EU software regulations: The new normal or innovation stagnation?

James W. Monroe
President and CEO,
Global RQC Med Device Solutions, LLC™

Correspondence to:
James W. Monroe
319 Shilling Drive
Somerset, NJ 08873 USA
jmonroe@globalrqc.com

Abstract
Advances in software and its application in a medical device and as a medical device have opened the door for many new technological capabilities in healthcare. Around the globe, government agencies have begun to take a heightened interest in how these devices are regulated. Whether it is software embedded in a medical device, software as a medical device, mobile medical applications, or artificial intelligence/machine learning mechanisms, there are potential risks to both user and patient. Cybersecurity is the gateway for evaluating vulnerabilities and protecting devices and patients. In this article, we examine how the EU has introduced new regulations regarding software, cybersecurity, and the impact on the total product life cycle development and innovation of new technologies. Privacy rules in compliance with the EU General Data Protection Regulation may present innovators with challenges by limiting AI's usage of patient data.

Introduction
With the boom of the internet, the ubiquity of the smartphone, and exponential advancements in software technology and applications, it is no surprise that these developments have implications for the medical device industry and regulation. Across the world, regulators are reshaping the process of bringing medical devices to market either on a country-by-country basis or through collective initiatives. In recent years, we have seen the formation of the Global Harmonization Task Force, only to see it dissolve based on individual interests of countries. We have also seen the formation of the International Medical Device Regulators Forum (IMDRF) whose mission it is to provide a global harmonised message regarding the regulation of medical devices.[1]

Among regulatory bodies, the FDA, it would appear, has had the most rigorous approach to regulating medical devices, as well as to staying ahead of the curve with technological advances. Most recently, there has been a surge in activity from other regulatory bodies including those in the EU, Australia, Canada, and Japan, to name a few, as they are now implementing stricter protocols for how medical devices are regulated and the requirements that must be met to bring them to market. The EU, for example, totally revamped its regulatory process with the implementation of the EU Medical Device Regulation of 2017 (EU MDR 2017/745).[2] The many changes include increased requirements of the clinical evaluation report, Notified Body accreditation, new General Safety and Performance Requirements (formally essential requirements checklist), and new regulations regarding software, and, in particular, "software *as* a medical device" (SaMD), not just "software *in* a medical device".

For software in a medical device, regulations, standards, and guidance documents have been available for many years as the software in the devices has matured.[3–7] External to the medical device field, we have seen various types of malicious attacks on computer systems that either destroy or interrupt how these systems operate. The medical device industry has not been immune from cyber attacks. It was even determined that a stand-alone device – not connected to a computer network – can be subject to interference from unauthorised individuals. A new concept (depending on its usage), software as a medical device, has now become front and centre in the regulated medical device world. The EU along with the implementation of EU MDR 2017/745, has issued several guidelines on how stakeholders must address software concerns, whether it be in a medical device or as a medical device. Several industry standards serve to support these regulations. In this article, we will look at various aspects of these regulations and consider the potential positive or negative effects on innovation.

Software as a medical device
SaMD can best be described as software that utilises an algorithm (logic, set of rules, or model) that operates on data input (digitised content) to produce an output that is intended for medical purposes that are defined by the SaMD manufacturer. The risks and benefits posed by SaMD outputs are largely related to the risk of inaccurate or incorrect output of the SaMD, which may affect the clinical management of a patient.

Stand-alone software – SaMD – must meet the requirements of a medical device:

> *'Medical device' means any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) and does not achieve its primary intended action by pharmacological, immunological or metabolic.*[1]

As such, these SaMD "devices" must conform to the same requirements of other devices to be placed on the market in the EU under EU MDR 2017/745. The IMDRF also has a definition for SaMD,[1] which is included in IMDRF/SaMD WG/N10FINAL:2013. It is defined as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device".

