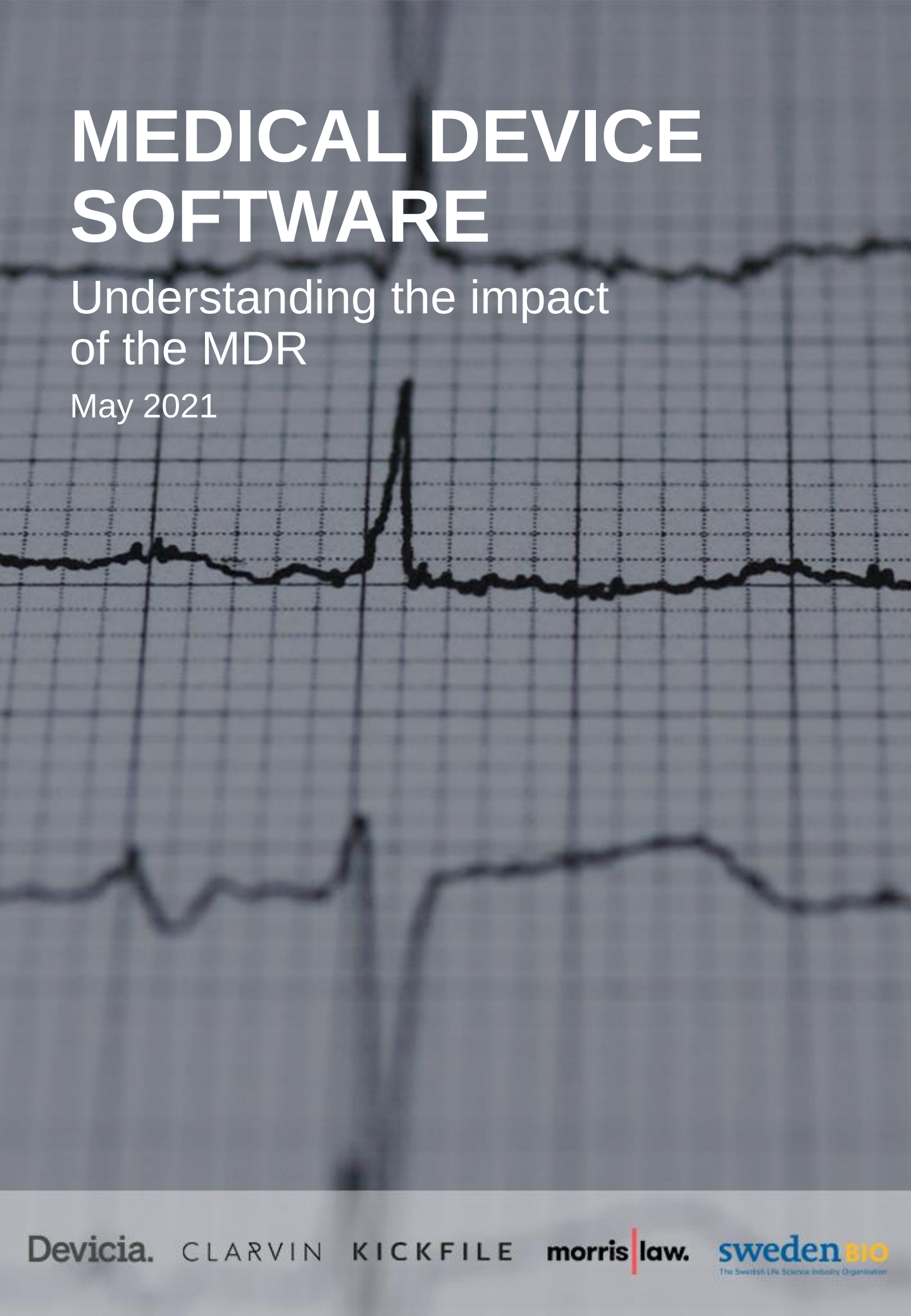


MEDICAL DEVICE SOFTWARE

Understanding the impact of the MDR

May 2021

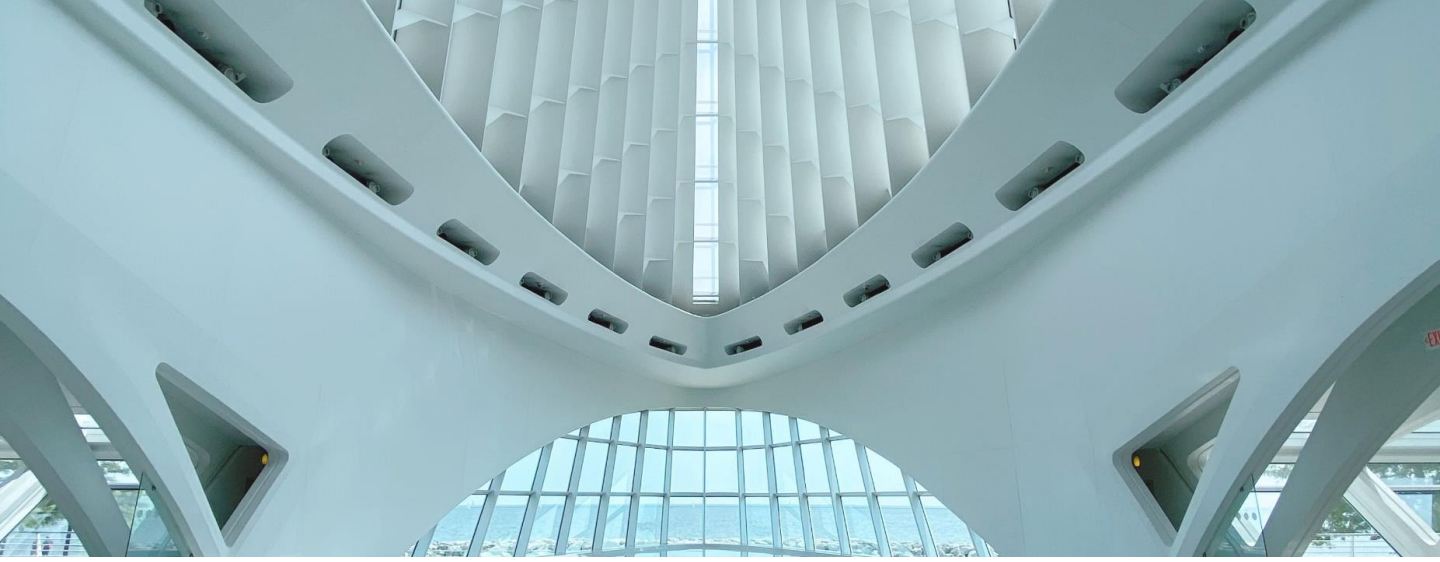
Devicia. CLARVIN KICKFILE morris law. swedenBIO

Introduction

The advancements in technology and digital revolution of the healthcare and medical device industry have created a vast amount of technical solutions, software applications and other software being used for medical purposes. The legal framework regulating medical devices hasn't kept up with the rapid movement and advancements in technology, creating an urgent need for updated regulations, covering critical aspects of development, classification and security of medical device software. The solution on the EU-market was presented in the Regulation (EU) 2017/745 – Medical Devices Regulation ("**MDR**"), with its date of application on May 26, 2021. The upcoming MDR brings changes to concepts, definitions and procedural requirements which affect all players in the medical device industry, particularly the manufacturers of medical device software. This white paper is intended to provide a brief overview of the key impact of the MDR on medical device software ("**MDSW**"). A follow-up white paper will be published during the summer in which clinical evidence requirements for MDSW and related topics will be discussed in detail.

Disclaimer

The information provided in this white paper is the authors' interpretation of the legal framework and shall not constitute legal advice. An individual interpretation must be made in each specific case. Hence, readers are responsible for their interpretation and should assess the impact on their specific medical device(s) and operations.



DEFINITIONS – WHAT IS MDSW?

Under the Medical Device Directive ("**MDD**"), software is considered a medical device if the intended use falls within the scope of the directive, meaning that the software is intended to be used for a medical purpose. The definition of a medical device is more or less maintained with the introduction of the MDR but with some important clarifications and extensions of the scope.

The EU medical device definition has contained the term 'software' since 2009, when it was incorporated following pressure from the Swedish Medical Products Agency. In an attempt to achieve international harmonisation on what software is to be considered as a medical device, the International Medical Device Regulators Forum (IMDRF) introduced the phrase 'software as a medical device' ("**SaMD**"), which 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'. If a hardware medical device needs software to achieve its intended purpose, the software is not SaMD but rather a part of the hardware medical device. The U.S. Food and Drug Administration (FDA) has adopted the term SaMD, whilst in the EU the term 'medical device software' is used instead. The main reason for this is that in the EU, both software that fulfils a medical intended purpose and software intended to drive or influence the use of a hardware medical device is now regulated as MDSW under the MDR. Accordingly, it shall be noted that the term "stand alone software", which was used in the MDD, is no longer used in the MDR. The rationale for the change is that software should be qualified and classified solely based on its intended purpose, regardless of its location.

