the decision?***" This type of explanatory understanding at the level of individual decisions or predictions is the basis for some of the more promising research on interpretability.[59]

Explained variance, i.e. "Given a blank sheet, ***what would be the minimum input data needed to receive this decision?***" is on the opposing end of counterfactuals, i.e. "*Given the complete picture, what is the minimum change needed to also change the answer?*" Explained variance involves the AI providing "*the minimum set of input data needed to come close to its decision*". The minimum set of information depends on the desired level of closeness, which may differ for novice versus expert users. For example, an AI predicting the probability of survival from COVID-19 infection may explain to the user that "age" contributed to 80% of its prediction. For some users this may be sufficient information, whereas other users may want the AI to explain 99% of its prediction adding that patient history contributed to 15%, specific lab results 3%, symptoms 0.5%, etcetera. [60]

'Inexplicable' devices are not unusual, as healthcare has long been known for accepting 'inexplicable' devices for certain purposes, as long as the technical file includes a description of the technology and adequate evidence of safety and performance. For example, manufacturers demonstrated via randomized controlled studies that electro-convulsive therapy is highly effective for severe depression, even though the mechanism of action is unknown. Likewise, for many drugs under the medicines regulations, such as Selective Serotonin Reuptake Inhibitors (SSRI) or anaesthetic agents.

If a technology is significantly more effective than traditional methods in terms of diagnostic or therapeutic capabilities, but it cannot be explained, then **it poses ethical issues to hold back technology, simply on the basis that we cannot explain or understand it**. **Explicability is a means (to trust), not a goal. A blanket requirement that machine-learning systems in medicine be explicable or interpretable is therefore unfounded and potentially harmful**[61]. Of course, the advantage of making the model interpretable is that it helps the user gain confidence in the AI system faster, which in turn allows the company to be successful commercially.

Enclosed AI, i.e. AI that has no actionable outcome, **may not require transparency** towards the care provider or patient, but does require sufficient level of explicability[62] to the manufacturer or service engineer to allow verification, error detection and troubleshooting. An example would be an AI that controls the cooling of an MRI motor coil.

6.1.1. TRANSPARENCY ON THE USE OF AUTOMATED DECISION MAKING

The rules in the EU General Data Protection Regulation (EU) 2016/679 (GDPR)[63] imply that **when it is not immediately obvious that the user is interacting with an automated decision making process rather than a human** (e.g. because there is no meaningful human involvement techniques to for example improve a sensor or optics within a device), that a software device must **inform users** of this; in particular patients, and include meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[59] *The Ethical Algorithm: The Science of Socially Aware Algorithm Design, Michael Kearns and Aaron Roth, 1 November 2019, Oxford University Press*

[60] *Other methods are emerging for programmatically interpretable reinforcement learning in which the black box and other models become not the ultimate output of the learning process, but an intermediate step along the way. As an example, consider DeepMind's OCT AI. It uses optical coherence tomography (OCT) scans. These 3D images provide a detailed map of the back of the eye. DeepMind split the AI in two parts. The first AI identifies all that is abnormal, such as bleeding in retina, leakage of fluid or water logging of the retina. It highlights all those features. The second AI then categorizes them as for example diabetic eye disease with a percentage representing the confidence. Even if the AI appeared to have it wrong, some of cases made the scientists realize that the algorithm had noticed something that the healthcare professionals had not spotted. Some of those cases were very ambiguous, challenging cases and the researchers realized that their gold standard might have to be adapted. Source: DeepMind Podcast, Episode 5 "Out of the lab", August 27, 2019.*

[61] *Artificial Intelligence and Black-Box Medical Decisions: Accuracy versus Explainability. London AJ, Hastings Cent Rep. 2019;49(1):15–21. doi:10.1002/hast.973*

[62] *Explicability: property of an AI system that important factors influencing the prediction decision can be expressed in a way that humans would understand. Modified from "explainability" as defined by draft IEC 22989 - Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, published 2019-10-31.*

[63] *GDPR Art. 13(2) (f) controllers must, at the time when the personal data are obtained, provide the data subjects with further information necessary to ensure fair and transparent processing about the existence of automated decision-making and when such is the case, include meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Art. 22 The data subject shall have the right not to be subject to a decision based solely on automated processing […] which […] significantly affects him or her.*
[…] data controller shall implement suitable measures to safeguard the data subject's rights, freedoms, and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
For guidance related to automated-decision making and profiling under GDPR, see wp251rev.01 published by Art. 29 Working Part (WP29), re-endorsed by European Data Protection Board (EDPB) as GDPR: Guidelines, Recommendations, Best Practices. EDPB is the successor of WP29. EDPB is the entity comprising the national information protection authorities. It guards and enforces the consistent implementation of the GDPR across the EU.

6.1.2. TRANSPARENT DECISION-MAKING

Manufacturers are motivated to make AI decisions transparent for several reasons:

1. To gain user trust, integrate their device into clinical care and ensure adoption (= commercial success)
2. To clarify the liability, i.e. did the doctor or the user make a mistake, was it the AI, incorrect or unforeseen input data, or a malicious actor, e.g. hackers or disgruntled employees?

Unless if testing evidence is sufficient, transparency may also be needed

3. To allow manufacturers to determine operating parameters (when the device works or does not work), limitations to the intended use, contra-indications, inclusion and exclusion criteria for input data.
4. To enable debugging of the system and detect potential issues of bias.

The EU MDR and EU IVDR does not require devices to explain or render transparent their decisions to the user, nor does it preclude manufacturers from placing 'inexplicable'[64] devices on the market. The EU MDR and EU IVDR instead requires that manufacturers demonstrate that the safety and performance of their devices reaches state of the art considering its intended use. For some devices, this implies that decisions made by AI are 'explained' to the point of becoming actionable to the user[65], to ensure the safe and effective use of the device. I.e. a technical explanation of a neural network used for precision medicine by laying out its weights, transfer and activation function generally does not render the decision-making actionable to the user. Instead, the software for instance can give an indication of how the calculated dose is influenced by the patient's disease progression, the measured symptom manifestation and the patient's preferences. As another example, identifying an upcoming delirium in hospitalized patients before symptoms clearly manifest themselves to the naked eye, without any information on causation or logic behind the prediction may not be sufficient for doctors, as the condition can manifest itself in many, often contradictory ways[66]. This AI is intended to influence the user's behaviour. It must be able to "explain" it's decision-making, i.e. provide underpinning information, in an understandable way to become effective.

GDPR Article 12-14 require that controllers provide meaningful information about the AI's logic, as well as the significance and envisaged consequences. Transparency according to the GDPR is about enabling data subjects to understand and to make use of their rights in GDPR Art. 15 to 22[67], if necessary. GDPR Article 15 on the data subjects' rights to access information about the processing of their data is however formulated too ambiguously to conclude that a data subject has the right to obtain an individualised explanation of automated assessments and decisions, rather than just general information on the methods adopted by the AI system.[68]

The EU Committee on Legal Affairs[69] does not require AI *decisions* to be explained to the *user*. Instead it proposes that AI is *developed, deployed and used in an easily explainable manner* so as to ensure that there can be a review of the technical processes of the technology.

- **Rather than legislators issuing a blanket requirement for all AI to be explained, COCIR suggests AI to be made transparent to the point of becoming actionable to the user, if required to ensure the safe and effective use of the device**

[64] *The terms "explicable" and "explainable" are mostly interchangeable – both describe things that can be explained. The terms have differentiated slightly in modern use, though. Explicable tends to describe things that are seemingly without logic, especially human actions, feelings, and creations. Explainable tends to describe nonhuman things, especially natural and supernatural phenomena. Grammarist.com; accessed 23 June 2020.*

[65] *Actionable items and explanation are in principle independent. An AI agent may return (1) an actionable items without (2) an explanation, or vice versa. The AI may for example inform the user (1) "this patient is developing sepsis, administer antibiotics" or (2) "this patient's age and history are indicative of this patient developing sepsis", whereas the latter may not be actionable. A "useful" actionable item provides a patient-specific explanation.*

[66] *Delirium can be hyperactive, hypoactive, mixed, with or without motoric symptoms*

[67] *GDPR Art. 15 (right of access by the data subject), Art. 16 (right of rectification), Art. 17 (right of erasure, "right to be forgotten"), Art. 18 (right to restriction of processing)*

[68] *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliamentary Research Service - Scientific Foresight Unit (EPRS - STOA). 25 June 2020*

[69] *Draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL), art. 8(f)), 4 April 2020, Committee on Legal Affairs, website European Parliament, accessed 8 May 2020.*

6.1.3. TRANSPARENT ALGORITHM CHANGE

In case of AI that changes during runtime, manufacturers can increase trust necessary for implementation by informing regulators and users about:

1. How the AI learns over time
2. What the allowed change envelope/boundaries are of the AI
3. What caused a significant change of the AI behaviour
4. How the performance and safety is being assured as it adapts
5. How quality control of new training data is assured
6. What triggers algorithm change
7. What performance and confidence levels[70] are during a given time frame
8. Whether and how a user can reject an algorithm change or roll-back to a previous state[71]

For troubleshooting purposes, a manufacturer may also want to be able to monitor actual performance and change/drift of an evolving algorithm to detect performance deficits, for example by implementing **traceability** through an audit trail.[72]

6.2. CONFIDENTIALITY & DATA PROTECTION

The General Data Protection Regulation (EU) 2016/679 (GDPR)[73] requires safeguarding the protection of personal information when processed. The EU MDR and EU IVDR have provisions with regards to the processing of personal data, notably with regards to assuring the effective implementation to the regulation. Manufacturers, Competent Authorities, European Commission and Notified Bodies may perform inspections, investigations, and audits to assure effective implementation of the regulation. If these activities involve processing personal data, such as through inspection of AI test data, then they must respect confidentiality and protect the data in accordance with EU MDR Article 109 (Confidentiality) & 110 (Data Protection) and EU IVDR Article 102 (Confidentiality) & 103 (Data Protection). These articles refer to the Data Protection Directive 95/46/EC, which has now been superseded by the GDPR.

In the EU, the broad application of artificial intelligence techniques in medicine is currently hindered by limited dataset availability for algorithm training and validation, due to the absence of standardized electronic medical records, and strict requirements to protect patient privacy. As artificial intelligence thrives in the availability of big data, traditional principles of data protection, such as data minimisation and purpose limitation have an important drawback as they preclude some unexpected discoveries from combining data collected for different purposes. Repurposing data, not for profiling, but for research and statistical purposes, including by private companies for commercial purposes, is nevertheless admissible under the GDPR when appropriate safeguards are in place to protect the rights and freedoms of the data subject and for ensuring statistical confidentiality. Such safeguards should be determined through EU or Member State law. Such law may also provide derogations from the rights referred to in GDPR Articles 15 (right to access), 16 (right to erasure), 18 (right to restriction of processing) and 21 (right to object).

A difficult issue concerns whether access to the data sets of personal information supporting statistical inferences should be limited to the companies or public bodies (e.g. hospitals) who have collected the data. On the one hand, allowing, or even requiring, that the original controllers do not make the data accessible to third parties, may affect competition and prevent beneficial uses of the data. On the other hand, requiring the original controllers to make their data sets available to third parties would cause additional data protection risks. The Scientific Foresight Unit of the European Parliamentary Research Service concludes that repurposing data sets for scientific and statistical purposes, including by commercial companies, is possible under the GDPR, as long as the data is not used for profiling and appropriate precautions are in place preventing abusive uses of personal data. [74]

[70] *Note that it is important to calibrate the uncertainty. What you don't want is AI that gives the wrong answer and tells you that it is extremely confident in that wrong answer. See also: The need for uncertainty quantification in machine-assisted medical decision making. Nature Machine Intelligence. 7 January 2019.*

[71] *This requirement is similar to Article 8(h) of the draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), 4 April 2020, Committee on Legal Affairs, website European Parliament, accessed 8 May 2020. This draft regulation refers to "makes it possible [...] to revert to historical functionalities"*

[72] *Privacy safeguards inhibit storing of necessary data. For example, AI systems that provide video or audio recommendations are updated over time, changing in response to the availability of content and user reactions. The only way such systems could be precisely replicable over time would be if every interaction of every user was stored indefinitely, which would be unacceptable from a privacy point of view and also questionable from an environmental sustainability point of view.*

[73] *General Data Protection Regulation, Article 5, Official Journal of the European Union, 27 April 2016.*

[74] *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliamentary Research Service - Scientific Foresight Unit (EPRS - STOA). 25 June 2020*

Fortunately, technical solutions in healthcare to simultaneously address the demands for data protection and utilization for training and validation purposes can be achieved.[75] The bottleneck for European healthcare companies however remains access to data at scale. Datasets often stem from relatively few institutions, geographic regions or patient demographics, and might therefore contain unquantifiable bias due to their incompleteness with respect to co-variables such as comorbidities, ethnicity, gender and so on. **A European Health Data Space equipped with standardized electronic medical records and technical solutions to protect the privacy, in combination with EU or Member State derogations can help close the gap with non-European countries that offer normative environments that are more facilitative to the full development and deployment of AI systems.**

6.3. ELEMENTS OF TRUST REQUIRED BY EU MDR AND EU IVDR

6.3.1. PERFORMANCE

Thanks to its more reliable memory, rigorous reasoning and incredible speed, computers are in many ways superior to humans in terms of performance. Just consider how well electronic calculators are doing compared to human calculus or how consistently AI is performing in terms of pattern recognition in radiology and clinical diagnostics, not subject to fatigue as humans are (but perhaps less robust against noise and outliers not contained in the training datasets). In addition, some AI systems are trained using large numbers of examples and may detect subtle patterns in data that are not apprehensible to humans. Nevertheless, for many tasks AI does not yet reach human capabilities, notably because it currently lacks "common sense", i.e. the capability to apply abstract concepts, reason conceptually[76], use novel viewpoints, transfer knowledge to new domains or generalize knowledge by interpolating between known training examples or extrapolating beyond the space of known training examples. Consequently, some AI used today in for example radiology may have difficulty analyzing patterns in images from modalities that were not part of its training data set. Manufacturers must carefully identify and define such limitations and describe them in the device labeling, for example in the instructions for use.[77]

The EU MDR and EU IVDR requires manufacturers to describe in the instructions for use[78]**, if applicable, the intended purpose with a clear specification of indications, contra-indications, patient target group or groups, intended users and operating parameters and limitations**[79] **of their device.** If applicable, manufacturers must also include the performance characteristics[80], accuracy, precision and stability, the limits of accuracy[81] and the analytical performance[82]. From the perspective of describing performance there are similarities between an in vitro diagnostic device analyzing samples and a device analyzing data, in that software can be described, as applicable, in terms of analytical sensitivity, analytical specificity, trueness, precision, etc.[83]

[75] *For an overview of current and next-generation methods for federated, secure and privacy-preserving artificial intelligence for medical imaging applications, alongside potential attack vectors and future prospects in medical imaging and beyond see Secure, privacy-preserving and federated machine learning in medical imaging. G. Kaissis e.a., Nature Machine Intelligence, 8 June 2020.*

[76] *E.g., DeepMind's AlphaGo was trained using 5 million games to play the game of Go on a square board. It is unable to play Go on a rectangular board, even though for humans this would be very easy.*

[77] *Note that using the same training data will not necessarily yield models with the same precise output due to the nature of the techniques involved. For example, stochastic gradient descent (SGD) is one of the most elective and state-of-the-art techniques for machine learning and involves estimating objective function gradients on subsets of the training dataset. Some of these data subsets are created by random sampling, in order to reduce the computational burden and allow for faster iteration, which speeds up the learning process. Because the model's training is based on random subsets of the training data, it is not possible to guarantee that the same training data will lead to the same model output. More generally, the initial weights applied to different features within a neural network's architecture are chosen at random. These different starting points for a model's training can lead to models that perform slightly different, even if they were trained on the identical dataset.*

[78] *EU MDR GSPR 23.4 and EU IVDR GSPR 20.4 for the requirements pertaining the information in the instructions for use*

[79] *EU MDR & EU IVDR Annex I Chapter III Requirements regarding the information supplied with the device in EU MDR GSPR 23.1(g) or EU IVDR GSPR 20.1(g) Residual risks which are required to be communicated to the user and/or other person shall be included as limitations, contra-indications, precautions or warnings in the information supplied by the manufacturer, and GSPR 23.4(s) regarding Information in the instructions for use: information that allows the user and/or patient to be informed of any warnings, precautions, contra-indications, measures to be taken and limitations of use regarding the device. That information shall, where relevant, allow the user to brief the patient about any warnings, precautions, contra-indications, measures to be taken and limitations of use regarding the device. [...]*