Examples of software as a medical device (SaMD) include the following:

1. IDx-DR, IDx LLC, a retinal diagnostic software device is a prescription software device that incorporates an adaptive algorithm to evaluate ophthalmic images for diagnostic screening to identify retinal diseases or conditions.
2. Accipiolx, by MaxQ-AI Ltd., is a software workflow tool designed to aid in prioritising the clinical assessment of adult non-contrast head CT cases with features suggestive of acute intracranial haemorrhage in the acute care environment. Accipiolx analyses cases

using an artificial intelligence algorithm to identify suspected findings. It makes case-level output available to a PACS/workstation for worklist prioritisation or triage.

3. QuantX is a computer-aided diagnosis (CADx) software device used to assist radiologists in the assessment and characterisation of breast abnormalities using MR image data.
4. ClearView cCAD, ClearView Diagnostics Inc., is a software application designed to assist skilled physicians in analyzing breast ultrasound images. ClearView cCAD automatically classifies shape and orientation characteristics of user-selected regions of interest (ROIs). The device uses multivariate pattern recognition methods to perform characterisation and classification of images.

The IMDRF in IMDRF/SaMD WG/N41FINAL:2017 – Software as a Medical Device Clinical Evaluation[6] outlines how developers and manufacturers should evaluate software from a clinical standpoint to establish the following:

- That there is a valid clinical association between the output of a SaMD and the targeted clinical condition (to include pathological process or state); and
- That the SaMD provides the expected technical and clinical data

A valid clinical association is an indicator of the level of clinical acceptance and how much meaning and confidence can be assigned to the clinical significance of the SaMD's output in the intended healthcare situation and the clinical condition/physiological state. Analytically and technically, analytical validation measures the ability of an SaMD to accurately, reliably, and precisely generate the intended technical output from the input data. Said differently, analytical validation:

- Confirms and provides objective evidence that the software was correctly constructed – namely, that it correctly and reliably processes input data and generates output data with the appropriate level of accuracy, and repeatability and reproducibility (i.e., precision); and

Across the world, regulators are reshaping the process of bringing medical devices to market either on a country-by-country basis or through collective initiatives.

- Demonstrates that (a) the software meets its specifications and (b) the software specifications conform to user needs and intended uses.

The analytical validation is generally evaluated and determined by the manufacturer during the verification and validation phase of the software development lifecycle using a quality management system (QMS).[8]

Clinical validation is the third requirement of an SaMD. Clinical validation measures the ability of an SaMD to yield a clinically meaningful output associated with the target use of SaMD output in the target healthcare situation or condition identified in the SaMD definition statement.[6]

"Clinically meaningful" refers to the positive impact of an SaMD on the health of an individual or population, to be specified as meaningful, measurable, patient-relevant clinical outcome(s), including outcome(s) related to the function of the SaMD (e.g., diagnosis, treatment, prediction of risk, prediction of treatment response), or a positive impact on individual or public health.

Clinical validity is evaluated and determined by the manufacturer during the development of SaMD before it is distributed for use (pre-market) and after distribution while the SaMD is in use (post-market). Clinical validation of SaMD can also be viewed as the relationship between the verification and validation results of the SaMD algorithm and the clinical conditions of interest. Clinical validation is a necessary component of clinical evaluation for all SaMD and can be demonstrated by either:[6]

- Referencing existing data from studies conducted for the same intended use;
- Referencing existing data from studies for a different intended use, where extrapolation of such data can be justified; or
- Generating new clinical data for a specific intended use.

The SaMD definition statement, as defined in *SaMD N12*,[8] is used by the SaMD manufacturer to identify the intended medical purpose of the SaMD (treat, diagnose, drive clinical management, inform clinical management), to state the healthcare situation or condition that the SaMD is intended for (critical, serious, non-serious), and to describe the core functionality of the SaMD. The rigour to meet these requirements is outlined in IMDRF/SaMD G/N12FINAL:2014 and is based on the state of the healthcare situation or condition and the significance of information to be provided by the SaMD to the healthcare decision.[8,9]

Artificial intelligence/ machine learning

Artificial intelligence (AI) is the mechanism through which human intelligence is incorporated into machines through a set of rules (algorithm). The term AI refers to something made by humans – a non-natural thing that has the ability to understand or think accordingly. It can also be interpreted as the capability to train a computer to act like the human brain in the way it thinks. AI focuses on three major aspects (skills): learning, reasoning, and self-correction.