SaMD = software intended to be used for one or more medical purposes that perform these purposes *without being part of* a hardware medical device (definition introduced by IMDRF and mainly used in the US and previously used under MDD)

MDSW = software that is intended to be used, alone or in combination, that fulfils a medical intended purpose and software intended to drive or influence the use of a hardware medical device (definition used in EU under MDR)

MDR CLASSIFICATION RULES – CLASSIFY YOUR MDSW

Similar to the MDD, the MDR requires that medical devices are classified by application of classification rules. However, in the MDD, there are no classification rules specified explicitly for software. The guidance document MEDDEV 2.1/6 “Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices” states that stand alone software shall be considered an active medical device, which implies that rule 9, 10, 11 and 12 of the MDD classification rules may apply. As of today, under the MDD, the majority of SaMD are classified in class I according to these rules, which means the manufacturer can obtain a CE mark by self-certification without notified body conformity assessment.

Classification rule 11

Along with the date of application of the MDR, new classification rules will be introduced. Mind especially classification rule 11, specified in Annex VIII of the MDR, which reads as follows:

> *“Software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is classified as class IIa, except if such decisions have an impact that may cause:*
>
> • *death or an irreversible deterioration of a person’s state of health, in which case it is in class III; or*
>
> • *a serious deterioration of a person’s state of health or a surgical intervention, in which case it is classified as class IIb.*
>
> *Software intended to monitor physiological processes is classified as class IIa, except if it is intended for monitoring of vital physiological parameters, where the nature of variations of those parameters is such that it could result in immediate danger to the patient, in which case it is classified as class IIb.*
>
> *All other software is classified as class I.”*

Consequently, the majority of MDD SaMD products which previously were class I will now be at least class IIa. Furthermore, this will imply that manufacturers of up-classified software products must comply with additional and stricter requirements, involve a notified body for conformity assessment, and undergo a more rigorous CE marking process. Guidance on the classification of MDSW according to the MDR is provided in the Medical Device Coordination Group (MDCG) guidance document 2019-11[1] on qualification and classification of software. Remember, the MDR requires implementation of a quality management system and technical documentation regardless of classification of the device.

[1] https://ec.europa.eu/docsroom/documents/37581

Grace period for up-classified MDSW

In November 2019, the Council of the European Union published a second amendment to the MDR which introduced a change to Article 120(3). The change means that medical devices classified as class I under the MDD, that will undergo an up-classification under the MDR, will not have to be CE marked in accordance with the MDR by May 26, 2021. Instead, the Declaration of Conformity ("**DoC**") issued under the MDD may remain valid until May 26, 2024 at the latest, allowing manufacturers of up-classified MDSW an additional three years to comply with the requirements and recertify under the MDR. However, the requirements of the MDR relating to post-market surveillance ("**PMS**"), market surveillance, vigilance, and registration of economic operators shall apply in parallel with the corresponding requirements in the MDD.

Significant change

The grace period described above which allows DoCs towards the MDD to be valid until May 26, 2024 is applicable for MDSW under the provision that it does not undergo any significant change. Hence, significant changes in design or intended purpose cannot be made during this period.

The MDCG guidance document 2020-3[2] on significant changes regarding the transitional provision under Article 120 is intended to provide clarification on the changes to a MDSW that should be considered a "significant change in design or a significant change in the intended purpose". Annex C of the guidance is explicitly intended to provide clarification regarding what is considered as a significant change of a MDSW. Still, there are many uncertainties regarding significant changes to MDSW, as software is never finalized in a way that a physical device typically is. Software is generally developed in an agile manner and continuously improved during its life cycle. To determine which changes or updates are considered significant is complex. Manufacturers should therefore be mindful of the updates and improvements made to the MDSW during the grace period. Generally, changes made to eliminate bugs or minor layout changes do not constitute a significant change to a MDSW; whereas changes in the operating system, database structure, modifications in the software architecture or user interface are considered significant.

[2] https:/ec.europa.eu/docsroom/documents/40301/

Stricter requirements on cybersecurity

For manufacturers of MDSW, and for medical devices that incorporate electronic programmable systems, the MDR introduces new requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access. See General Safety and Performance Requirements #17.4, #18.8 and #23.4(ab) in Annex I of the MDR.

The security risk management process has the same elements as the safety risk management process, requiring a security risk management plan, security risk analysis, security risk evaluation, security risk control, evaluation of residual security risk and security risk report. The elements originating from the cybersecurity risk management process may of course be included in the overall safety risk management process documentation for the product.

For further guidance on how to address cybersecurity aspects for medical devices, consult the MDCG guidance document 2019-16[3] on cybersecurity for medical devices. The guidance covers both pre- and post-market aspects of cybersecurity.