[80] *EU MDR Annex I GSPR 23.4(e) and EU IVDR Annex I GSPR 20.4.1.(w)*

[81] *EU MDR Annex I GSPR 15.1 Diagnostic devices and devices with a measuring function, shall be designed and manufactured in such a way as to provide sufficient accuracy, precision and stability for their intended purpose, based on appropriate scientific and technical methods. The limits of accuracy shall be indicated by the manufacturer.*

[82] *EU IVDR Annex I GSPR 14.1 Devices having a primary analytical measuring function shall be designed and manufactured in such a way as to provide appropriate analytical performance in accordance with point (a) of Section 9.1 of Annex I, taking into account the intended purpose of the device.*
EU IVDR Annex I GSPR 20.4.1 (w) analytical performance characteristics, such as analytical sensitivity, analytical specificity, trueness (bias), precision (repeatability and reproducibility), accuracy (resulting from trueness and precision), limits of detection and measurement range, (information needed for the control of known relevant interferences, cross-reactions and limitations of the method), measuring range, linearity and information about the use of available reference measurement procedures and materials by the user; (x) clinical performance characteristics as defined in Section 9.1 of this Annex; (z) where relevant, clinical performance characteristics, such as threshold value, diagnostic sensitivity and diagnostic specificity, positive and negative predictive value;

[83] *EU IVDR 20.4.1(x) requires clinical performance characteristics to be provided in the instructions for use as defined in GSPR 9.1 [...] They shall achieve the performances, as stated by the manufacturer and in particular, where applicable: the analytical performance, such as, analytical sensitivity, analytical specificity, trueness (bias), precision (repeatability and reproducibility), accuracy (resulting from trueness and precision), limits of detection and quantitation, measuring range, linearity, cut-off, including determination of appropriate criteria for specimen collection and handling and control of known relevant endogenous and exogenous interference, cross-reactions; and the clinical performance, such as diagnostic sensitivity, diagnostic specificity, positive predictive value, negative predictive value, likelihood ratio, expected values in normal and affected populations.*

Not just the device performance and limitations must be described, the **Medical Device Regulations also require that a device achieves state-of-the-art[84] safety and performance[85] in terms of its intended use before a manufacturer can place it on the market.** It provides a clear framework on how this must be proven via risk management[86] and clinical evaluation[87]. Dedicated guidance for the clinical evaluation of software was published[88], drawing on the IMDRF guidance N41 Clinical Evaluation of Software as a Medical Device (SaMD)[89]. The principles described in this guidance are also suitable for AI-based software. Even when an AI reaches superhuman performance, state-of-the-art may continue to evolve. Diagnostic accuracy, patient outcomes, efficiency, and cost savings may continue to improve. As technology is continuously evolving, so is state-of- the-art. That is why **the regulations require manufacturers to perform Post-Market Clinical Follow-up and Post-Market Surveillance to ensure device safety and performance remains state-of-the-art during the lifetime of the device[90].**

Robustness is the ability of the system to maintain its level of performance under any circumstances[91] as described in its intended use and intended operating conditions. Manufacturers must ensure that the AI in a robust way achieves state-of-the-art safety and performance considering its intended use and within its operating parameters.[92][93]

6.3.2. MINIMIZE BIAS

From a scientific point of view, **bias is the tendency of a statistic to overestimate or underestimate a parameter[94]**. From a legal point of view, **bias is any prejudiced or partial personal or social perception of a person or group[95]**. It goes beyond the scope of this paper to discuss the differences between the scientific and legal definition; suffice to know that we attribute a broader meaning to the legal definition, mainly because the scientific definition generally is understood to refer to systematic estimation errors[96], whereas the legal definition can also apply to one-off errors in perception.

Aiming for software to be unbiased is desirable. Zero bias is however impossible to achieve. Bias may enter the AI development chain at different stages (see Figure 6). We humans all have our blind spots. Any data set that relies on humans taking decisions will therefore have some form of bias. Every hospital is different, every country is different, and every patient is different. You can never achieve zero bias when extrapolating. In the medical world, clinical investigations of devices for adults have historically underrepresented women, minority racial or ethnic groups, and to some extent also patients over age 65[97]. AI can maintain or even amplify such bias through its decisions, or in trying to optimize its function it might ignore a minority if the minority looks different from the general population, in order to optimize for the general population.

[84] *State of the art refers to the developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience. The state of the art embodies what is currently and generally accepted as good practice in technology and medicine. The state of the art does not necessarily imply the most technologically advanced solution. The state of the art described here is sometimes referred to as the "generally acknowledged state of the art". Source: IEC Guide 63:2019, 3.18*

[85] *EU MDR Annex I for the general safety and performance requirements applicable to devices. Article 2 (52) MDR defines clinical performance as the ability of a device, resulting fro or indirect medical effects which stem from its technical or functional characteristics, including diagnostic characteristics, to achieve its intended purpose as claimed by the manufacturer, thereby leading to a clinical benefit for patients, when used as intended by the manufacturer; whereas Article 2 (41) of EU IVDR defines clinical performance as the ability of a device to yield results that are correlated with a particular clinical condition or a physiological or pathological process or state in accordance with the target population and intended user. Source: EU 2017/745 (MDR), Article 2 (52); EU 2017/746 (IVDR), Article 2 (41)*

[86] *EU MDR and EU IVDR Annex I GSPR 3 for the risk management system requirements*

[87] *EU MDR Chapter VI Clinical Evaluation and Clinical Investigations, Annex XIV Clinical Evaluation and Post-Market Clinical Follow-up and Annex XV Clinical Investigations. See EU IVDR Chapter VI Clinical Evidence, Performance Evaluation and Performance Studies, Annex XIII Performance Evaluation, Performance Studies and Post-Market Performance Follow-up, Chapter XIV Interventional Clinical Performance Studies and certain other Performance Studies.*

[88] *MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software, 17 March 2020.*

[89] *IMDRF N41: Clinical Evaluation of Software as a Medical Device (SaMD), published 2017-11-21*

[90] *EU MDR Chapter VII Post-Market Surveillance, Vigilance and Market Surveillance, Annex XIV Clinical Evaluation and Post-Market Clinical Follow-up. See EU IVDR Chapter VII Post-Market Surveillance Vigilance and Market Surveillance and Annex XIII Performance Evaluation, Performance Studies and Post-Market Performance Follow-up.*

[91] *Draft IEC 22989 - Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology, published 2019-10-31. An AI system can behave as expected within a certain range of acceptable outputs. Even if the output is not ideal, but still falls within an acceptable range of variations, then the system should still be considered robust. Outside of this range, the system would not be robust any more.*

[92] *Typical examples for robustness goals are:*
meet one or more thresholds over a set of statistical metrics that need to hold on some evaluation data invariance of performance against certain types of data perturbations invariance of performance against systematic changes of input data (e.g. drift, change of operating scenario) stability of training results under small variations of the training set, given the stochastic nature of many machine learning algorithms consistent system output for similar input data, e.g. resistance to so-called adversarial examples

[93] *Robustness of AI that changes itself during use often depends on the robustness of the network or information system used to provide the data for learning. European Union Directive 2016/1148 "Concerning measures for a high common level of security of network and information systems", brings in legislation "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems".*

[94] *A statistic and a parameter are very similar. They are both descriptions of groups. The difference between a statistic and a parameter is that statistics describe a sample. A parameter describes an entire population. A statistic is biased if it is calculated in such a way that it is systematically different from the population parameter being estimated.*

[95] *Article 4 (m) of draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), 4 April 2020, Committee on Legal Affairs, website European Parliament, accessed 8 May 2020.*

[96] *The scientific definition of bias uses the words "tendency" and "statistic", which alludes to there being a systematic nature.*

[97] *Women, because it is harder to find a woman that is not childbearing to participate in clinical investigations; minority racial or ethnic groups because it is harder to find enough people of that subgroup, elderly, because it sometimes carries more risks to include them. Diversity in Medical Device Clinical Trials: Do We Know What Works for Which Patients? Fox-Rawlings SR, Gottschalk LB, Doamekpor LA, Zuckerman DM., Milbank Q. 2018;96(3):499–529. doi:10.1111/1468-0009.12344.*

The EU MDR and EU IVDR requires manufacturers to minimize bias[98]. For manufacturers to establish that bias is minimized, they need to assess the AI for bias and ensure bias has been minimized if considered harmful. They can for example compare the software output against an independent reference standard (e.g. a ground truth, biopsy, or expert consensus), or they can perform certain sanity tests in terms of accuracy on every group that they can efficiently identify from the data[99]. The challenge is for computer scientists to get an accurate picture of which group(s) could be potentially subject to bias. The difference might not show up in aggregate, but only when focusing on a sub-population within that group, where no test can exhaustively cover the space of all permutations.

A big challenge to address bias is that enough and complete data must be available, which is rarely possible under GDPR, causing the tradeoff between fairness and accuracy (see Chapter 5). Also, testing AI for non-discrimination on an ethical basis is at odds with GDPR and poses risks to users' privacy. Under current GDPR requirements, developers should not be able to access attributes such as ethnicity and therefore could not test for ethnic representation in a dataset.

- **COCIR recommends** updating IEC 82304-1 by requiring manufacturers to assess AI for bias and if bias is found and considered harmful, to minimize the bias.
- **COCIR recommends** updating IEC 82304-1 by requiring manufacturers to add to the limitations or contraindications to the use by any minority group that can potentially be subject to a risk of significant bias.

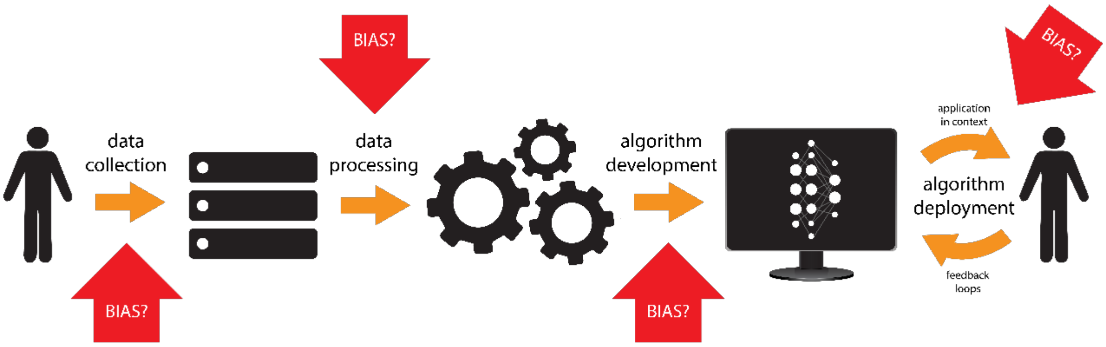


Figure 6 *Bias entry points in the AI development chain. Bias can creep in at different stages of AI development: during (1) data collection, (2) data processing operations such as cleaning, enrichment and aggregation or through assumptions in the design of data processing pipelines, (3) human judgement about the model construction and evaluation metrics can introduce biases in the processes of algorithm development and testing and (5) through context changes or user interaction.*

The other way around, software can play an important role in identifying and minimizing bias. This is not specific to artificial intelligence, but to software in general. Historically it was hard to prove unintended discriminatory bias based on e.g. race. Software can enable feedback loops that make it easier to detect and fix bias issues. **The European Health Data Space can capitalize on this** by breaking down health data silos[100] into a single virtual electronic health record and allowing secondary use to detect bias, including in AI-based medical devices. The latter would require health service providers to store not just the output, but also the use of a medical device in the patient's electronic health record, as some member states have indicated will be required on their territory[101]. Health service providers can record the use of a medical device via the device's Unique Device Identifier (UDI). Allowing manufacturers to use this anonymized data to fulfill their post-market surveillance responsibilities would enable the healthcare domain to minimize bias in the most effective way.

98. *Requirements regarding bias:*
EU MDR Annex XV Chapter II Clinical Investigations 3.6.4 Details of measures to be taken to minimise bias, such as randomisation, and management of potential confounding factors.
EU IVDR Annex I GSPR 9.1 [...] Devices [...] shall achieve the performances, as stated by the manufacturer and in particular, where applicable: [...] trueness (bias)
EU IVDR Annex XIII 2.3.1. Clinical performance studies shall be designed in such a way as to maximize the relevance of the data while minimising potential bias.
EU IVDR Annex XIII 2.3.2 The clinical performance study plan shall contain in particular [...] description of and justification for the design of the clinical performance study, its scientific robustness and validity, including the statistical design, and details of measures to be taken to minimise bias, such as randomisation, and management of potential confounding factors;

99. *Multicalibration: Calibration for the (Computationally-Identifiable) Masses," by Úrsula Hébert-Johnson, Michael P. Kim, Omer Reingold, Guy N. Rothblum; https://arxiv.org/abs/1711.08513*

100. *The ERN database is an example of a patient registry on rare diseases. It aims to serve as a blueprint to connect patient registries and databases so they provide cross-border interoperability. European Commission website. Accessed 25 May 2020. GAIA-X is another initiative to stimulate cloud federation from the German perspective, presented by the German government on 29 October 2019. The purpose of the project is to cater for European standards and reference architectures to create EU-based 'virtual hyperscale providers'. Federal Ministry of Economic Affairs and Energy Website. Accessed 25 May 2020.*

101. *CELEX: 32017R0745 Czech Republic's draft national EU MDR law indicates that health service providers must record the use of a class IIb or III device in the patient's medical records. That this must be recorded via the Unique Device Identifier has not been specified in the draft national law.*

Obviously, to avoid label bias[102], health service providers would also need to apply Good Data Management Practices (GDMP)[103], otherwise the dataset will not be representative of reality.

- Because it is **impossible** to develop AI with zero bias, COCIR recommends possible future legislative initiatives to align with EU MDR/IVDR by requiring manufacturers to "minimize bias" rather than to obtain "zero bias".

6.3.3. REPEATABILITY

The EU MDR and EU IVDR require the repeatability of devices that incorporate electronic programmable systems, devices that include software or software that are devices in themselves[104]. This requirement has its roots in Council Directive 93/42/EEC[105], where it only applied to electronic programmable systems, rather than to devices that include software or software that are devices in themselves.

Repeatability can be defined as "the degree to which the software output and performance under the same conditions produces results that can be accepted as being identical". This implies that a manufacturer must determine the degree of repeatability expected for the intended purpose of their devices, i.e. what the minimum performance must be in light of the intended purpose and state-of-the-art and in relation to that define the related change boundaries accordingly[106][107].

Note that the EU Committee on Legal Affairs[108] proposes AI operations to be "reproducible"[109], rather than "repeatable". This provides for more flexibility in terms of implementation, e.g. it allows for the AI to be rolled back to a previously stored state or another AI instance to be used to reproduce the operation.

Many devices have a performance that is subject to change, e.g., a Computed Tomography (CT) machine used to visualize the same object a thousand times is subject to wear and tear and to fluctuations in environmental conditions. It will never run exactly the same, but still, when using the same acquisition parameters a user will generally consider the output identical, even across large time spans, because the machine will have been calibrated regularly to keep its performance on a minimum performance level established by the manufacturer so as to keep output identical in light of the intended purpose of the device and considering state-of-the-art.

Similarly, whereas computer programs generally excel at repetitive behavior, certain AI (e.g. probabilistic AI, soft computing and fuzzy logic), in order to cope with very noisy input data, will employ an execution flow that is non-deterministic, but will nevertheless each time reach a deterministic answer. For example, you can run the program a hundred times, it will never run the same way twice, but it will (should) consistently produce the same average result. It has inherent variability to tolerate imprecision, uncertainty and partial truth in real world data to solve complex problems while achieving tractability,

[102] *Label bias is inaccuracy in the data labels*

[103] *GDMP aim for data privacy, confidentiality and protection and for data to be useful for training and performance evaluation. Typical activities include:*
Data selection:
Identify the data attributes and the amount of data that is needed. Apply the principle of data economy so that only data that is needed is eventually collected.
Identify the data sources. Consider if data should be collected from various locations (pooling data from various locations, possibly spanning different countries and continents, possibly applying a federated learning approach).
Data anonymization/pseudonymization
Data cleaning
Detect and correct any corrupt data
In case of data pooling/federated learning, when data are gathered from different sources and combined, additional considerations apply, for example to avoid unintended duplicate data sets and as such risk introducing bias
Data labeling – so data can be pooled without loss of meaning
Relevant standards: ISO/IEC 25024 "Measurement of data quality" and ISO/IEC 25012 "Data quality model"

[104] *EU MDR Annex I GSPR 17.1 and EU IVDR Annex I GSPR 16.1: Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.*

[105] *Council Directive 93/42/EEC essential requirement 12.1 for the requirement on repeatability*

[106] *The software should for example provide the same result for multiple scans of the same patient acquired by the same user, with a degree of agreement corresponding to Kappa coefficient > 0,9.*

[107] *In practice, it is often difficult to describe precisely the limitations and level of accuracy to be expected under different conditions in lay terms. However, research has shown it is helpful for an AI application's performance to be contextualized by presenting it alongside existing human performance statistics, as well as giving concrete examples of successful and unsuccessful use cases, particularly any challenging edge-cases for humans or known pitfalls which the system has been explicitly designed to overcome. See: "Hello AI": Uncovering the Onboarding Needs of Medical Practitioners for Human-AI Collaborative Decision-Making (Nov 2019); hps://dl.acm.org/doi/10.1145/3359206*

[108] *Draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)), 4 April 2020, Committee on Legal Affairs, website European Parliament, accessed 8 May 2020. See Article 8(d).*

[109] *AQA Science. A measurement is reproducible if the investigation is repeated by another person, or by using different equipment or techniques, and the same results are obtained. N.B. "the same" results implies identical, but in reality "the same" means that random error will still be present in the results. https://www.gcse.com/science/reproducible.htm. Accessed February 1, 2021.*

robustness and low cost[110]. As such probabilistic or stochastic locked models provide output that converges to a single, fixed average value[111],[112] (e.g., Monte Carlo simulations used for weather forecasting or to determine drug dose response portions).