Machine learning (ML) is the methodology of the way a computer learns automatically on its own through experiences it had and improves without being explicitly programmed. ML is an application or subset of AI. ML focuses on the development of programs so that it can access data to use it for itself. The entire process makes observations of data to identify the possible patterns being formed and make better future decisions. The goal of ML is to allow the systems to learn by themselves through the experience, without any kind of human intervention or assistance. Additionally, *deep learning* is a subset of ML that utilises neural networks to mimic brain-like behaviour. DL utilises larger sets of data than ML and focuses on information processing patterns.[10]

AI and ML systems in medicine have the potential to significantly improve healthcare, for example, by offering earlier diagnoses of diseases or recommending optimally individualised treatment plans. Yet the emergence of AI/ML in medicine also creates challenges that regulators must pay attention to. Which medical AI/ML-based products should be reviewed by regulators? What evidence should be required to permit marketing for AI/ML-based software as a medical device (SaMD)? How can we ensure the safety and effectiveness of AI/ML-based SaMD that may change over time as they are applied to new data?[10]

Mobile medical apps

Mobile apps that meet the definition of a medical device must comply with the requirements of EU MDR 2017/745. Many mobile apps are not medical devices, meaning they do not meet the requirement of medical device as defined in the EU.[2] The use of mobile technologies is opening up new and innovative ways to improve health and healthcare delivery. Mobile applications (apps) can help people manage their own health and wellness, promote healthy living, and gain access to useful information when and where they need it. Users include healthcare professionals, consumers, and patients.

The development of mobile medical apps can improve healthcare and provide consumers and health care professionals with valuable health information. As mobile platforms become more user friendly, computationally powerful, and readily available, innovators have begun to develop mobile apps of increasing complexity to leverage the portability that mobile platforms can offer. Some of these new mobile apps are specifically targeted to assist individuals in their own health and wellness management. Other mobile apps are targeted to healthcare providers as tools to improve and facilitate the delivery of patient care.[11,12]

Device regulations focus only on the apps that present a greater risk to patients if they don't work as intended and on apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices. Similar to traditional medical devices, certain mobile medical apps can pose potential risks to public health. Some mobile medical apps may pose risks that are unique to the characteristics of the platform on which the mobile medical app is run.[11,12] An example is the interpretation of radiological images on a mobile device could be adversely affected by the smaller screen size, lower contrast ratio, and any uncontrolled ambient light of the mobile platform.

> Machine-learning algorithms require vast amounts of high-quality training data. However, organisations face a number of barriers limiting their ability to access the data necessary to take advantage of AI effectively.

General Data Privacy Regulation

Data are key aspects of AI/ML. Machine-learning algorithms require vast amounts of high-quality training data. However, organisations face a number of barriers limiting their ability to access the data necessary to take advantage of AI effectively.[13] In May 2018, the EU introduced the General Data Privacy Regulation (GDPR), the new European privacy law.[14] The GDPR creates specific rules for how individuals may access, rectify, transfer, and delete personal data held by third parties. All organisations doing business in the EU must comply with the GDPR, although many have failed to do so.[15] Given AI's heavy reliance on data, the GDPR's rules for data have substantial implications for the development and use of AI, especially applications involving machine learning.[16]

GDPR has created an artificial scarcity of data by making it more difficult for organisations to collect and share data. In addition, it has made it more difficult for companies to use AI applications that automate decision-making regarding individuals using personal information.[14] As a

result, the GDPR has put the EU at a competitive disadvantage in the development and use of AI.

