European Union (EU) In Vitro Diagnostic Regulation 2017/746 (IVDR) and Cybersecurity

Author: Denise McDermott
Senior Regulatory Compliance Specialist, Compliance & Risks

4 October, 2023

Further regulatory developments may have occurred after publication. To keep up-to-date with the latest compliance news, sign up to our newsletter

European Union (EU) In Vitro Diagnostic Regulation 2017/746 (IVDR) and Cybersecurity

About The Author

Denise McDermott, Senior Regulatory Compliance Specialist, Compliance & Risks

Denise McDermott is a senior regulatory compliance specialist on the Global regulatory compliance team at Compliance & Risks.

Prior to this she worked in the medical device industry for 13 years across a number of areas including regulatory affairs, post-market surveillance, customer complaints, quality, and technical support.

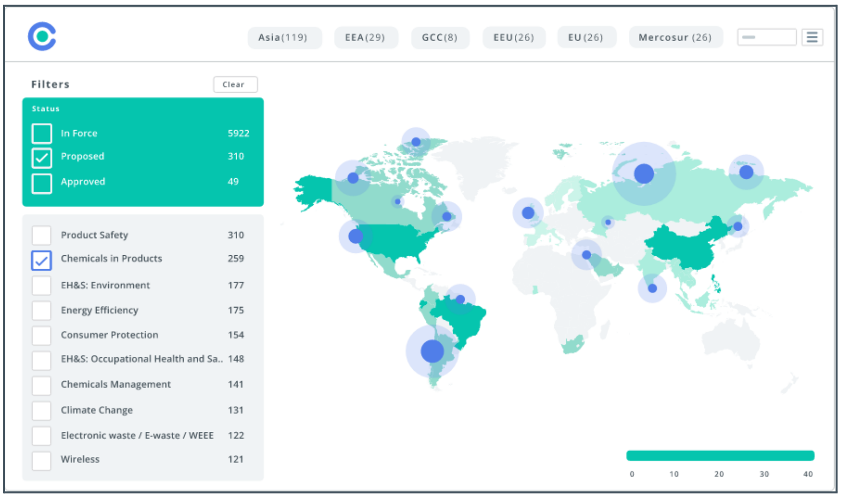
She has experience in several areas including IVDR, CE marking, labeling, customer and quality technical communications and regulatory risk assessments. Denise holds an honours degree in biochemistry and a Ph.D. in cancer biology.

Unlocking Market Access

At Compliance & Risks, we help you keep on top of global regulatory changes and their impact worldwide. We have the right technology, regulatory content and expertise to help you unlock market access, protect revenue and elevate the role of compliance.

Our Solution includes:

- C2P: The most advanced product compliance and ESG compliance software on the market, helping you streamline your compliance process and unlock market access around the world.
- Regulatory Content: We provide the broadest and most comprehensive product compliance regulatory content on the market, monitoring 195+ countries, 20 industry sectors, 42 topics and 87,000+ regulatory sources.
- Ask our Experts: Direct access to our team of experts for support



Filters

Status

□	In Force	5922
☑	Proposed	310
□	Approved	49

□	Product Safety	310
☑	Chemicals in Products	259
□	EH&S: Environment	177
□	Energy Efficiency	175
□	Consumer Protection	154
□	EH&S: Occupational Health and Sa..	148
□	Chemicals Management	141
□	Climate Change	131
□	Electronic waste / E-waste / WEEE	122
□	Wireless	121

Additionally, we offer:

- Market Access Services: Our Market Access team helps you understand your product compliance obligations by transforming regulations into actionable knowledge with tailored advice for you and your business.

Why choose C2P?

- Stay ahead of regulatory changes with the world's most comprehensive regulatory database

- Avoid delays with alerts of changes to regulations & requirements in real time
- Improve efficiency with powerful collaboration and workflow tools to keep compliance evidence up-to-date & live linked back to Regulations, Standards & Requirements

Contact us to speak to one of our team today to learn how you can simplify your regulatory compliance process.

For more information, please visit www.complianceandrisks.com

Important Notice: All information provided by Compliance & Risks Limited and its contributing researchers in this report is provided for strategic and informational purposes only and should not be construed as company-specific legal compliance advice or counsel. Compliance & Risks Limited makes no representation whatsoever about the suitability of the information and services contained herein for resolving any question of law. Compliance & Risks Limited does not provide any legal services.

1. Introduction

The European Union (EU) In Vitro Diagnostic Regulation 2017/746[1] (IVDR), became applicable on 26 May 2022 and introduced important changes to the regulation of in vitro diagnostic medical devices (IVDs) across the EU.

The regulations set out conditions for maintaining high safety standards for IVDs, while taking into account potential technological progress into the future. In that regard, the new regulations include requirements for software placed on the EU market, and apply stringent rules around clinical evidence and post-market surveillance.

As per the IVDR, an “in vitro diagnostic medical device means any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, **software or system**, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:

A. Concerning a physiological or pathological process or state;
B. Concerning congenital physical or mental impairment;
C. Concerning the predisposition to a medical condition or a disease;
D. To determine the safety and compatibility with potential recipients;
E. To predict treatment response or reactions;
F. To define or monitoring therapeutic measure.”

Requirements in the IVDR surrounding devices that incorporate electronic programmable systems and software are crucial to prevent attacks on medical devices that ultimately harm the patient, with potentially fatal consequences. Therefore cybersecurity risks must be effectively minimized or managed and requirements must be adhered to in order to prevent harm. In order to ensure safe and secure medical devices, manufacturers must consider security throughout the lifecycle of a device, from secure development to security risk management processes, verification and validation as well as a security post market processes.