Also, AI may use differential privacy, a technique that carefully injects random noise to protect individual privacy. The goal of such systems is to protect privacy by making it impossible to reverse engineer the precise inputs used, while still delivering an output that's close enough to the accurate answer.

AI can also change through learning during runtime and as such make it subject to variation. Manufacturers that utilize machine-learning capabilities to adapt precision medicine software to a specific patient or health institution, can employ data validation pipelines, calibration or acceptance tests to ensure that variation remains within safety and performance specifications, before applying a new AI model learned on the data of a specific patient or health institution. For example, when AI is used to measure a parameter, the manufacturer must determine the accuracy and precision of the measurement function. Whereas accuracy refers to the trueness, the proximity of the measurement results to the true value, precision refers to the repeatability or reproducibility of a measurement. Through a literature study, manufacturers must determine the accuracy and precision required for the intended purpose in consideration of state-of-the art and then establish via technical and scientific means whether their device meets that accuracy and precision.

- **COCIR recommends** updating IEC 82304-1:2016[113] by requiring manufacturers to inform the user of the performance characteristics of their AI-based device needed to discern the degree to which the software output and performance under the intended use conditions produces identical results, for example by communicating its precision, sensitivity, specificity, confidence, operating parameters...
- **COCIR recommends** manufacturers of AI that changes through learning to consider a design capable of storing discrete states of a learned model and capable of returning to a previously stored state in order to reproduce results.

6.3.4. RELIABILITY

The EU MDR and IVDR[114] require the reliability of devices that incorporate electronic programmable systems. These are devices that include software or that are software devices in themselves. This requirement has its roots in Council Directive 93/42/EEC[115], where it applied to electronic programmable systems, rather than to devices that include software or software that are devices in themselves.

The origin being related to electronic programmable systems and the General Safety and Performance Requirements[116] (GSPR) considering reliability and performance as two separate terms, reveals that the term "reliability" must be understood as robustness in the meaning of "not breaking", "not crashing", rather than as "credibility" or "performance"[117], a topic discussed elsewhere in this paper. **Reliability in this context is understood as "the ability of a system or an entity within that system to perform its required functions under stated conditions for a specific period of time"**[118] or in the words of the European Commission's High-Level Expert Group on AI: "working properly with a range of inputs and in

[110] *Soft computing and fuzzy logic, L.A. Zadeh, IEEE Software, 935 1994, vol. 11, issue 6*

[111] *Wikipedia, Convergence of Random Variables, https://en.wikipedia.org/wiki/Convergence_of_random_variables, accessed February 1, 2021*

[112] *Wikipedia, Law of Large Numbers, https://en.wikipedia.org/wiki/Law_of_large_numbers, accessed February 1, 2021*

[113] *IEC 82304-1:2016 Health Software – Part 1: General requirements for product safety.*

[114] *EU MDR Annex I GSPR 17.1 and EU IVDR Annex I GSPR 16.1: Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.*

[115] *Council Directive 93/42/EEC essential requirement 12.1 for the essential requirement on reliability*

[116] *EU MDR Annex I GSPR 17.1 and EU IVDR Annex I GSPR 16.1: Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.*

[117] *The term performance is reference on numerous locations in the Medical Device Regulations, e.g. EU MDR Annex I GSPR 1 and EU IVDR Annex I GSPR 1: Devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose. They shall be safe and effective and shall not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, taking into account the generally acknowledged state of the art.*

[118] *IEC 27040:2015 Information technology — Security techniques — Storage security. A similar definition is provided by ISO/TS 14907-1:2015 Electronic fee collection — Test procedures for user and fixed equipment — Part 1: Description of test procedures : reliability is the ability of a device or a system to perform its intended function under given conditions of use for a specified period of time or number of cycles*

a range of situations"[119]; in the healthcare domain this becomes "working properly for a range of patients for a range of clinical conditions", i.e. *clinical performance*.

To test the reliability of devices, manufacturers apply a battery of test techniques, as defined through IEC 62304[120], IEC 82304-1[121] and the IEC 60601 series[122].

6.3.5. SAFETY

EU MDR and EU IVDR require manufacturers to establish, implement, document and maintain a risk management system[123]. **This system must be a continuous iterative process throughout the entire lifecycle of a device.** Devices must be safe and not compromise the clinical condition or the safety of patients, or the safety and health of users, or other persons, where applicable. Any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, **taking into account the generally acknowledged state of the art**.[124]

The EU MDR and EU IVDR contain a long list of General Safety and Performance Requirements (GSPR). Many of these requirements address risks that related to hardware, e.g. risks related to electricity, biocompatibility, sterility, etc. Some requirements also address software risks.

One such requirement stipulates that "devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, [...] **adopt appropriate means to reduce as far as possible consequent (A) risks or (B) impairment of performance** [...] **in the event of a single fault condition**"[125]. **A single fault condition is a "condition in which a single means for reducing a risk is defective or a single abnormal condition is present"**.[126] Note that this requirement does not stipulate that the fault must be fixed, but that appropriate means must be adopted to reduce the risk as far as possible or avoid impairment of performance. Performance is understood as essential performance, i.e. the performance of the clinical function(s) of the device[127]. Single fault conditions in other words must not cause or contribute to the loss or degradation of a clinical function that results in unacceptable risk. For example, an AI-based ventilator for life support must guarantee the life-support function including in case of a single fault condition, for example when earth leakage current occurs, or tubing disconnects.

To meet this requirement, medical device manufacturers generally use ISO 14971:2019[128]. This standard requires them to manage hazards in both normal and fault conditions, including **single fault conditions**. The standard requires risks to be reduced as low as possible and the benefits to outweigh the performance for the risks to be acceptable. Concretely, to meet the single fault requirement manufacturers:

A Identify essential performance and assure that it meets state-of-the-art[129] in light of the intended use.

B Specify performance limits between fully functional and total loss of the identified performance in both normal conditions and single fault conditions

C Evaluate risk of loss or degradation of the identified essential performance beyond the specified limits (where the resulting risk is unacceptable)

[119] *Ethics Guidelines for Trustworthy AI, High-Level Expert Group on Artificial Intelligence, 8 April 2019, European Commission website, accessed 6 May 2020*
[120] *IEC 62304:2006/A1:2015 Medical Device Software – Software lifecycle processes.*
[121] *IEC 82304-1:2016 Health Software – Part 1: General requirements for product safety.*
[122] *IEC 60601 is a series of technical standards for the safety and essential performance of medical electrical equipment.*
[123] *EU MDR and EU IVDR Annex I GSPR 3 for the risk management system requirements*
[124] *EU MDR and EU IVDR Annex I GSPR 1*
[125] *EU MDR Annex I GSPR 17.1 and EU IVDR Annex I GSPR 16.1 Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance. EU MDR Annex I GSPR 18.1 For non-implantable active devices, in the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks. . The regulations also mentions the term single fault condition in relation to fire and explosion (EU MDR Annex I GSPR 14.3 and EU IVDR Annex I GSPR 13.3) and electric shocks (EU MDR Annex I GSPR 18.7 and EU IVDR Annex I GSPR 17.5) and energy sources (EU IVDR Annex I GSPR 17.1)*
[126] *Single fault condition is defined in IEC 60601-1, section 3.116*
[127] *IEC 60601-1:2015, third edition including Amendments 1:2012 and 2:2020 Medical electrical equipment. Part 1: General requirements for basic safety and essential performance: essential performance is performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk*
[128] *ISO 14971:2019 Medical devices: application of risk management to medical devices*
[129] *EU MDR Annex I GSPR 23.4 (e) and EU IVDR Annex I GSPR 20.4.1 (w) define that the performance characteristics must be defined in the instructions for use. EU MDR and EU IVDR Annex I GSPR 1 "Devices shall achieve the performance intended by their manufacturer [...] into account the generally acknowledged state of the art."*

D Implement risk control measures to reduce these risks to an acceptable level for both normal conditions and single fault conditions (see Figure 7)

E Specify methods for the verification of the risk control measures effectiveness; and

F Asses which risk control measures need verification of effectiveness and perform functional tests.

Manufacturers perform and document activities (A) – (F) in their risk management file and test evidence so their Notified Body can carefully examine and scrutinize the evidence to confirm its validity and objectiveness.

Note that an AI making a wrong prediction (such as a false positive or false negative result) is not considered as a fault condition as long as this falls within the expected performance range (within expected diagnostic sensitivity and specificity in light of state of the art). AI drifting out of specification on the other hand, for example because Good Data Management Practices were not followed by the health institution, is considered a fault condition. It requires appropriate means to reduce as far as possible the consequences of that drift, for example by rolling back the algorithm to a previous state or performing a partial reset.

The EU MDR and EU IVDR also contain various requirements to **reduce as far as possible the risks brought by the IT environment**[130]**, including the loss of connectivity**, also a risk highlighted by the EU White paper on AI. This risk can for example be handled by a watchdog timer.[131]

[130] *Annex I GSPR 14.2 & EU MDR Annex I GSPR 13.2: Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible: [...] the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts; EU MDR Annex I GSPR 17.3 & EU IVDR Annex I GSPR 16.3 Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).*

[131] *A watchdog timer is an electronic timer that is used to detect and recover from computer malfunctions such as loss of connectivity. During normal operation, the software regularly resets the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the computer fails to reset the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to adopt actions to reduce consequent risks, for example by placing the system in a safe state and restoring normal system operation.*

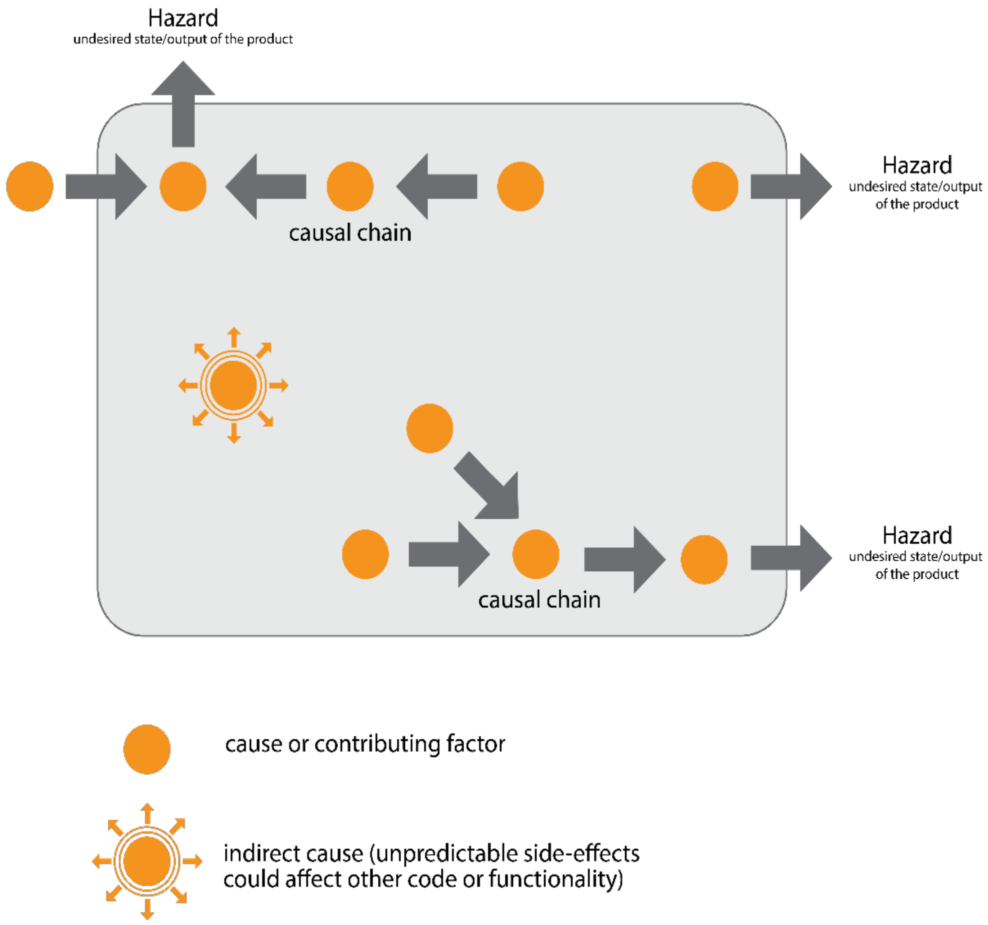

Hazard
undesired state/output of the product
causal chain
Hazard
undesired state/output of the product
Hazard
undesired state/output of the product
causal chain
● cause or contributing factor
indirect cause (unpredictable side-effects could affect other code or functionality)

Figure 7 *Risk control can occur at different locations along the causal chain. Generally it is best to implement risk control measures on the data input side of the software to limit the number of combinations of permutations of potential causes that can lead to hazards. The data input side is especially relevant to the prevention of use of erroneous information that could subsequently lead to a hazard. For example, an algorithm may be correct and work properly in determining a test result. If, however, various raw data acquired through sensors is faulty or parameters or options are input improperly the result could still be wrong. Examples of risk controls at the input side of the grey box would be consistency, fault, or range checks on sensor information or user interfaces error checks on operator entered information (which is not to say that all possible operator errors could be detected). Data validation checks on the data output side provide a safety net should some potential causes for hazards be missed or if identified but their corresponding risk control measures are not foolproof. If there is an adequate risk control measure at the end of the chain that prevents the hazardous output, then a manufacturer may not need to provide separate risk control for the individual causes in the chain. In some cases data output side risk controls are more effective and in others input side measures are. In many cases manufacturers need combinations of input, output, and intermediate risk control measures but this depends on the specific intended use and technical system and software design constraints. When defining risk controls it is important manufacturers recognize that risk control measures can add complexity. In such cases "more" risk control functionality could result in more defects and it is important manufacturers keep this in mind. When manufacturers identify risk control measures for indirect causes it is generally unproductive to attempt to trace every possible hazardous event from each indirect cause failure to each potential hazard. For indirect causes it is generally better to identify types of indirect causes and then identify detection mechanisms and risk controls for each to minimize risk should they occur, e.g. check sums to detect data corruption of critical data and safe shutdown or user notification of such events.*

The EU White Paper on AI recommends establishing obligations for manufacturers to **control mental safety risks** of human-AI interactions; the JURI report also adds **emotional risks**. Take as an example a personal assistant hearing the user say "Alexa, today I am going to kill myself". The intent is that such products can distinguish from context and voice intonation when the user is making a joke versus when the user has suicidal thoughts and control that these thoughts spiral the user downwards in its mental state. Note also that various software applications exist for treating mental disorders, such as apps for substance abuse and virtual reality applications for treatment of various phobias.

Emotional harm can also arise with medical devices, such as physiological stress after a false-positive. Whereas the EU MDR and EU IVDR talk about risks in general and do not explicitly refer to mental and emotional risks, such risks can be considered in scope of the regulation. For the practical implementation of a risk management system many manufacturers still rely on ISO 14971:2012, a standard cited in the Official Journal of the European Union for the Medical

Device Directives. Contrary to the more recent 2019 edition, the 2012 release of the standard does not require mental or emotional harm to be controlled.[132] From that perspective the Commission should send a clear signal to manufacturers by citing ISO 14971:2019 in the Official Journal of the European Union.