Additional requirements related to PMS

The purpose of PMS for any medical device is to collect information on how the product performs 'in the field' and as early as possible detect any risks or problems associated with the device, with the ultimate goal of enhancing patient safety. PMS is intended to be a pro-active and systematic process and should be conducted throughout the lifetime of the product.

The MDR introduces additional requirements related to PMS activities. One example is the requirement for a Periodic Safety Update Report ("**PSUR**") for class IIa, IIb and III devices.

The PSUR shall contain, amongst other things, a risk-benefit determination, main findings from PMCF and sales volumes for the device. The frequency of the PSUR depends on the classification of the device (annually for class III and IIb, every other year for class IIa). The PSUR shall be submitted to the notified body. Although not required to submit a PSUR, class I manufacturers are instead obliged to establish a PMS report which summarizes the results and conclusions from the collected PMS data. The PMS report shall be provided to the authorities upon request.

From a cybersecurity perspective, a solid and effective PMS system is crucial, as vulnerabilities relating to cybersecurity change and evolve over time, meaning that controls that were implemented during pre-market activities may be inadequate to maintain an acceptable benefit-risk level.

[3] https://ec.europa.eu/docsroom/documents/41863

Increased focus on clinical evidence

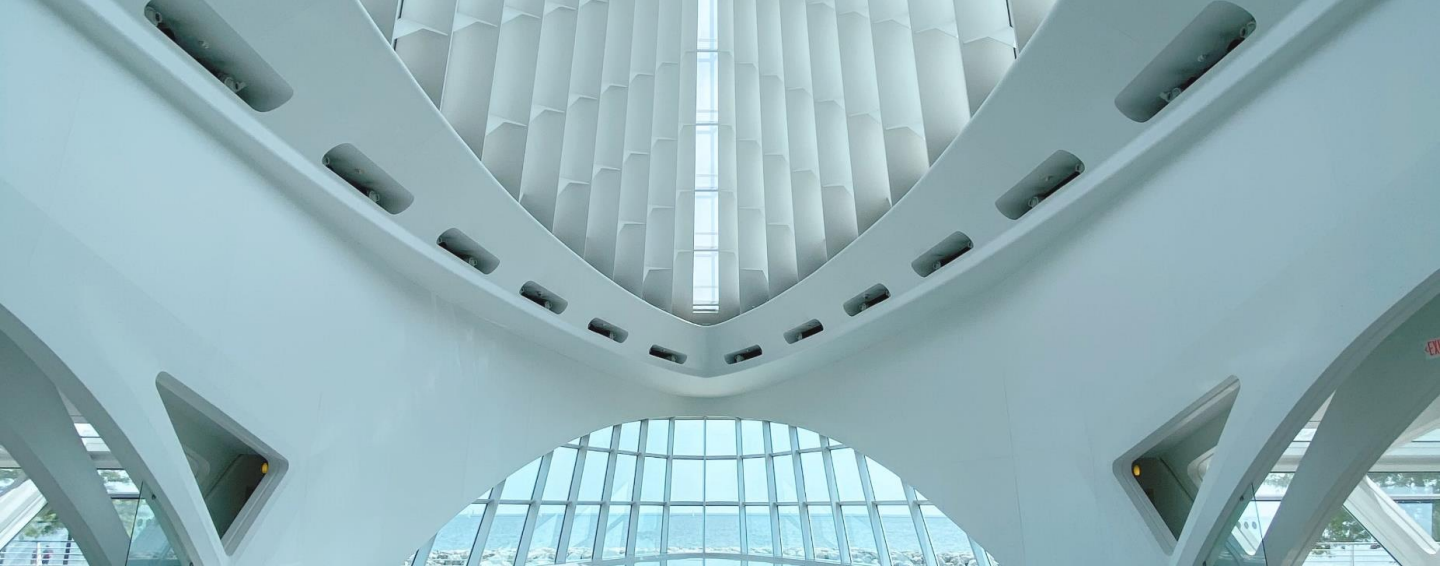
The requirement for a clinical evaluation report for all MDSW is not new under the MDR; however, the introduction of classification rule 11 described earlier means the majority of MDSW will now require a notified body, resulting in the clinical evaluation being scrutinised as part of the notified body's conformity assessment process. This includes assessing the suitability of data from equivalent devices, verifying that the clinical evidence and the clinical evaluation are adequate, and considering the connection between the clinical evaluation and the benefit-risk determination.