The GDPR generally prohibits organisations from using data for any purposes other than those for which they first collected it. Article 5 requires data be "collected for specified, explicit and legitimate purposes" and that the collected data be "adequate, relevant and limited to what is necessary".[17] These two restrictions – purpose specification and data minimisation – significantly limit organisations' innovation with data by restricting them from both collecting new data before they understand its potential value and reusing existing data for novel purposes. By imposing restrictions on the collection and use of data, the GDPR puts firms in the EU at a competitive disadvantage compared with firms in countries such as China, where companies have access to data on hundreds of millions of internet and mobile phone users.

The GDPR limits how organisations use personal data to make automated decisions about individuals in two ways. Article 22 of the GDPR establishes a right for individuals "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her".[14] This means whenever companies use AI to make a decision about individuals, the data subject has the right to have a human review that decision. This requirement makes it difficult and impractical for companies to use AI to automate many processes because they must develop a process for individuals who opt out of the automated one.[4]

Second, Articles 13–15 require organisations to provide individuals with "meaningful information about the logic involved" in automated decisions. This means firms must be able to explain how an AI system makes decisions that have a significant impact on individuals.[17] While the EU's guidelines have clarified that these requirements do not necessarily require a full disclosure of the algorithm, the information provided should be "sufficiently comprehensive for the data subject to understand the reasons for the decision".[18] This means organisations cannot always comply with requirements to explain the logic involved in an algorithmic decision-making process.[19] And even when companies *can* potentially offer an explanation of the logic involved, they may not be able to do so in a way that is concise and uses plain language, as required by the GDPR. As a result, these regulations will force many businesses to not use certain types of AI systems, especially more sophisticated ones, even when they may be more accurate, safer, and more efficient than the alternatives. Therefore, unless amended, the GDPR is expected to have a negative impact on the development and use of AI in Europe, putting European firms at risk of a competitive disadvantage in the emerging global algorithmic economy.[20]

Cybersecurity

Medical devices will always be subject to vulnerabilities, which cannot be eliminated entirely. From a defensive perspective, manufacturers and developers must take a multi-tiered approach to minimise threats.[7] MDCG 2019-16 Guidance on Cybersecurity for medical devices outlines steps required by developers to reduce/minimise risk to medical devices. The IMDRF has established a companion document to augment the EU guidance.[5]

Cybersecurity vulnerabilities can render medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities.

Cybersecurity vulnerabilities can render medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities. Such occurrences may result in the delay of diagnosis and/or treatment that may lead to patient harm. The need for effective cybersecurity to ensure medical-device functionality and safety has become more important with the increasing use of wireless, Internet- and network-connected devices, portable media, and the frequent electronic exchange of medical device–related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and, in turn, more clinically important.

Cybersecurity guidance by both the IMDRF and EU[5,21] outline procedures to develop medical devices to minimise the threat of attack to these devices. They include strategies for pre-market development including: security requirement, risk management, cybersecurity management plans, labelling, post-market considerations, vulnerability remediation, and incidence response.[2]

Conclusions

Medical devices are increasingly connected to the internet, hospital networks, and other medical devices to provide features that improve healthcare and increase healthcare providers' ability to treat patients. These features also increase the risk of potential cybersecurity threats. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially affecting the safety and effectiveness of the device.

The European Union has implemented guidelines that address what developers and manufacturers of medical devices must do to address safety concerns. While these guidelines directly address concerns of cybersecurity and which types of software can be considered medical devices, these guidelines may impose an undue burden with regard to bringing devices to market in the EU. Restrictions on how personal data may be used for AI algorithm development and requirements for clinical validation, which may be lengthy and costly, could inhibit innovation.

Thus, the developer of software products intended for market in the EU must consider the cost of development against these new guidelines and regulations and determine the least burdensome approach to address them. Furthermore, they must take into consideration global regulations and how best to comply with the different requirements of other regulatory bodies. Therefore, developers may choose to first market new and innovative device first in regions with less-stringent requirements than the EU. Overall, the development of software devices may benefit from a global harmonised set of requirements.

Acknowledgements

I would like to thank all those who have encouraged me over the years: family, friends, colleagues.