- The EU White Paper on AI suggests mental risks to be controlled. The EU MDR and EU IVDR require mental risks to be controlled, both in terms of risk-related usability as well as in terms of clinical performance and safety. In practice many manufacturers rely on EN ISO 14971:2012, a standard cited in the Official Journal of the European Union for the Medical Device Directives. This version of the standard does not cover mental risks. COCIR therefore recommends harmonization for EU MDR and EU IVDR of the new version, i.e. ISO 14971:2019 Medical devices: application of risk management to medical devices

6.3.6. ELIMINATE OR REDUCE RISK OF USE ERROR

Manufacturers of AI-based devices sometimes require a human in the loop to take control when the AI is less confident of its decision. Human behaviour however comes with its own risks. E.g., a level 2 self-driving car[133] requires a human in the loop to drive the car safely. It might take 100.000 km before the car has an accident; the human may by then have put too much confidence (overtrust and automation bias[134]) in the car and no longer pay enough attention to take back control of the car in a timely and safe manner.

In a perfect world, we would like users that trust AI when it works at 100% accuracy, but be hypersensitive, and be able to identify when it is not. In reality, people often tend to sway. If the first impression is positive, humans tend to not see when the AI makes mistakes, forget or forgive that it makes mistakes. How we must design our devices allowing users to calibrate their trust appropriately and how we must educate them in their first interactions with the device is an open field of research.

The medical domain can inspire. For example, a radiology study showed that the accuracy of the human-device combination may improve when a Computer-Aided-Detection algorithm identifies more than one choice to the radiologist[135]. Offering multiple options can maintain trust in the system and mitigate the risks of overtrust by putting the human expertise at work.

In other cases, the performance of the AI might be better than the performance of the human-AI team. **Sometimes it is necessary to take the human out of the loop altogether to get the best performance and reduce or eliminate use error.** For example, in a clinical diagnostic application used to read quantitative Polymerase Chain Reaction (qPRC) assays the regulator requires manufacturers to deactivate the possibility for the molecular biologist to intervene, because the precision and reliability of the AI outperforms that of the human-AI team. [136] Taking the human out of the loop takes away human variability and mitigates the risk of a lab using less control samples than required by the assay manufacturer. On the other hand, when AI is trained on rare diseases with fewer datasets, it may require the human to be in the loop to reach maximum performance. Striking the right balance is important and differs case by case. **The EU MDR and EU IVDR require manufacturers to eliminate or reduce the risk of use error.**[137] Inappropriate levels of trust in automation may cause suboptimal performance.[138]

[132] *ISO 14971:2012 Medical devices: application of risk management to medical devices focusses on physical harm. ISO 14971:2019 removed the word "physical" from the harm definition so that it also includes mental harm. The new definition reads: "harm: injury or damage to the health of people, or damage to property or the environment."*

[133] *Wikipedia, accessed February 2, 2020: Level 2 ("hands off"): The automated system takes full control of the vehicle: accelerating, braking, and steering. The driver must monitor the driving and be prepared to intervene immediately at any time if the automated system fails to respond properly. The shorthand "hands off" is not meant to be taken literally – contact between hand and wheel is often mandatory during level 2 driving, to confirm that the driver is ready to intervene.*

[134] *Overtrust is a form of risk compensation (Wikipedia, accessed 22 June 2020) and automation bias. K. Goddard, A. Roudsari and J. Wyatt, Automation bias: a systematic review of frequency, effect mediators, and mitigators, Journal of the American Medical Informatics Association, 19 (1) p121–127, 2012.*

[135] *Improving the radiologist-CAD interaction: Designing for appropriate trust. Jorritsma, W. & Cnossen, Fokie & Van Ooijen, Peter. (2014). Clinical Radiology. 70. 10.1016/j.crad.2014.09.017.*

[136] *The US FDA obliged the manufacturer to remove the human from the loop. K. Cobbaert (personal communication, February 17, 2020)*

[137] *EU MDR & EU IVDR Annex I GSPR 5: In eliminating or reducing risks related to use error, the manufacturer shall:*
(a) *reduce as far as possible the risks related to the ergonomic features of the device and the environment in which the device is intended to be used (design for patient safety), and*
(b) *give consideration to the technical knowledge, experience, education, training and use environment, where applicable, and the medical and physical conditions of intended users (design for lay, professional, disabled or other users).*

[138] *Other factors impact the safety and performance of human-AI teams. See "Ten challenges for making automation a 'team player' in joint human-agent activity", Klein et al., IEEE Computer Nov/Dec 2004.*

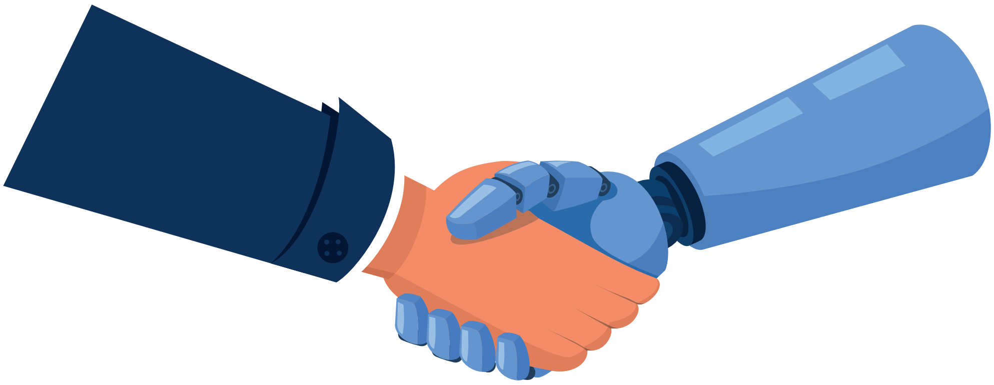
- **COCIR recommends** citing IEC 62366-1:2015+AMD1 Medical devices – Part 1: Application of usability engineering to medical devices in the Official Journal of the European Union for EU MDR and EU IVDR to give manufacturers a clear signal to identify and control inappropriate levels of user trust

6.3.7. SECURITY

EU MDR and EU IVDR require manufacturers to establish, implement, document and maintain a risk management system[139], including for security and cybersecurity risks. This system must be a continuous iterative process throughout the entire lifecycle of a device. In addition, the regulation requires manufacturers to control the risks related to the IT environment[140] and single fault conditions. This implies, among others, that manufacturers must mitigate the impact of security vulnerabilities in the host platform, in the operating system or in the network and to ensure their AI devices are resilient against attacks and manipulation.

The regulations also require manufacturers to define minimum requirements against unauthorized access and to protect their devices as far as possible against unauthorized access that could hamper the device from functioning as intended.[141] It also requires manufacturers to specify hardware, IT network characteristics and IT security measures and to inform the users via the instructions for use how to protect against unauthorized access.[142]

Of course, **security is a responsibility shared between manufacturer, integrator and operator[143]**. A manufacturer may deliver a secure device to a hospital, if the integrator deactivates its application hardening by reconfiguring it or if the operator allows department wide passwords, it will be used in an insecure way.



[139] *EU MDR and EU IVDR Annex I GSPR 3 for the risk management system requirements and EU MDR GSPR 17.2 & EU IVDR GSPR 16.2 for devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.*

[140] *EU MDR Annex I GSPR 14.2(d) and EU IVDR Annex I GSPR 13.2(d) [Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible] the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;*

[141] *EU MDR GSPR 17.2 & EU IVDR GSPR 16.2 For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.*

[142] *EU MDR GSPR 17.4 & EU IVDR GSPR 16.4 Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended.*

[143] *MDCG 2019-16 Guidance on Cybersecurity for medical devices. December 2019.*

7. COMPLIANCE AND ENFORCEMENT UNDER EU MDR AND EU IVDR

This section is intended for readers not familiar with Regulation (EU) 2017/745 on medical devices and Regulation (EU) 2017/746 on in-vitro diagnostic medical devices. It outlines in a nutshell the main elements that ensure AI-based devices are both safe and effective, both through ex ante and ex poste measures.

7.1. RISK-BASED

The Medical Device Regulations classify devices by means of risk-based classification rules. The EU MDR contains twenty-two classification rules; the EU IVDR contains seven, supported by implementing rules and definitions.

Classification leads to a regulatory class. The EU MDR distinguishes class I, IIa, IIb and III while the EU IVDR uses letters: class A, B, C and D. In addition, EU MDR distinguishes class I devices that contain a measuring function, are reusable surgical instruments or are sterile, whereas EU IVDR distinguishes sterile devices. The higher the risk, the higher the class and the more scrutiny is applied (see Figure 8).

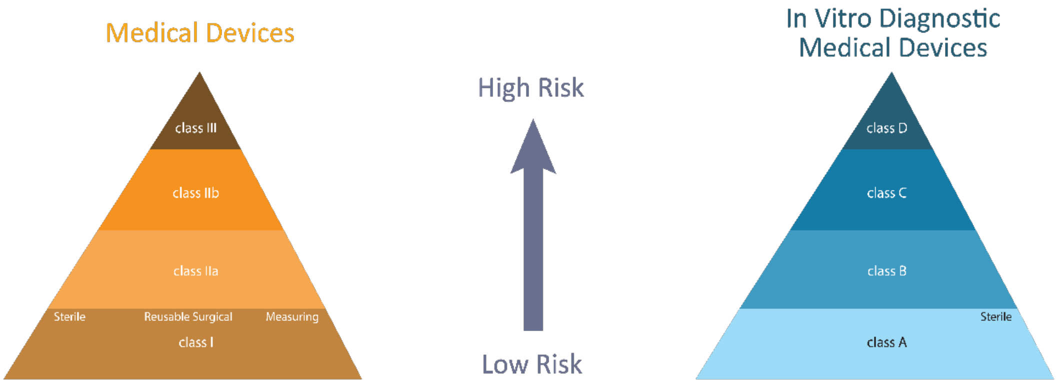
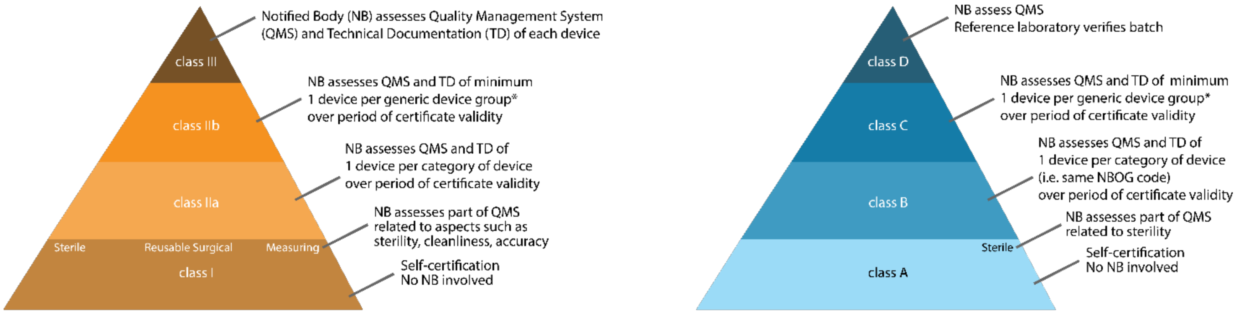


Figure 8 *Generally, the riskier the device, the higher the class.*

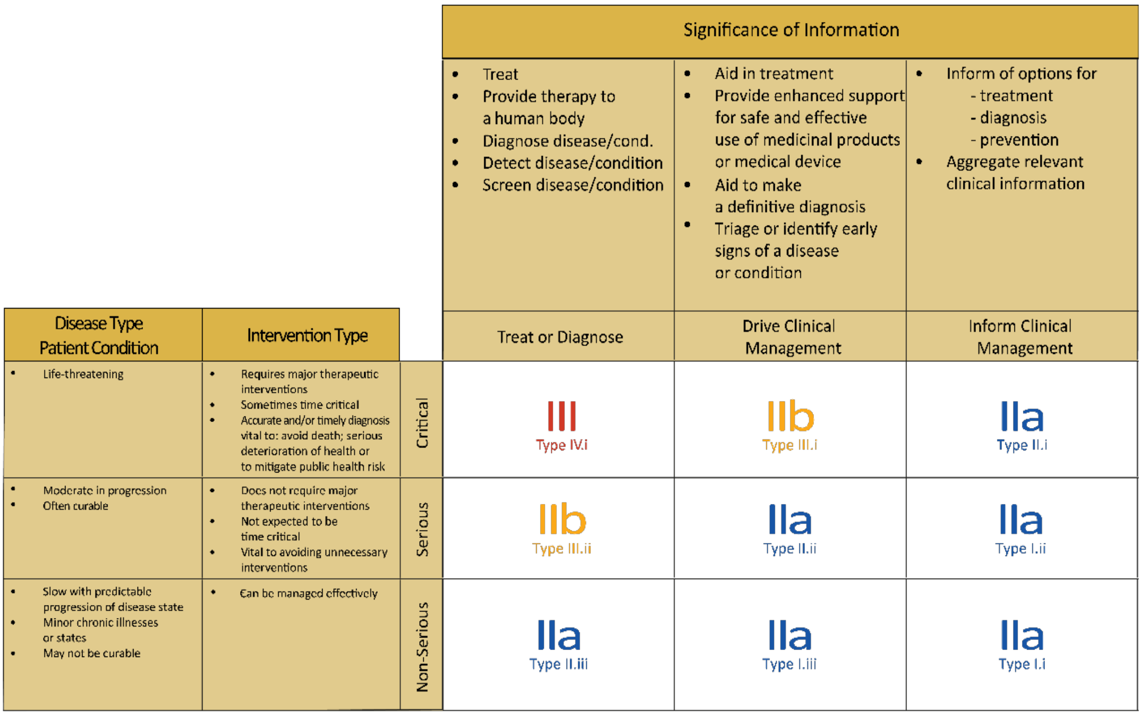

class III
Notified Body (NB) assesses Quality Management System (QMS) and Technical Documentation (TD) of each device
class IIb
NB assesses QMS and TD of minimum 1 device per generic device group* over period of certificate validity
class IIa
NB assesses QMS and TD of 1 device per category of device over period of certificate validity
Sterile
Reusable Surgical
Measuring
class I
NB assesses part of QMS related to aspects such as sterility, cleanliness, accuracy
Self-certification No NB involved
class D
NB assess QMS Reference laboratory verifies batch
class C
NB assesses QMS and TD of minimum 1 device per generic device group* over period of certificate validity
class B
NB assesses QMS and TD of 1 device per category of device (i.e. same NBOG code) over period of certificate validity
Sterile
NB assesses part of QMS related to sterility
class A
Self-certification No NB involved

*generic device group: a set of devices having the same or similar intended purposes or a commonality of technology allowing them to be classified in a generic manner not reflecting specific characteristics

Figure 9 *Higher-class devices are subject to more scrutiny.*

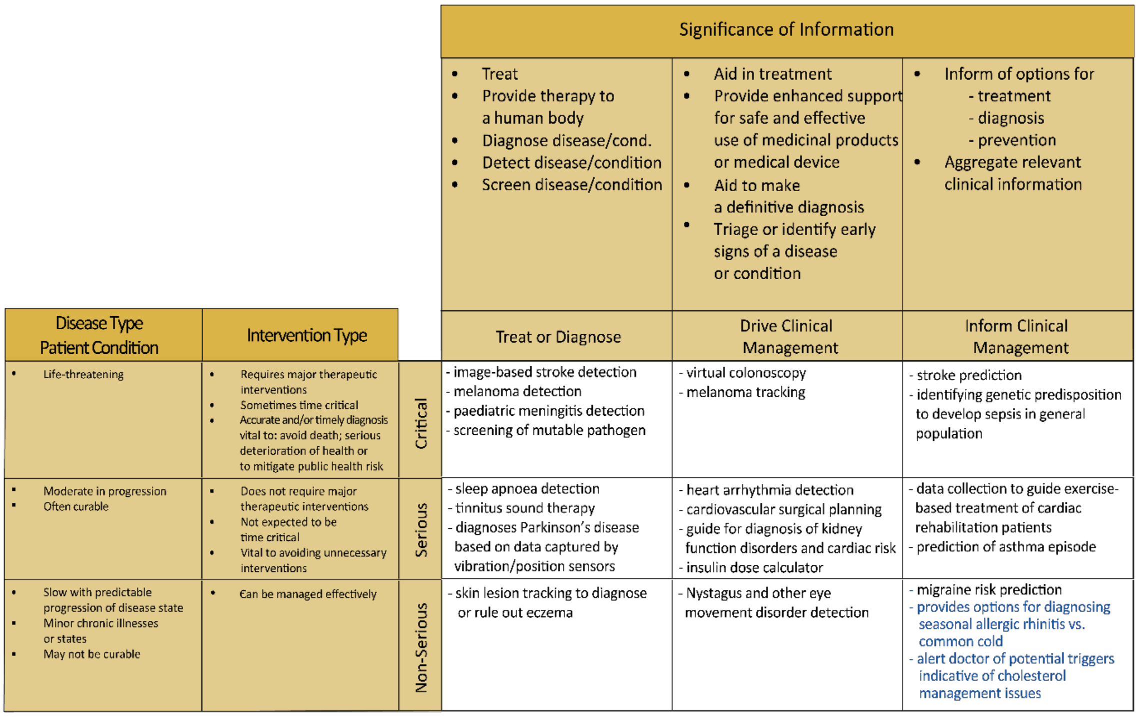
Software devices, including certain software-based hardware devices, are subject to Classification Rule 11 if they fall in scope of EU MDR. Rule 11 is interpreted by means of a risk framework agreed by the International Medical Device Regulators Forum (IMDRF), a voluntary group of medical device regulators from around the world that work together to accelerate international medical device regulatory harmonization and convergence. The framework assigns software according to 9 risk types (Figure 10 & Figure 11). Other rules may also apply, for example to consider hardware risks, which might be relevant for certain embodied AI. E.g. medical devices submitting energy to the human body, such as ionizing radiation, are subject to Classification Rule 9.