The MDR places greater emphasis on clinical evidence to demonstrate conformity with the general safety and performance requirements (GSPRs). To determine the appropriate level of clinical evidence to fulfil the requirements in the MDR for MDSW where the manufacturer claims a medical intended purpose, the MDCG published guidance document 2020-1[4] on clinical evaluation of MDSW. It clarifies that clinical evidence should consist of the three components 'valid clinical association', 'technical performance', and 'clinical performance'.

The requirement to demonstrate clinical performance coupled with reduced possibilities to refer to similar products make the need for more clinical investigations on MDSW apparent. In general, clinical investigations are mandated for new or modified implantable devices and class III devices; however, other products – including MDSW – in other risk classes often also require one or more clinical investigations for demonstration of safety and performance. If a clinical investigation is required, it's critical that the investigation is carried out in accordance with Good Clinical Practice ("**GCP**") (i.e., following the latest version of ISO 14155[5]), the MDR and the Declaration of Helsinki, and with approval from the relevant Competent Authority(ies) and Independent Ethics Committee(s). This being said, the uniqueness of indirect contact between subjects and the MDSW mean justifications for exemptions from elements of GCP may be applicable. In general, it's important that the investigation design and conduct take the differences between MDSW and physical medical devices into consideration.

[4] https://ec.europa.eu/docsroom/documents/40323

[5] Full standard title: ISO 14155:2020 Clinical investigation of medical devices for human subjects – Good clinical practice



Don’t forget EU and local legislation for personal data, patient data and security requirements

In addition to the requirements set out in the MDR, if the MDSW involves protecting or processing of personal data, one or more of the following European legislations could apply in parallel and should be evaluated:

- NIS directive
- GDPR
- EU Cybersecurity Act

Also, local legislation relating to patient safety and patient data (in Sweden: the Patient Safety Act and Patient Data Act) must be carefully considered, integrated and supported through appropriate functions and safety measures.

Considering the impact of significant changes and the stricter CE marking process, with support of clinical documentation and notified body conformity assessment, it’s clear that changing parts of the MDSW relating to security and processing of personal and patient data will result in increased costs and a drawn-out timeline for placing the MDSW on the market. Accordingly, it’s important to ensure that all these requirements are built in as early as possible in the software development process, and that agreements with healthcare providers using the MDSW in treatment of patients or other usage terms for the MDSW clearly reflect the division of responsibilities, data flows and correct appointment of data controller and data processor set-up.

Impact in summary:

1) The definition of MDSW under MDR covers both stand alone software and software intended to drive or influence the use of a hardware medical device.

2) MDR classification rule 11 introduces limits on what type of stand alone software can be classified as class I. The majority of MDD SaMD products which previously were class I will now be at least class IIa. Undertake an assessment of what classification will apply for your MDSW.

3) Medical device software being up-classified under MDR classification rule 11 may benefit from a grace period until May 26, 2024.

4) If a grace period applies to the MDSW, significant changes may not be made to the product during this period.

5) MDR introduces new and stricter requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access.

6) MDR introduces additional requirements related to post-market surveillance activities, for example requirements on Periodic Safety Update Reports for class IIa, IIb and III devices.

7) Classification rule 11 has knock-on effects on clinical evaluation as clinical evidence requirements generally increase with risk class and clinical evaluation reports for non-class I products becoming subject to notified body scrutiny.

8) Increased clinical evidence requirements results in more clinical investigations being carried out for MDSW products. MDR places increased focus on investigation conduct hence all investigations should be carried out in accordance with GCP, the MDR and the Declaration of Helsinki, and with approval from the relevant Competent Authority(ies) and Independent Ethics Committee(s). The uniqueness of indirect contact between subjects and MDSW mean justifications for exemptions from elements of GCP may be applicable.

9) The legal framework for MDSW is complex and involves a number of legislations, not only MDR, to support and secure patient safety and protection of personal and patient data. Make sure that your MDSW is compliant with all applicable EU and local legislation, and that appropriate agreements and terms are put in place to support division of responsibilities.

Sara Berglund Jonsson
QA & RA Consultant - Clarvin AB
+46 722 22 42 32
sara.berglund.jonsson@clarvin.com

Nicole Kvist
QA & RA Consultant – Clarvin AB
+46 722 22 05 85
nicole.kvist@clarvin.com

Elisabeth Liljensten
CEO - Devicia AB
+46 723 61 19 68
elisabeth.liljensten@devicia.com

Sofia Nordgren
CEO - Kickfile AB
+46 725 56 80 59
sofia.nordgren@kickfile.se

Siri Mårtensson Hjälmberg
Partner, Lawyer - Morris Law
+46 701 60 39 53
siri.martensson@morrislaw.se

Karin Odkrans
Associate - Morris Law
+46 708 83 73 46
karin.odkrans@morrislaw.se