Conflicts of interest

The author declares no conflict of interest.

References

1. IMDRF SaMD Working Group. Software as a Medical Device – Key Definitions. 2013. [cited 2020 Aug 6]. Available at: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf
2. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. 2017. [cited 2020 Sept 7]. Available from: http://data.europa.eu/eli/reg/2017/745/oj
3. MDCG 2019-11: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.
4. IMDRF SaMD Working Group. IMDRF/SaMD WG/N23 FINAL: 2015 – Software as a Medical Device (SaMD): Application of Quality Management System. 2015. [cited 2020 Aug 6]. Available at: http://www.imdrf.org/docs/imdrf/final/ technical/imdrf-tech-151002-samd-qms.pdf
5. IMDRF/CYBER WG/N60FINAL:2020: Principle and Practices for Medical Device Cybersecurity [cited 2020 Sept 7). Available at: http://www.imdrf.org/docs/imdrf/final/ technical/imdrf-tech-200318-pp-mdc-n60. pdf
6. Software as a Medical Device Working Group. IMDRF/SaMD WG/N41FINAL: 2017: Software as a Medical Device (SaMD): Clinical Evaluation. 2017. [cited 2020 Aug 6]. Available at: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-170921-samd-n41-clinical-evaluation_1.pdf
7. Medical Device Coordination Group. MDCG 2019-16 Guidance on Cybersecurity for medical devices. 2019. [cited 2020 Aug 6]. Available at: https://ec.europa.eu/docsroom/documents/38924
8. IMDRF/SaMD WG/N12FINAL:2014 - "Software as a medical device": possible framework for risk categorization and corresponding considerations.[cited 2020 Sept 7). Available at: http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf
9. MEDDEV 2.1/6 July 2016 – Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices.
10. Gerke S, Babic B, Evgeniou T, Cohen IG. The need for a system view to regulate artificial intelligence/machine learning-based software as medical device. NPJ Digit Med. 2020;3:53. https://doi.org/10.1038/s41746-020-0262-2
11. When is an app classed as a medical device? Genetic Digital. Mar 2013. [cited 2020 Sep 5]. Available from: http://www.geneticdigital.co.uk/2013/03/when-should-an-app-be-classed-as-a-device/
12. Medicines and Healthcare Products Regulatory Agency. Medical Device Technology Forum on the use of software as a medical device. 2020. [cited 2020 Sep 5]. Available from: http://www.mhra.gov.uk/Howweregulate/NewTechnologiesForums/DevicesNewTechnologyForum/Forums/CON084987
13. Wallace N, Castro D. The impact of the EU's new Data Protection Regulation on AI. Center for Data Innovation. March 2018. [cited 2020 Sep 5]. Available from: https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj
15. International Association of Privacy Professionals and Ernst & Young. Annual Privacy Governance Report 2018. 2018. [cited 2020 Sep 5]. Available from: https://iapp.org/resources/article/iapp-ey-annual-governance-report-2018/
16. Groeneveld K. Four ways how GDPR impacts AI. LinkedIn. 2018 Mar 12. Available from: https://www.linkedin.com/pulse/four-ways-how-gdpr-impacts-ai-kees-groeneveld/
17. Information Commission Office (ICO). Rights related to automated decision-making, including profiling. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/
18. Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679. 2018 Feb 6 [cited 2020 Sep 5]. Available from: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
19. Allen & Overy. Preparing for the General Data Protection Regulation. 2018. Available from: https://www.allenovery.com/en-gb/global/news-and-insights/the-eu-general-data-protection-regulation
20. Koerner K. GDPR – boosting or choking Europe's data economy? Deutsche Bank. 2018 Jun 13. Available from: https://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN-PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000470381
21. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (2019). Available from: https://eur-lex.europa.eu/eli/reg/2019/881/oj

Author information

James W. Monroe, MS, RAC, CQA, is the President and CEO of Global RQC Med Device Solutions, LLC™ , a global medical device consulting firm focusing on regulatory affairs, quality assurance, and regulatory compliance.