The vast majority of medical device software is class IIa or higher under the EU MDR or class B or higher under the EU IVDR, requiring an ex ante and ex post conformity assessment by a notified body.



			Significance of Information		
			• Treat • Provide therapy to a human body • Diagnose disease/cond. • Detect disease/condition • Screen disease/condition	• Aid in treatment • Provide enhanced support for safe and effective use of medicinal products or medical device • Aid to make a definitive diagnosis • Triage or identify early signs of a disease or condition	• Inform of options for - treatment - diagnosis - prevention • Aggregate relevant clinical information
Disease Type Patient Condition	Intervention Type		Treat or Diagnose	Drive Clinical Management	Inform Clinical Management
• Life-threatening	• Requires major therapeutic interventions • Sometimes time critical • Accurate and/or timely diagnosis vital to: avoid death; serious deterioration of health or to mitigate public health risk	Critical	III Type IV.i	IIb Type III.i	IIa Type II.i
• Moderate in progression • Often curable	• Does not require major therapeutic interventions • Not expected to be time critical • Vital to avoiding unnecessary interventions	Serious	IIb Type III.ii	IIa Type II.ii	IIa Type I.ii
• Slow with predictable progression of disease state • Minor chronic illnesses or states • May not be curable	• Can be managed effectively	Non-Serious	IIa Type II.iii	IIa Type I.iii	IIa Type I.i

Figure 10 *Classification Rule 11§1 is based on the IMDRF SaMD risk framework. This risk framework considers the significance of the information (x-axis) and the criticality of the disease or condition (y-axis) to assess the risk of software. This table does not cover Classification Rule 11§2 and §3, the latter covering also class I software, such as fertility apps.*



			Significance of Information		
			• Treat • Provide therapy to a human body • Diagnose disease/cond. • Detect disease/condition • Screen disease/condition	• Aid in treatment • Provide enhanced support for safe and effective use of medicinal products or medical device • Aid to make a definitive diagnosis • Triage or identify early signs of a disease or condition	• Inform of options for - treatment - diagnosis - prevention • Aggregate relevant clinical information
Disease Type Patient Condition	Intervention Type		Treat or Diagnose	Drive Clinical Management	Inform Clinical Management
• Life-threatening	• Requires major therapeutic interventions • Sometimes time critical • Accurate and/or timely diagnosis vital to: avoid death; serious deterioration of health or to mitigate public health risk	Critical	- image-based stroke detection - melanoma detection - paediatric meningitis detection - screening of mutable pathogen	- virtual colonoscopy - melanoma tracking	- stroke prediction - identifying genetic predisposition to develop sepsis in general population
▪ Moderate in progression ▪ Often curable	▪ Does not require major therapeutic interventions • Not expected to be time critical • Vital to avoiding unnecessary interventions	Serious	- sleep apnoea detection - tinnitus sound therapy - diagnoses Parkinson's disease based on data captured by vibration/position sensors	- heart arrhythmia detection - cardiovascular surgical planning - guide for diagnosis of kidney function disorders and cardiac risk - insulin dose calculator	- data collection to guide exercise-based treatment of cardiac rehabilitation patients - prediction of asthma episode
• Slow with predictable progression of disease state ▪ Minor chronic illnesses or states ▪ May not be curable	• €an be managed effectively	Non-Serious	- skin lesion tracking to diagnose or rule out eczema	- Nystagus and other eye movement disorder detection	- migraine risk prediction - provides options for diagnosing seasonal allergic rhinitis vs. common cold - alert doctor of potential triggers indicative of cholesterol management issues

Figure 11 *Examples provided by the IMDRF (in black) and the US Food and Drug Administration (in blue). For the complete intended use statement, see IMDRF N12 document[144] on risk stratification of Software as a Medical Device or in the FDA Draft guidance on clinical decision support systems[145].*

7.2. OVERSIGHT AND TRANSPARENCY DURING ENTIRE DEVICE LIFETIME

The Medical Device Regulations require ex ante as well as ex post controls on the safety and performance of medical devices, i.e. from device conception to retirement (see Figure 12)

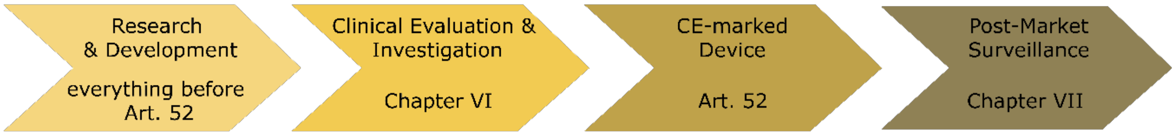


Figure 12 *The ex ante and ex post controls part of EU MDR.*

Manufacturers that wish to place an AI-based device on the market must design and manufacture the device so it achieves the intended performance, in such a way that, during normal conditions of use, it is suitable for the intended purpose. The device must be safe and effective and not compromise the clinical condition or the safety of the patient, or the safety and health of its users, or, where applicable, other persons, provided that any risks which may be associated with its use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, taking into account the generally acknowledged state of the art.[146] To achieve state of the art manufacturers often rely on standards, for example to implement safety and security risk management and software development processes.

[144] *IMDRF N12 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations. 18 September 2014*
[145] *Draft FDA Guidance on Clinical Decision Support Software, issued September 27, 2019*
[146] *EU MDR and Annex I, General Safety and Performance Requirement I*

In addition the manufacturer must continue to evaluate the safety and performance of the device during the entire lifetime of the device, actively collecting and evaluating clinical data during routine use in order to assure the safety and performance of the device (see Figure 13). Such oversight is required under EU MDR and EU IVDR through the requirements on post-market surveillance and post-market clinical follow-up[147].

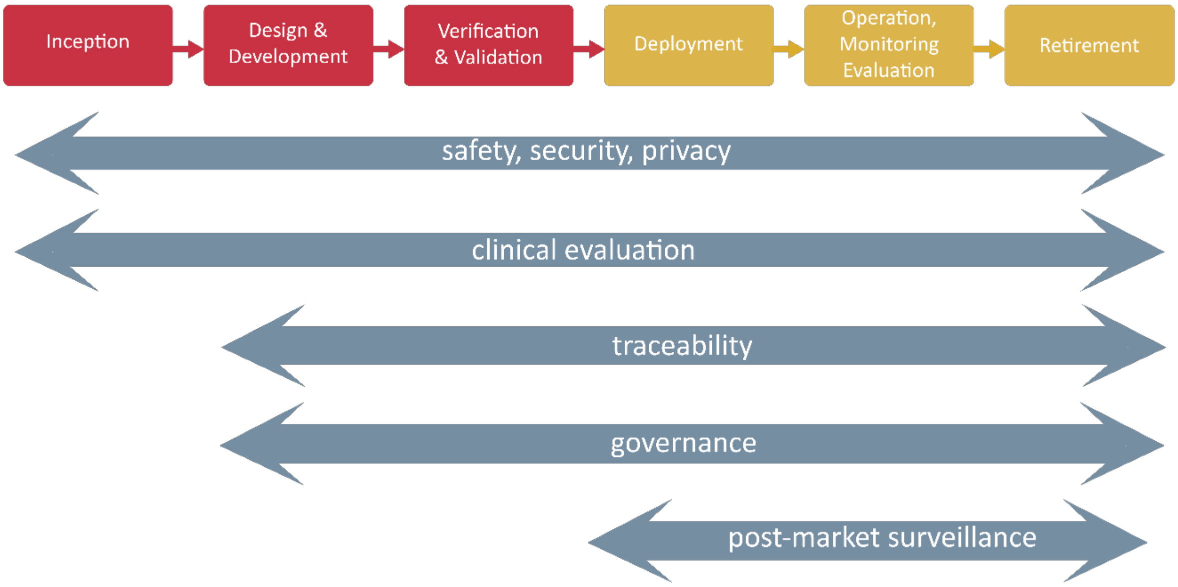


Figure 13 *Lifecycle phases of an AI-based medical device mapped onto a selection of legal requirements*

Transparency is also ensured to the general public through the European database EUDAMED. This database contains information submitted by manufacturers, notified bodies and competent authorities. The European Commission issued a fact sheet[148] describing what information is accessible to the general public.

7.3. GOVERNANCE

The EU MDR and EU IVDR have an elaborate governance system (see Figure 14). Distributors check importers and manufacturers[149]. In turn importers check manufacturers[150]. Manufactures check their suppliers and subcontractors[151]. Manufacturers and critical suppliers in turn are checked by Notified Bodies[152], which in turn are checked by competent authorities[153]. Competent authorities are checked by the Commission. If a manufacturer has no legal entity established in the EU it needs an authorized representative that checks the manufacturer.[154] These checks occur both ex ante and ex post through device conformity assessments, audits, announced and unannounced inspections and market surveillance. In addition (not shown on the visual), certain higher risk medical devices are checked by expert panels or reference laboratories. Health institutions that develop their own AI-based devices for in-house use are subject to surveillance by competent authorities.[155]

[147] *EU MDR Chapter VII Post-Market Surveillance, Vigilance and Market Surveillance, EU MDR Annex XIV Clinical Evaluation and Post-Market Clinical Follow-Up and EU MDR Annex XIII Performance Evaluation, Performance Studies and Post-Market Performance Follow-Up*
[148] *Fact sheet on MDR requirements for Transparency and Public Information. European Commission DG Health and Food Safety – Unit B6. Published July 2020.*
[149] *EU MDR and EU IVDR Annex I, General Safety and Performance Requirement I*
[150] *EU MDR and EU IVDR Art. 13 General obligations of importers*
[151] *EU MDR and EU IVDR Art. 10 General Obligations of manufacturers*
[152] *EU MDR and EU IVDR Chapter IV Notified Bodies*
[153] *EU MDR Section 3 Market Surveillance and EU IVDR Chapter VII Post-Market Surveillance, Vigilance and Market Surveillance*
[154] *EU MDR and EU IVDR Art. 11 Authorised Representative*
[155] *EU MDR and EU IVDR Art. 5 Placing on the market and putting into service*

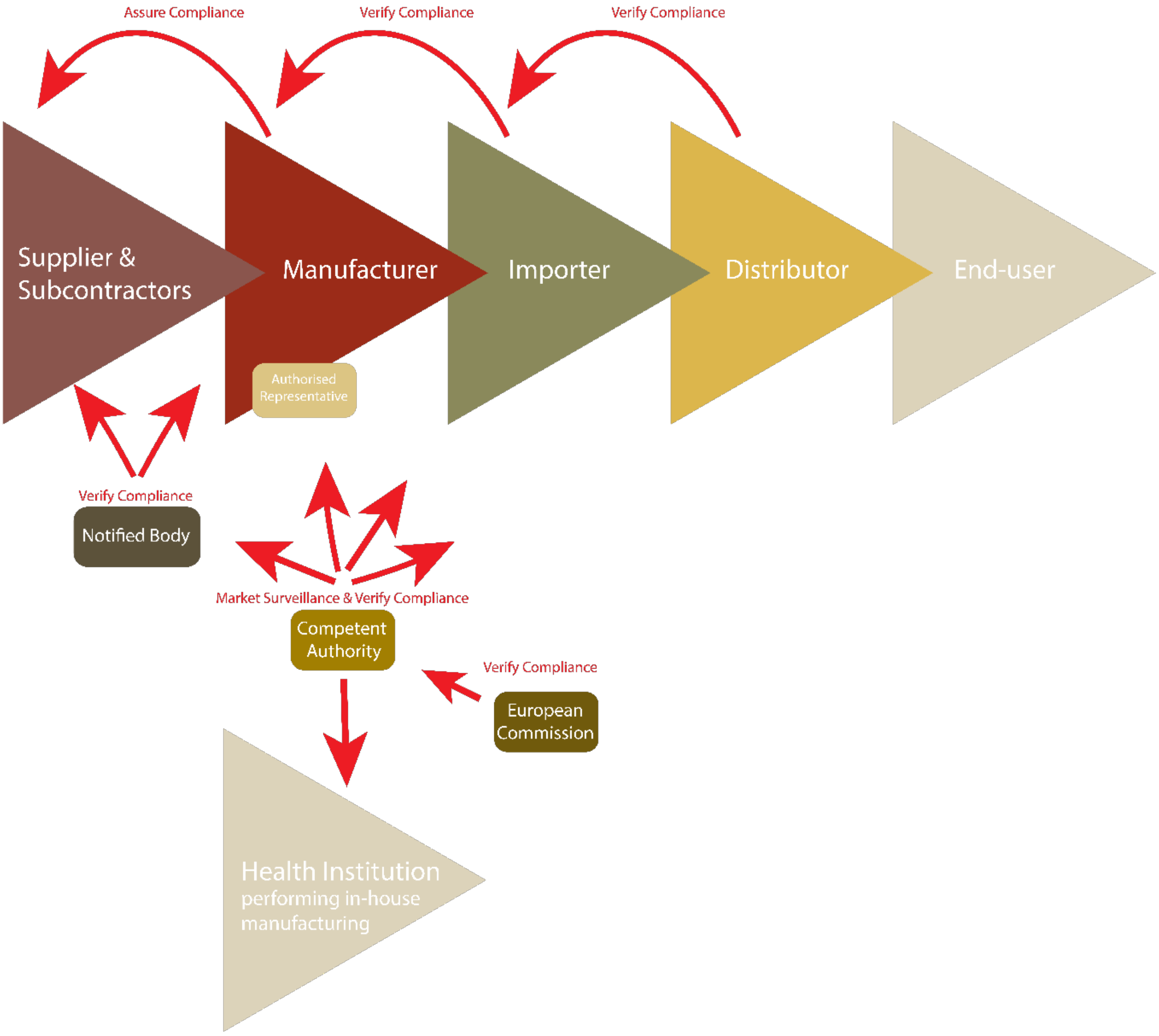


Figure 14 *EU MDR and EU IVDR have an elaborate governance system.*

7.4. NOTIFIED BODIES

Depending on the device class, the manufacturer must follow a compliance assessment procedure that involves the notification of a third-party, independent body. In the EU, such organization is called a Notified Body. The vast majority of medical device software requires the involvement of a notified body. The need to involve a notified body significantly drives up the cost for manufacturers.

The role of a notified body is to evaluate whether the device complies and whether the manufacturer's quality system meets the requirements of the regulation. The Notified Body accomplishes this by on-site audits at the manufacturer's production sites and by assessing the technical documentation of a device prior to certification on a sampling basis.

The conformity assessment of the device involves a qualified technical expert reviewing the technical documentation, sometimes supplemented by tests performed by an independent test laboratory. The clinical evaluation report is reviewed by a qualified domain expert, often a medical doctor. Notified Bodies must prove to Competent Authorities that they have in-house expertise to assess a particular type of product and production process. This is dependent on the Notified Body Operation Group (NBOG) codes[156] the Notified Body is accredited for. There are specific NBOG codes for software-only devices and for products that include software. For a Notified Body to be designated under the EU MDR or EU IVDR they must prove through joint assessments by member states that they meet the requirements of the regulation. Once designated the Notified Body is notified in NANDO[157], a European Database, with an indication of the NBOG codes they have been designated for.

Once the Notified Body determined that the manufacturer has conformed to the relevant assessment criteria, it issues a CE certificate to show that the device meets the requirements. The manufacturer then signs a Declaration of Conformity and applies the CE mark with the Notified Body number.

The role of the notified body does not stop there. After the device is on the market, it performs quality system audits during which it looks at how the manufacturer performs post market surveillance and how the findings feed into the clinical evaluation report. The audits affect whether or not the manufacturer's device can retain the CE-label.

7.5. TESTING

Type Examination is possible under EU MDR, but almost never practiced for software devices. DEKRA being the only Notified Body currently accredited for Type Examination of software is an indication that type testing of software is more a theoretical rather than a practical possibility. The reason for this is that it is impossible to test software exhaustively.[158] Generally Notified Bodies assess software devices through the full quality assurance route (see Figure 15). Only through the combination of assessing (1) rigorous development and (2) testing processes can Notified Bodies have a reasonable assurance of the safety and performance of software.

Notified Bodies also verify whether the test evidence provided by the manufacturer via the technical file and the clinical evaluation report meet the regulation, is scientifically sound and state-of-the-art from a technical and clinical point of view and whether the risks are acceptable and are outweighed by the benefits.

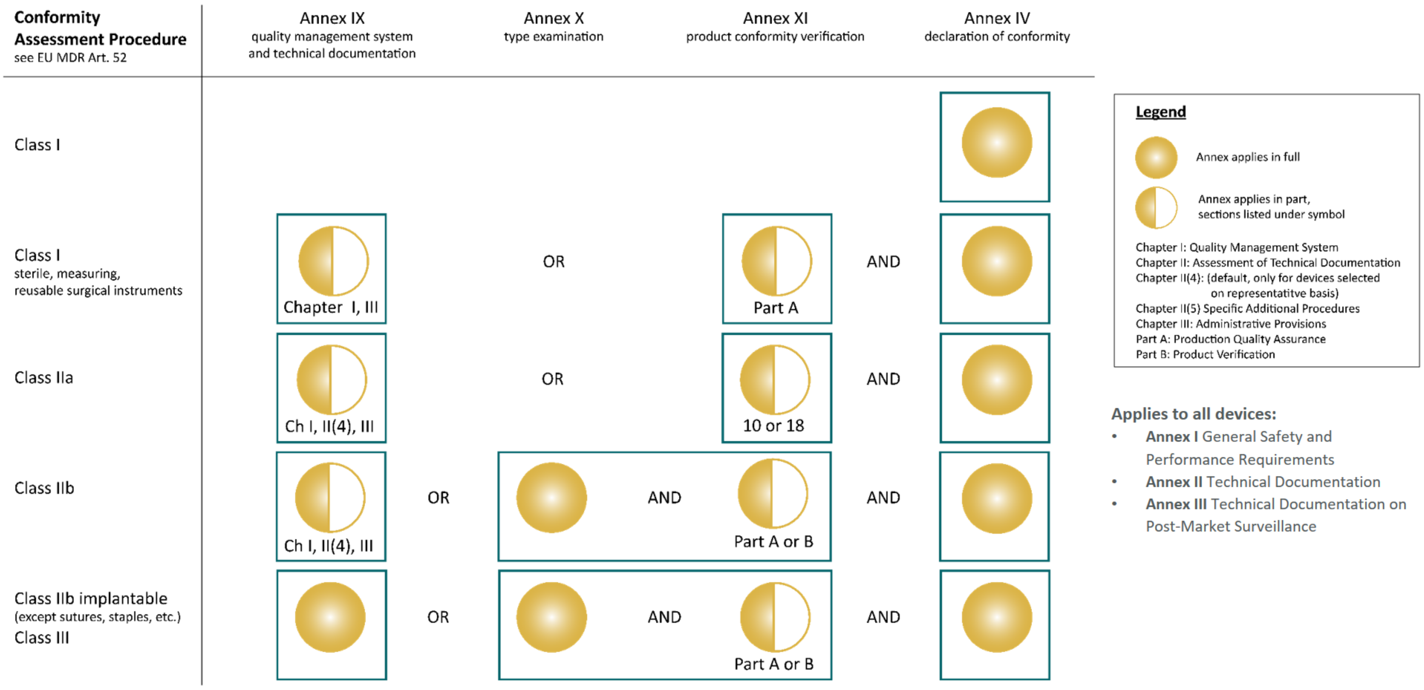
Test protocols are not standardized due to the wide variety of software technology and the diversity of clinical domains in which it is used. Regulatory guidance of the clinical evaluation of medical device software requires that manufacturers prove through a literate study that their test protocols are scientifically valid and that results meet state-of-the-art. State-of-the-art can be a standard, a well-known method described in literature a benchmark device, another technology or human level performance. In cases where manufacturers rely on testing to establish whether their device meets state-of-the-art they generally collect and use their own datasets; in rare cases reference datasets are available, governed by academia or consortia and endorsed by regulators or professional societies, e.g.

- MIMIC-III[159], a freely accessible critical care database for predictive analytics established by academia.
- Lung Image Database Consortium Image Collection (LIDC)[160] - Established by US National Cancer Institute and endorsed by the FDA.

In any case**, the clinical evidence must contain clinical data from the European population, or a justification of why clinical evidence is transferrable to the European population[161].**

Considering the difficulty for industry to collect datasets for research, training and testing purposes under GDPR, the creation and availability of reference datasets supporting regulatory compliance and endorsed by professional societies should be further encouraged.

[156] *NBOG codes under the EU MDR MD F 2017-3 and under EU IVDR IVD F 2017-4 European Commission website, accessed 28 May 2020.*
[157] *https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.notifiedbody&dir_id=34*
[158] *If you take a simple software function with just two inputs, where each input comprises a 32 bit integer, then the full range of inputs to be tested would be that between -2 to the power of 31 all the way to +2 to the power of 31 minus one. If you were to test all possible combinations of these 2 inputs, you end up with more than a trillion combinations that you would need to test, for just one single function in your software. On a 2.2 GHz Intel processor that would take you more than 300.000 years. If you realize that software often contains thousands of lines of code, it should not surprise you that exhaustive testing is not achievable.*
[159] *https://mimic.physionet.org/, accessed 18 May 2020*
[160] *https://wiki.cancerimagingarchive.net/display/Public/LIDC-IDRI, accessed 18 May 2020*
[161] *MDCG 2020-5 Clinical Evaluation – Equivalence – A guide for manufacturers and notified bodies, April 2020*



Conformity Assessment Procedure see EU MDR Art. 52	Annex IX quality management system and technical documentation		Annex X type examination		Annex XI product conformity verification		Annex IV declaration of conformity
Class I							●
Class I sterile, measuring, reusable surgical instruments	◐ Chapter I, III		OR		◐ Part A	AND	●
Class IIa	◐ Ch I, II(4), III		OR		◐ 10 or 18	AND	●
Class IIb	◐ Ch I, II(4), III	OR	●	AND	◐ Part A or B	AND	●
Class IIb implantable (except sutures, staples, etc.) Class III	●	OR	●	AND	◐ Part A or B	AND	●

Legend

● Annex applies in full

◐ Annex applies in part, sections listed under symbol

Chapter I: Quality Management System
Chapter II: Assessment of Technical Documentation
Chapter II(4): (default, only for devices selected on representatitve basis)
Chapter II(5) Specific Additional Procedures
Chapter III: Administrative Provisions
Part A: Production Quality Assurance
Part B: Product Verification

Applies to all devices:

- **Annex I** General Safety and Performance Requirements
- **Annex II** Technical Documentation
- **Annex III** Technical Documentation on Post-Market Surveillance

Figure 15 *Conformity Assessment Procedures under EU MDR. The vast majority of medical device software is class IIa or higher and requires a conformity assessment involving a notified body.*

EU MDR and EU IVDR focus on testing evidence of the AI's performance, rather than on the review of AI's training data. Training data may be owned by the patient or user and may not be representative of the environment in which the AI is ultimately being used.

Whereas specific test protocols are generally not defined through standards, standards do define the elements of good testing.[162] The standards specify the need for independence of the test team, the need for code reviews, unit testing, verification, validation, adherence to coding guidelines, static code analysis, etc. In addition, regulatory guidance[163] explains what is required of manufacturers in terms of proving the clinical safety and performance of their medical device software, through evidence such as scientific validity, analytical and clinical performance.

7.6. ADDRESSES

7.6.1. MANUFACTURERS OF AI-BASED MEDICAL DEVICES AND THEIR ACCESSORIES

The EU MDR and EU IVDR apply to manufacturers of among others medical device software[164] that comprises AI, hardware devices that comprise AI and AI-based accessories for medical devices or in vitro diagnostic medical devices.

7.6.2. HEALTH INSTITUTIONS MANUFACTURING AI-BASED MEDICAL DEVICES FOR IN-HOUSE USE

The EU MDR and EU IVDR apply to health institutions that develop AI-based devices for in-house use.[165]

[162] *In the medical device space the most important standards are ISO 14971 on safety risk management for medical devices, IEC 27000 on security quality management systems (endorsed by ENVISA), IEC 62366 on the usability of medical devices and a number of standards specific to software: IEC 62304 on software lifecycle management and IEC 82304-1 on software safety requirements.*

[163] *MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software*
MDCG 2020-5 Clinical Evaluation – Equivalence. A guide for manufacturers and notified bodies.
MDCG 2020-6 Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC. A guide for manufacturers and notified bodies.

[164] *Medical device software is software that is intended to be used, alone or in combination, for a purpose as specified in the definition of a "medical device" in the medical devices regulation or in vitro diagnostic medical devices regulation. See MDCG guidance 2019-11 on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.*

[165] *EU MDR & EU IVDR Article 5(5) for conditions and responsibilities related to health institutions developing devices for in-house use. Also national provisions apply to in-house manufacturers.*

7.6.3. MANUFACTURERS OF AI-BASED MEDICAL DEVICES SOLD AS A SERVICE

The EU MDR and EU IVDR apply to manufacturers of devices sold as a service to persons established in Europe, regardless of whether a software device used to provide the service is running on a server based in or outside of the EU.[166]

7.6.4. MANUFACTURERS OF CUSTOM-MADE AI-BASED MEDICAL DEVICES

The EU MDR applies to manufacturers of custom-made devices, i.e. devices specifically made in accordance with a written prescription of any person authorised by national law by virtue of that person's professional qualifications which gives, under that person's responsibility specific design characteristics, and is intended for the sole use of a particular patient exclusively to meet their individual conditions and needs.[167]

Devices, which need to be adapted to meet the specific requirements of any professional user and devices which are mass-produced by means of industrial manufacturing processes in accordance with the written prescriptions of any authorised person, are not considered custom-made devices, but regular medical devices.

Note: increasingly open-source specifications are made available so patients can make, assemble and develop their own AI-based devices, such as bionic legs[168]. The EU MDR and EU IVDR does not apply to patients developing and manufacturing AI-based devices for their own use. Manufacturers of parts or components for such devices are subject to the EU MDR or EU IVDR under certain conditions as discussed in the next section.

7.6.5. MANUFACTURERS OF AI-BASED PARTS OR COMPONENTS FOR A MEDICAL DEVICE

Manufacturers of AI parts or components intended to upgrade or change products placed on the market are subject to EU MDR or EU IVDR in a number of scenarios:

1. If manufacturer places AI on the market as a part or component intended specifically to replace an identical or similar part or component of a device[169], e.g. a software update to patch a security vulnerability.
2. If a manufacturer places AI on the market as part or component intended specifically to replace a part or component of a device and that significantly changes the performance or safety characteristics or the intended purpose of the device[170]
3. If a manufacturer places AI on the market intended specifically as addition to a device (rather than to replace a part or component of a device; see Figure 16)
    a. To in itself fulfill one or more of the purposes listed in the definition of a medical device or in vitro diagnostic medical device, e.g., a Computer-Aided-Detection algorithm added to a portable ultrasound transducer. This CAD algorithm is medical device software.
    b. To **not** in itself fulfill one or more of the purposes listed in the definition of a medical device or in vitro diagnostic medical device, but to specifically enable the medical device to be used in accordance with its intended purpose(s) or to specifically and directly assist the medical functionality of the medical device in terms of its intended purpose[171]. This includes new purposes claimed by the AI-manufacturer. E.g., a kit to upgrade a motorized wheelchair with facial recognition software that translates facial expressions into real-time wheelchair commands.[172] The AI-based kit is considered an accessory[173] for the *new* wheelchair.

[166] *EU MDR & EU IVDR Article 6 on devices used by information society services. Whereas the EU was first to regulate software as a service, other countries are now issuing similar legislation. E.g. the US Food and Drug Administration communicated via its "Policy for device software functions and mobile medical applications" that it considers providers of website subscriptions or software as a service that entail medical functionality to be manufacturers of a medical device and subject to its regulation.*

[167] *EU MDR Annex XIII Procedure for Custom Made Devices*

[168] *For an example of open source artificially intelligent prosthetic legs, see https://opensourceleg.com/*

[169] *EU MDR Article 23(1) and EU IVDR Article 20(1) on parts or components*

[170] *EU MDR Article 23(2) and EU IVDR Article 20(2) on parts or components intended to impact the original device in a significant way*

[171] *This wording is taken from the definition of an accessory for a medical device or in vitro diagnostic medical device. Source: EU MDR Article 2(2) and EU IVDR Article 2(4).*

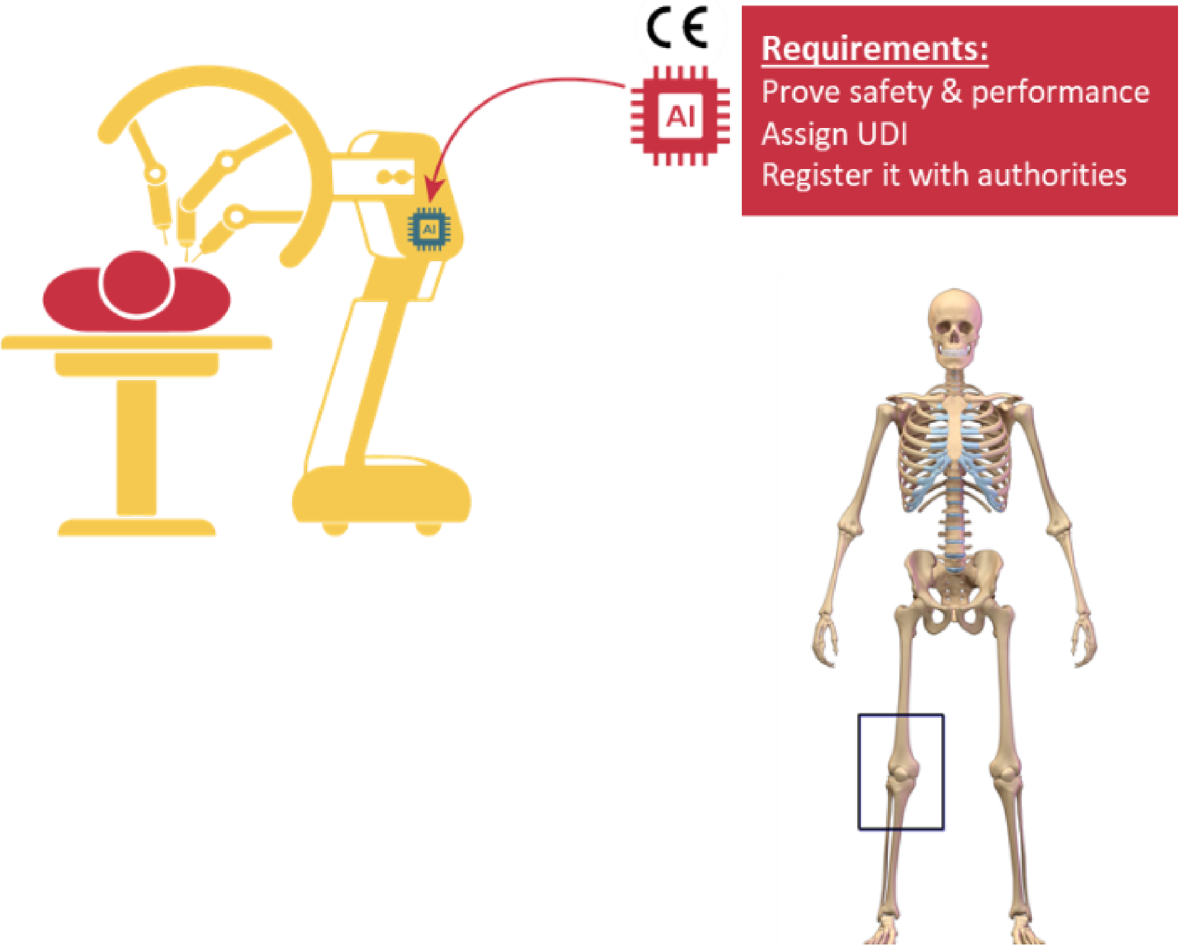
[172] *Intel's Wheelie, see https://www.intel.ai/hoobox/#gs.xzgt73*

[173] *EU MDR Article 1(4) and EU IVDR Article 1(2) consider accessories to be devices, implying that all requirements pertaining devices are applicable also to accessories for medical devices or in vitro diagnostic medical devices.*

4. If a manufacturer places AI on the market intended to be used in combination with a product that is not a medical device in its own right in order to fulfil one or more purposes listed in the definition of a medical device or in vitro diagnostic device[174]. E.g. an AI that turns a consumer camera into a melanoma detection device.[175]

AI placed on the market for general purposes or to build medical devices is not subject to the regulation. E.g., AI intended as training platform or component for a manufacturer to develop an AI-based product. Such AI is not subject to the EU MDR or EU IVDR. If the general purpose AI is used as critical component[176] in the finished medical device, then the AI supplier is considered critical supplier and subject to inspections by notified bodies or competent authorities. Examples:

1. AI placed on the market for detection of sigmoid shapes can be trained by a third party to detect lung lesions. If the AI is considered a critical component, then the supplier is subject to inspections.
2. AI placed on the market for reading curves generated by a thermal cycler by means of quantitative Polymerase Chain Reaction (qPCR) assays can be trained by a third party for assays for specific medical purposes, such as detection of COVID-19 virus.[177] If the AI is considered a critical component, then the supplier is subject to inspections.



Requirements:
Prove safety & performance
Assign UDI
Register it with authorities

Figure 16 *Manufacturer A places a surgical robot on the market. Manufacturer B places a software upgrade on the market intended to execute a new surgical script so that the robot can now also perform a total knee arthroplasty (new specific medical purpose). The software manufacturer is subject to EU MDR as the upgrade replaces the original software intended specifically to change the intended purpose of the robot. Even if the manufacturer places the software on the market as an add-on script rather than to replace the original software, the software manufacturer is still subject to EU MDR; in that scenario the software is considered an accessory for the surgical robot to which the software manufacturer has attributed a new medical claim, i.e. perform knee surgery.*

[174] *EU MDR Article 2(1) for the definition of a medical device, which refers to [...] software [...] alone or in combination, for human beings for one or more of the following medical purposes [...]. Similar text exists in EU IVDR Article 2(2) in the definition of an in vitro diagnostic medical device.*

[175] *Increasingly the computing resources of consumer products are opened up for edge computing purposes, i.e. processing of data where it is generated or captured. E.g. Canon Hacker Development Kit.*

[176] *Critical, in the sense of significantly impacting the safety or performance characteristics or the intended purpose of the medical device*

[177] *Build your own Device, COCIR, February 2018, discusses the relation between manufacturer and health institution responsibilities when software is changed by the health institution within or outside of the change boundaries set by the manufacturer*

7.6.6. ECONOMIC OPERATORS

Under the EU MDR and EU IVDR certain economic operators have responsibilities.

Manufacturers not established in the EU require an authorized representative. An authorized representative is a legal entity established in Europe representing the manufacturer. Authorized representatives are severely liable for defective products they are responsible for.

Manufacturers, authorized representatives and importers[178] need to register in a European database called EUDAMED. In some member states distributors[179] need to register in a national database. Economic operators have responsibilities aimed at avoiding "illegal" devices, including software devices, from being placed on the EU market or put into service.

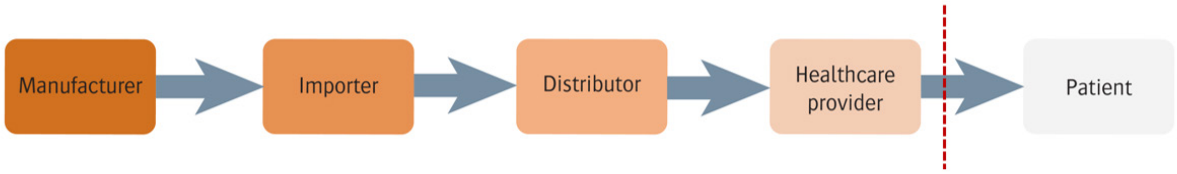


Figure 17 *Economic operators must log which medical devices it delivered to the next economic operator in the distribution chain. This traceability is required from manufacturer to healthcare provider. If a recall is required this traceability should assure that all defective medical devices can be removed from the market. For privacy reasons and except for implant registries traceability is NOT required for the last step in the distribution chain: from healthcare provider to patient. The implication is that manufacturers or app stores selling directly to patients do not need to log which patient they sold a medical device app to.*

7.7. KEEPING OF RECORDS AND DATA

Having sufficient training and testing data is important for the development of AI. Often this includes personal data.

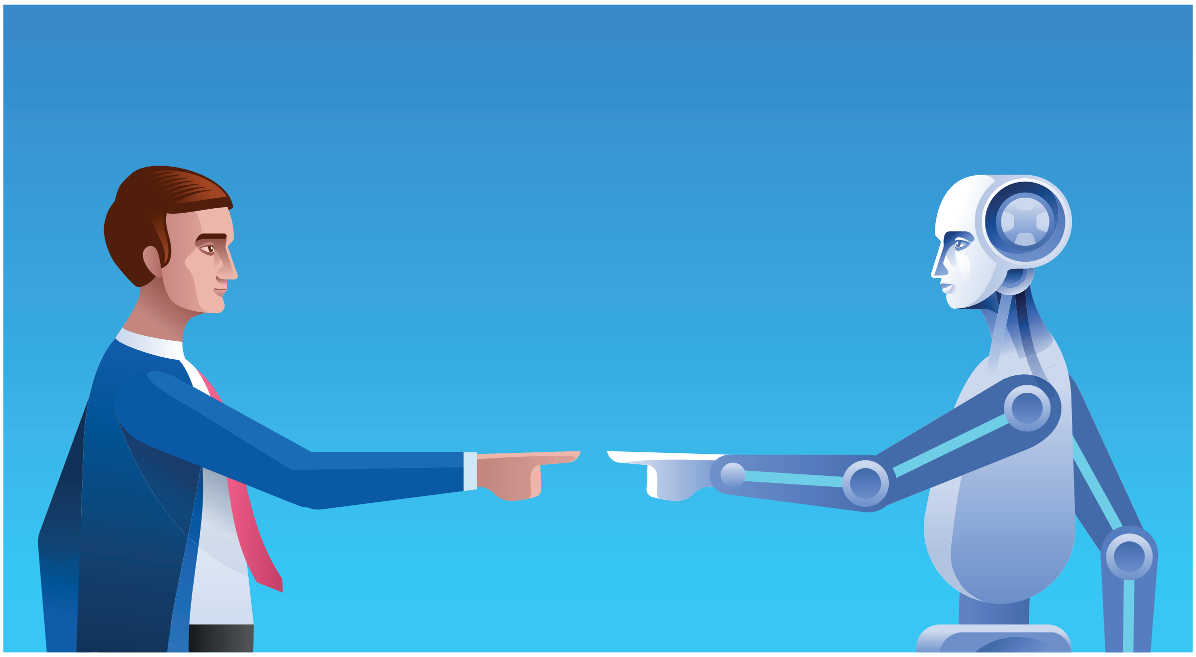
Increasing the amount of data stored however introduces higher storage costs, complex processing, higher security and higher risks. The General Data Protection Regulation also imposes limits on the retention of personal data. IEC 82304-1 General requirements for product safety of health software therefore requires manufacturers to provide all information necessary for the user or the responsible organization to safely decommission and dispose of the health software, including of the personal and health-related data.[180]

Even though there are good reasons to dispose of personal and health-related data, the Medical Device Regulations require manufacturers to retain some of that data. These regulations require the retention of among others the procedures and techniques for monitoring, verifying, validating and controlling the design of the devices, and the corresponding documentation as well as the data and records arising from those procedures and techniques. This documentation includes AI testing data used to provide evidence of compliance. In exceptional cases also AI training data may need to be retained if it is needed to demonstrate safety or performance. This documentation must be retained for a minimum of 10 years after the last device has been placed on the market[181], or 15 years in the case of implantable devices, even if the person having given consent to use the data asks for the withdrawal of that consent (right to be forgotten).[182] In some member states (e.g. Belgium) the documentation must be provided to the competent authority in case the manufacturer stops its activities or goes bankrupt before the data retention period is exceeded.[183] Whereas the EU MDR and EU IVDR lack similar documentation retention requirements for health institutions, national provisions may exist.

Important limitations may exist regarding the extent with which datasets can be stored or shared. Some datasets may be subject to copyrights and may require special licensing agreements. Retaining data sets may be in conflict with some copyright provisions, particularly if non-infringement is based on only temporary use of copies. Providing third party

[178] *EU MDR Article 2(33) and EU IVDR Article 2(26) define an importer as any natural or legal person established within the Union that places a device from a third country on the Union market*
[179] *EU MDR Article 2(34) and EU IVDR Article 2(27) defines a distributor as any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a device available on the market, up until the point of putting into service*
[180] *IEC 82304-1:2016 Requirement 7.2.2.9*
[181] *EU MDR Annex IX Administrative Provisions Section 7 and EU IVDR Annex X Chapter III Administrative Provisions Section 6*
[182] *GDRP Art. 17.1(b) the data subject withdraws consent on which the processing is based according to point [...] and where there is no other legal ground for the processing;*
[183] *Voorontwerp van wet betreffende medische hulpmiddelen, Federaal Agentschap voor Geneesmiddelen en Gezondheidsproducten*

access to underlying data could also conflict with EU privacy laws requiring deletion of personal data, and could conflict with contractual obligations to not retain data supplied by business clients for training models. For products using on-device processing - so called federated learning - there is purposefully no central log of data. If an obligation to share data sets for such applications is imposed, it would undermine the significant privacy benefits of this innovative technique. Organizations who have built devices using open-source models may also have no way to know the provenance of the data used to train the models unless the publisher has chosen to release it, which they will have no obligation to do (especially if they are outside of Europe).



8. INTERNATIONAL COMPARISON

Through the International Medical Device Regulators Forum (IMDRF) authorities reached consensus on what software, including software that uses artificial intelligence, is considered a Medical Device. Regulators call it Software as a Medical Device (SaMD)[184]. Internationally there are large differences with respect to the scope of SaMD that a country regulates (see Figure 18).

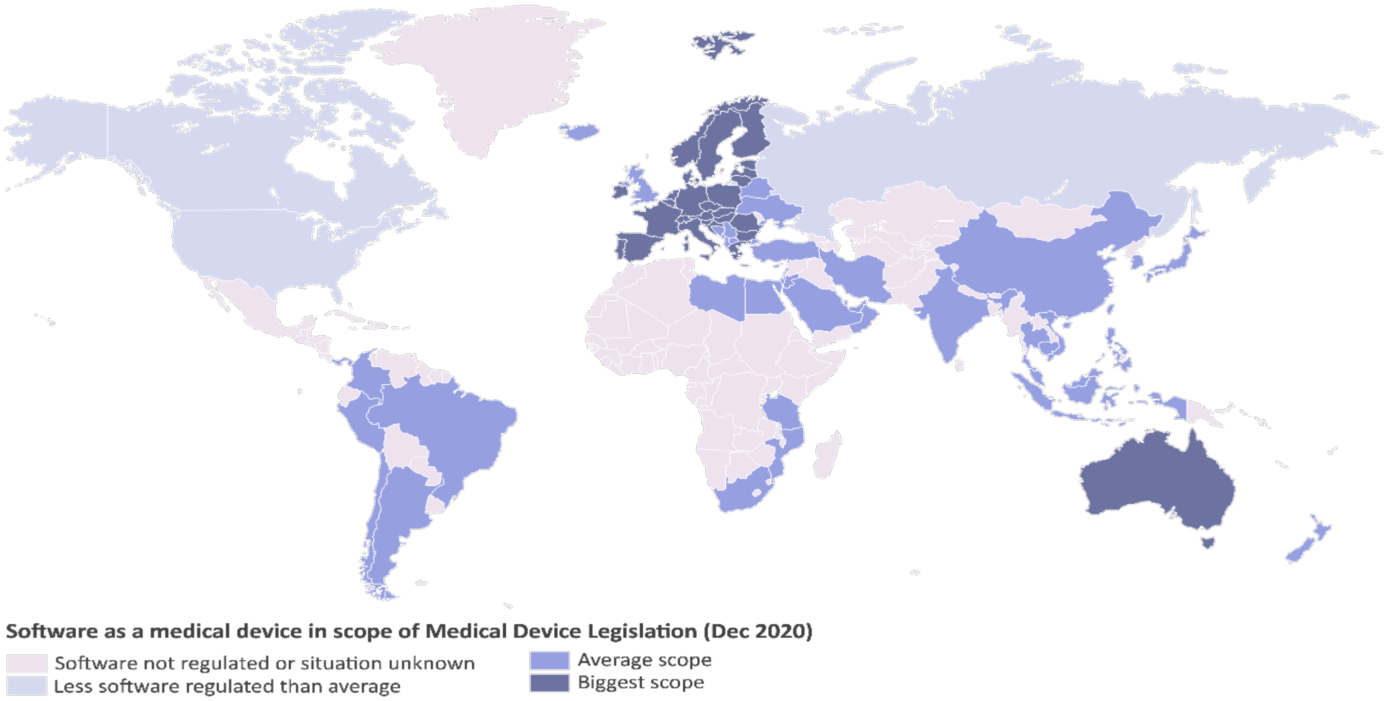

Software as a medical device in scope of Medical Device Legislation (Dec 2020)
Software not regulated or situation unknown
Less software regulated than average
Average scope
Biggest scope

Figure 18 *Regulatory fragmentation of Software as a Medical Device*

The US FDA for example uses the fault lines provided by the IMDRF SaMD Risk Framework[185] to clarify what software is not in scope of its regulation, whereas the EU uses functional exemptions instead. In the EU, SaMD with functionality that is limited to store, communicate, lossless compression or simple search, is not regulated[186]. In the U.S., SaMD to Inform Clinical Management is not regulated if it is intended for a Health Care Professional to independently review and understand the basis of the software recommendation on condition the software does not perform signal or image acquisition, processing or analysis. Consequently, the EU regulation has a larger scope than that of the US, including significantly more clinical decisions support software intended to inform clinical management.

In the U.S., the FDA is examining alternative regulatory pathways for software. For example, the FDA has proposed a software "Precertification" program which is intended to be a regulatory model that is more streamlined and efficient, resulting in getting product to market and on patients faster than existing methods. This would also shorten response times for any post-market issues that might come up. This "Pre-Cert" program[187] involves focusing primarily on the product developer, instead of focusing primarily on the product itself. If the developer can demonstrate a culture of quality, excellence, and responsiveness, then the FDA believes that a streamlined approval process may be allowed. In that respect, the FDA approaches the European Medical Device Regulation, which is based on the assessment of the manufacturer's quality system and an assessment of the product on a sampling basis.

[184] *IMDRF N10 Software as a Medical Device (SaMD): Key Definitions. IMDRF website. 9 December 2013. http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf Accessed 19 May 2020.*

[185] *IMDRF N12 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations. 18 December 2014. IMDRF website http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf. Accessed 20 May 2020.*

[186] *MDCG 2019-11 Guideline – Guidance on the Qualification and Classification of Software in MDR 2017/745 and IVDR 2017/746. 11 October 2019. European Commission website.*

[187] *More information about the Pre-Cert program can be found at https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program*

9. STANDARDS

For artificial intelligence, common and reliable definitions, approaches and methodologies are needed to establish a level of certainty and the basis for building trust into the new technology. Several Working Groups within ISO/IEC JTC1 SC42 (Artificial Intelligence) are currently developing horizontal AI standards, relevant for various industry sectors. Discussions on AI standardization needs specifically for medical devices have started at the recent meetings of IEC/TC 62 (Electrical Equipment in Medical Practice) and ISO/TC 215 (Health Informatics). IEC/TC 62 decided to establish a Software Network and Artificial Intelligence Advisory Group (SNAIG) as well as a liaison to ISO/IEC JTC1 SC42. ISO/TC 215 has established an ad-hoc group on Artificial Intelligence.

ISO/IEC JTC1 SC42 is creating AI standards applicable to all sectors. The following projects have been started:

- ISO/IEC 20546 Information technology — Big data — Overview and vocabulary
- ISO/IEC TR 20547-1 Information technology — Big data reference architecture — Part 1: Framework and application process
- ISO/IEC TR 20547-2 Information technology – Big data reference architecture – Part 2: Use cases and derived requirements
- ISO/IEC 20547-3 Information technology – Big data reference architecture – Part 3: Reference architecture
- ISO/IEC TR 20547-5 Information technology – Big data reference architecture – Part 5: Standards roadmap
- ISO/IEC 22989 Artificial Intelligence – Concepts and terminology
- ISO/IEC 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/AWI TR 23347 Statistics — Big Data Analytics — Data Science Life Cycle
- ISO/AWI TR 23348 Statistics — Big Data Analytics — Model Validation
- ISO/IEC 23894 Information Technology – Artificial Intelligence – Risk Management
- ISO/IEC TR 24027 Information Technology – Artificial Intelligence – Bias in AI systems and AI aided decision making
- ISO/IEC TR 24028 Information Technology – Artificial Intelligence – Overview of trustworthiness in Artificial Intelligence
- ISO/IEC TR 24029-1 Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview
- ISO/IEC 24029-2 Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 2: Formal methods methodology
- ISO/IEC TR 24030 Information technology – Artificial Intelligence – Use cases
- ISO/IEC TR 24368 Information Technology – Overview of ethical and societal concerns
- ISO/IEC TR 24372 Information Technology – Artificial Intelligence – Overview of computational approaches for AI systems
- ISO/IEC 24668 Information Technology – Artificial Intelligence – Process management framework for Big data analytics
- ISO/IEC 38507 Information Technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations

The Structure of the workgroup is as followed:

- WG1 – Foundational standards (terminology, framework)
- WG2 – Big Data (vocabulary, reference architecture)
- WG3 – Trustworthiness (incl. risk, robustness, bias)

- WG4 – Use cases and applications
- WG5 – Computational approaches
- JWG1 – Governance implications for AI

Within IEEE the following standards exist or are being developed:

- P7001 - Transparency of Autonomous Systems
- P7002 - Data Privacy Process
- P7003 - Algorithmic Bias Considerations
- P7009 - Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems
- P7010 - Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems
- P7011 - Standard for the Process of Identifying and Rating the Trustworthiness of News Sources
- P7014 - Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems
- P2049.1 Standard for Human Augmentation: Taxonomy and Definitions
- P2049.2 Standard for Human Augmentation: Privacy and Security
- P2049.3 Standard for Human Augmentation: Identity
- P2049.4 Standard for Human Augmentation: Methodologies and Processes for Ethical Considerations
- P2801 Recommended Practice for the Quality Management of Datasets for Medical Artificial Intelligence
- P2802 Standard for the Performance and Safety Evaluation of Artificial Intelligence Based Medical Device: Terminology
- P2817 Guide for Verification of Autonomous Systems
- P3333.1.3 Standard for the Deep Learning-Based Assessment of Visual Experience Based on Human Factors
- P3652.1 Guide for Architectural Framework and Application of Federated Machine Learning

Streamlining medical device regulations globally within a single cohesive framework requires relying on internationally harmonized standards for specific guidance relevant to software's unique challenges. IEC 62304[188] assists manufacturer in applying a risk-based approach to software development and maintenance throughout the product lifecycle. IEC 62304 may be the most widely referenced and useful risk-based software lifecycle standard in the medical device industry today. It contains, among others, requirements relating to requirements management, architecture and design, development, configuration management, verification, defect management and design review of medical device software. It also contains requirements that relate to change management, but these do not specifically reference artificial intelligence. IEC 62304 lacks requirements on validation as these are in scope of IEC 60601 and IEC 82304-1. COCIR recommends that IEC 62304 and 82304-1 be updated with regards to artificial intelligence.

ISO 14971 is another important standard for medical device manufacturers. It covers risk management of medical devices, whereas IEC 80001 covers risk management for IT-networks incorporating medical devices.

- **COCIR recommends** citing relevant AI standards in the Official Journal of the European Union for EU MDR and EU IVDR as they become available. Harmonizing relevant international standards under applicable EU regulations will further the common understanding, the transparency, and the trust between stakeholders.

[188] *IEC 62304:2006 Medical device software - Software lifecycle processes. AAMI. Accessed 17 April 2020.*

10. VOLUNTARY LABELLING SYSTEM FOR HEALTH APPS

In the context of the EU policy on digital health for 2014-2020, notably with respect to the ambition to create digital tools and data for citizen empowerment and person-centered healthcare, DG CNECT, supported by DG Grow, initiated the creation of a technical specification on the quality and reliability of health and wellness apps (CEN/ISO/IEC TS 82304-2). The specification aims to support the uptake of innovative digital-based tools for health.

DG CNECT observed that there are many uncoordinated national initiatives for the assessment of app quality. This has frustrated app developers as their product may be very successful in one market, but had to comply with a very different set of criteria in other countries around Europe and across the world. From the European Commission's perspective that was an opportunity to improve this aspect within the digital single market.

There was also a concern that there are hundreds of thousands of apps in the wild already being marketed for health and wellness purposes with an unknown quality or safety. A technical specification leveraging existing standards can play an important role.

The specification defines a quality label to visualize the quality and reliability of health apps (see Figure 19 Draft health app quality label). The specification is intended for use by app manufacturers as well as by app checkers in order to communicate the quality and reliability of a health app. Consumers, patients, carers, health care professionals and the wider public will be able to use the quality label when recommending or selecting a health app for use.

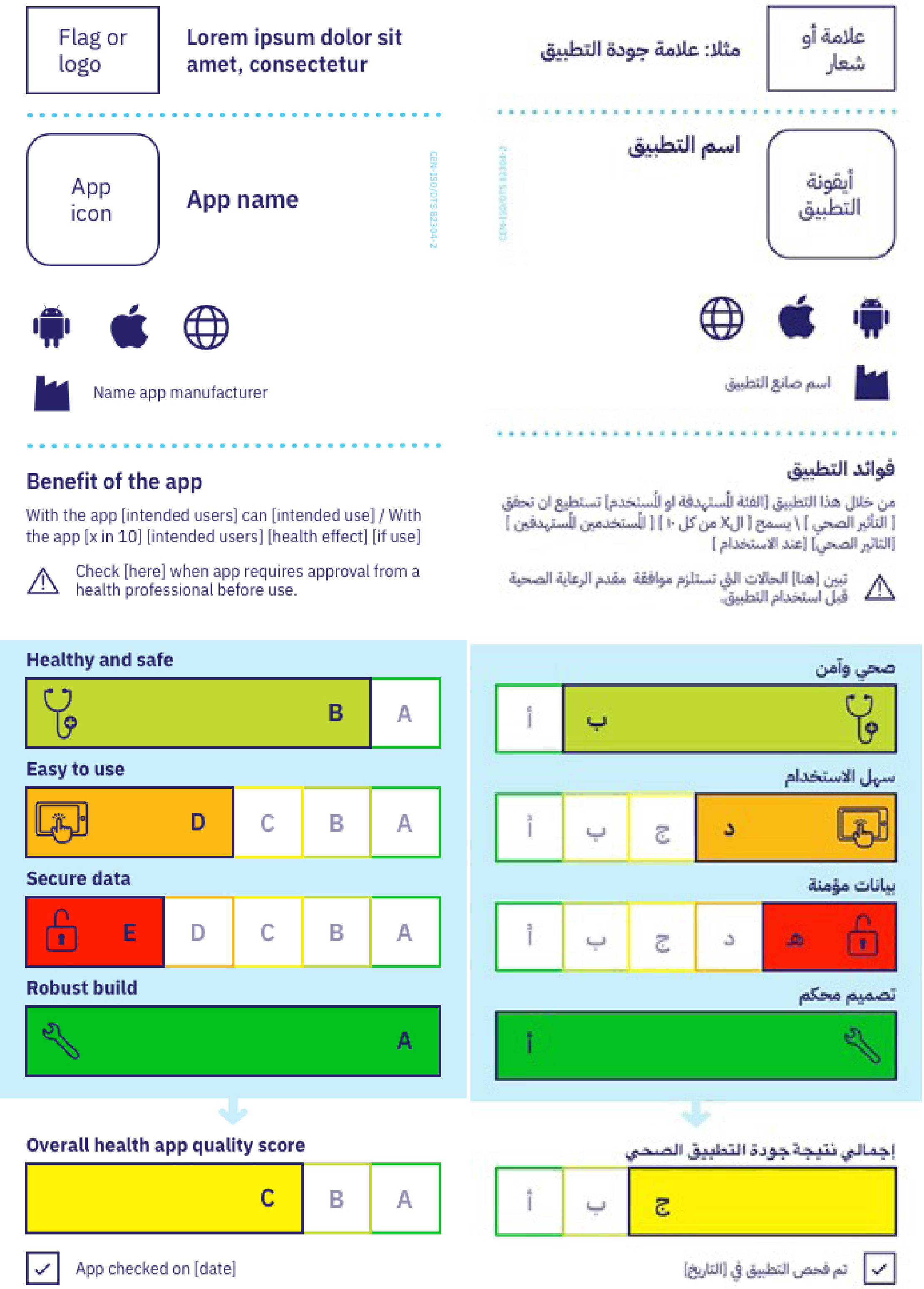
The creation of the specification is being led by the European Committee for Standardization (CEN), working with the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), and the European Committee for Electrotechnical Standardization (CENELEC).

The specification is intended to apply to any app that is being promoted explicitly to improve health and wellness, building on the definition of health from the World Health Organization (WHO) "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity". It applies to both medical device software as well as to health software that is not subject to the Medical Device Regulations, including artificial intelligence. The aspects captured or evaluated by the specification are listed in Table 2.

PRODUCT INFORMATION			
Product			
App manufacturer			

HEALTHY AND SAFE	EASY TO USE	SECURE DATA	ROBUST BUILD
Health requirements	Accessibility	Privacy	Technical robustness
Health risks	Usability	Security	Interoperability
Ethics			
Health benefit			
Societal benefit			

Table 2 *Aspects captured or evaluated by CEN/ISO/IEC TS 82304-2*



With the app [intended users] can [intended use] / With the app [x in 10] [intended users] [health effect] [if use]

⚠ Check [here] when app requires approval from a health professional before use.

من خلال هذا التطبيق [الفئة المُستهدفة او المُستخدم] تستطيع ان تحقق
[التأثير الصحي] \ يسمح [الـX من كل ١٠] [المُستخدمين المُستهدفين]
[التأثير الصحي] [عند الاستخدام]

⚠ تبين [هنا] الحالات التي تستلزم موافقة مقدم الرعاية الصحية
قبل استخدام التطبيق.

Figure 19 *Draft health app quality label. The label can be used with different character sets and script directions within a maximum number of characters. Translations of the label and icons shall be tested with local low health literates for adequate understanding. If the label is used in a digital marketplace or repository, the appropriate label shall be shown on the display mechanism in proximity to the price of the product.*

11. SUMMARY OF RECOMMENDATIONS

COCIR recommends that manufacturers of AI-system that changes through learning during runtime add a pre-determined *Algorithm Change Protocol* to the technical documentation of their device for evaluation during conformity assessment. Manufacturers that make significant changes to the pre-determined *Algorithm Change Protocol* need to update the technical documentation, including the clinical evaluation. They need to perform a new conformity assessment. Changes that are in scope of the Algorithm Change Protocol are not significant changes. Changes that go beyond the change of the Algorithm Change Protocol can be significant. (Chapter 4)

COCIR recommends manufacturers of AI that changes through learning to consider a design capable of storing discrete states of a learned model and capable of returning to a previously stored state in order to reproduce results. (Chapter 6.3.3)

COCIR recommends citing in the Official Journal of the European Union relevant AI standards for EU MDR and EU IVDR as they become available. This will further the common understanding, the transparency, and the trust between stakeholders. (Chapter 9) As a start, COCIR recommends harmonizing:

- *ISO 14971:2019 Medical devices: application of risk management to medical devices* to give manufacturers a clear signal that also mental risks must be controlled (Chapter 6.3.5)
- *IEC 62366-1:2015+A1 Medical devices – Part 1: Application of usability engineering to medical devices* to give manufacturers a clear signal to identify and control inappropriate levels of user trust (Chapter 6.3.6)

COCIR recommends updating two standards commonly used in healthcare in view of artificial intelligence:

- *IEC 62304:2006/At 1:2015 Medical device software—Software lifecycle processes*
    - > Requiring among others that manufacturers define an Algorithm Change Protocol (ACP) for AI that changes through learning during runtime (Chapter 4)
- *IEC 82304-1:2016 Health Software – Part 1: General requirements for product safety* (Chapter 4)
    - > by requiring manufacturers to describe AI attributes in user-facing documentation:
        - If, for what aspects and how the AI provides human oversight or control
        - If, for what aspects and how the AI changes
            - > Define if AI is locked or changes through learning during runtime
            - > Provide a description of change dynamics and change boundaries
            - > Define if and how humans can control change
    - > by requiring manufacturers to inform user on how to adjust the “knob” when fairness/accuracy trade-offs exist and can be adjusted by the user (Chapter 5)
    - > by requiring manufacturers to assess AI for bias and if bias is found and considered harmful, to minimize the bias. (Chapter 6.3.2)
    - > by requiring manufacturers to add to the limitations or contraindications to the use any minority group that can potentially be subject to a risk of significant bias (Chapter 6.3.2)
    - > by requiring manufacturers to inform the user of the performance characteristics of their AI-based device needed to discern the degree to which the software output and performance under the intended use conditions produces identical results, for example by communicating its precision, sensitivity, specificity, confidence, operating parameters, … (Chapter 6.3.3)

Explicability is a means (to trust), not a goal. Rather than legislators issuing a blanket requirement for all AI to be explained, **COCIR suggests** that, in alignment with EU MDR and EU IVDR, AI to be made transparent to the point of becoming actionable to the user, if required to ensure the safe and effective use of the device (Chapter 6.1).

Also in alignment with EU MDR and EU IVDR **COCIR recommends** manufacturers to “minimize bias”, rather than obtain “zero bias”, as COCIR considers the latter to be impossible (Chapter 6.3.2).

12. ACRONYMS

ACP	Algorithm Change Protocol
AI	Artificial Intelligence
APAP	Automatic Positive Airway Pressure
CA	Competent Authority
CT	Computed Tomography
EFOMP	European Federation of Organisations for Medical Physics
EU	European Union
EUDAMED	European Medical Device Database
EU IVDR	Regulation (EU) 2017/746 on in vitro diagnostic medical devices
EU MDR	Regulation (EU) 2017/745 on medical devices
FDA	Food and Drug Administration
GDMP	Good Data Management Practices
GDPR	General Data Protection Regulation (EU) 2016/679
GSPR	General Safety and Performance Requirement
IMDRF	International Medical Device Regulators Forum
LIDC	Lung Image Database Consortium Image Collection
NB	Notified Body
NBOG	Notified Body Operational Group
QMS	Quality Management System
qPRC	quantitative Polymerase Chain Reaction
SaMD	Software as a Medical Device

GENERAL INFORMATION ABOUT COCIR

COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries.

Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007. COCIR is unique as it brings together the healthcare, IT and telecommunications industries.

Our focus is to open markets for COCIR members in Europe and beyond. We provide a range of services in the areas of regulatory, technical, market intelligence, environmental, standardisation, international and legal affairs.

COCIR is also a founding member of DITTA, the Global Diagnostic Imaging, Healthcare IT and Radiation Therapy Trade Association (www.globalditta.org).

COCIR COMPANY MEMBERS:

Abbott 雅培 · ACCURAY · AGFA HealthCare · AGFA · Alcon · alert

align (invisalign | iTero) · Apple · BARCO · BAYER · BioLizard · BD · Canon CANON MEDICAL

Carestream · Dedalus HEALTHCARE SYSTEMS GROUP · Dentsply Sirona · Elekta · EOS imaging · Epic

esaote · FRESENIUS MEDICAL CARE · FUJIFILM · GE · HITACHI Inspire the Next · HOLOGIC The Science of Sure · iba · IBM

强生(中国)医疗器材有限公司 Johnson & Johnson Medical (China) Ltd. · KONICA MINOLTA · Medtronic 美敦力 Further, Together · nova motum SERVICES & CONSULTING · PHILIPS · Roche · SAMSUNG

SIEMENS Healthineers · stryker · TERUMO BLOOD AND CELL TECHNOLOGIES · thirona · varian · WeHealth Digital Medicine · ZEISS

NATIONAL TRADE ASSOCIATIONS MEMBERS:

AGORIA	BELGIUM
LE DISPOSITIF MÉDICAL snitem Pour faire avancer la santé	FRANCE
bvitg	GERMANY
ZVEI	GERMANY
ETOSZ ASSOCIATION OF HEALTH TECHNOLOGY SUPPLIERS AND MEDICAL DEVICE MANUFACTURERS	HUNGARY
CONFINDUSTRIA Dispositivi Medici	ITALY
Associação Portuguesa das Empresas de Dispositivos Médicos apormed tecnologias para a saúde	PORTUGAL
FHI MEDICAL TECHNOLOGY	THE NETHERLANDS
FME POWERED BY DUTCH TECHNOLOGY	THE NETHERLANDS
VERENIGING VAN ORGANISATIES VOOR ICT IN DE ZORG	THE NETHERLANDS
fenin federación española de empresas de TECNOLOGÍA SANITARIA	SPAIN
SWEDISH Medtech	SWEDEN
TIP GÖR DER	TURKEY

© COCIR MAY 2021 / D-NICE GRAPHIC DESIGN

COCIR Advancing Healthcare

COCIR *How to join us*

COCIR aisbl | Bluepoint Building | Boulevard A. Reyerslaan 80 | 1030 Brussels | Belgium
Tel +32 (0)2 706 89 60 | Email info@cocir.org | www.cocir.org | @COCIR