While technological advances in the medical device field bring a host of new opportunities for improved patient care, it is also imperative to consider any data privacy challenges that may occur. Sensitive patient data may be transmitted or stored, and this information must be protected. Failure to comply with such regulations can have dire consequences. Many challenges lie ahead for IVDR, however it is imperative for all involved, that a high level of safety and performance is maintained, and that supply of essential devices is effectively sustained.

2. EU In Vitro Diagnostic Regulation 2017/746 (IVDR) and Cybersecurity

Among the new aspects introduced by IVDR, there is now a focus on ensuring that devices placed on the EU market are fit for the new technological challenges linked to cybersecurity risks.

In terms of cybersecurity provisions, the IVDR covers requirements relating to risks associated with any potentially negative interaction between software and the IT environment within which it operates. It covers requirements for post-market surveillance systems for devices including software, that meet the definition of an in vitro diagnostic medical device. The IVDR states that "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."

Cybersecurity requirements listed in Annex I of the IVDR, deal with both premarket and post-market aspects. Annex I, section 13.1. states that if "the device is intended for use in combination with other devices or equipment, the whole combination, including the connection system, shall be safe and shall not impair the specified performances of the devices. Any restrictions on use applying to such combinations shall be indicated on the label and/or in the instructions for use." The interaction between the software and the IT environment is described in section 13.2.d, while interoperability and compatibility with other devices or products is outlined in section 13.5, which states; "Devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the interoperability and compatibility are reliable and safe."

Section 16 of Annex I of the IVDR on electronic programmable systems, describe requirements for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, and states that they 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."

As per section 16.1 on repeatability, reliability and performance, devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, must be designed with these features in mind. Manufacturers are also required to describe the minimum requirements for IT security measures including protection against illegal access. The manufacturer should also be aware of provisions related to post-market surveillance in the IVDR in the context of cybersecurity for example, post-market surveillance per article 78, vigilance per article 82 and trend reporting per article 83. Overall, the manufacturer should manage cybersecurity across the entire life cycle of a medical device.

3. Medical Device Coordination Group (MDCG) Guidance Documents on Medical Device Cybersecurity

Medical Device Coordination Group (MDCG) documents provide valuable guidance on cybersecurity requirements for IVDs, in particular MDCG 2019-16[2] and MDCG 2020-1[3] with guidance on qualification and classification of software found in MDCG 2019-11[4].

MDCG 2019-16 was published with the aim of providing manufacturers with guidance on how to fulfil all the relevant essential requirements of Annex I to the MDR and IVDR with regard to cybersecurity. It describes requirements and basic cybersecurity concepts, and also covers secure design and manufacture, documentation and instructions for use, post market surveillance and vigilance. Annex I of MDCG 2019-16 describes mapping of IT security requirements to NIS Directive Cooperation Group measures, while Annex II gives several examples of cybersecurity incidents/serious incidents. Annex III lists standards which may be considered, including EN ISO 14971 Risk management, EN 62304 Software life cycle, EN ISO/IEC 27000 and EN ISO/IEC 27001 on Information technology, IEC 62443-4-2 Security for industrial automation and control systems, IEC 82304-1 Health Software and IEC/TR 60601-4-5 Medical electrical equipment-Part 4-5 Safety related technical security specifications for medical devices, among others. Annex IV provides a figure illustrating the relationship between processes for cybersecurity risk management and safety risk management.

MDCG 2020-1 covers guidance on clinical evaluation (MDR) and performance evaluation (IVDR) of medical device software. It offers guidance on the clinical evidence required for medical device software (MDSW) as per the MDR and IVDR. As per this guidance, “MDSW 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”. On the other hand, as per MDCG 2019-11, software driving or influencing the use of a medical device may be qualified as an accessory for a medical device. MDCG 2019-11 should be consulted for guidance on the appropriate qualification and classification of software. As per Article 56 (1) of the IVDR; “The manufacturer shall specify and justify the level of clinical evidence necessary to demonstrate conformity with the relevant general safety and performance requirements." Software which is an IVD must conform with the same performance evaluation requirements as other IVDs including the generation of a performance evaluation plan, generation of clinical evidence, demonstration of conformity with the relevant general safety and performance requirements (GSPRs); performance evaluation report and continuous update of documentation throughout its life cycle. To offer further guidance, Annex I of MDCG 2020-1 covers the methodological principles for generation of clinical evidence and Annex II includes examples of performance evaluation strategies.

4. International Medical Device Regulators Forum Documents on Medical Device Cybersecurity

The International Medical Device Regulators Forum has published several documents regarding cybersecurity in medical devices including Principles and Practices for Medical Device Cybersecurity, published in 2020[5], and Principles and Practices for the Cybersecurity of Legacy Medical Devices[6] and Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity, both published in 2023[7].

Principles and Practices for Medical Device Cybersecurity describes best practices for medical device cybersecurity, including IVDs. It covers medical devices that contain software, as well as software as a medical device (SaMD). SaMD is a term used by the IMDRF for software intended for one or more medical purposes that perform those purposes without being part of a hardware medical device. The document provides an overview of the general principles of medical device cybersecurity, as well as recommendations regarding best practices in the pre-market and post-market management of medical device cybersecurity.

Principles and Practices for the Cybersecurity of Legacy Medical Devices is complementary to Principles and Practices for Medical Device Cybersecurity and considers cybersecurity in the context of legacy medical devices that either contain software or exist as software only. Specifically, this document describes legacy medical device cybersecurity within the context of the total product life cycle and provides recommendations for medical device manufacturers and healthcare providers in communication and risk management as well as recommendations for the application of cybersecurity in legacy devices.

Finally, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity provides recommendations on the implementation of a software bill of materials (SBOM) and covers cybersecurity concerns relevant to the SBOM. It is again complementary to Principles and Practices for Medical Device Cybersecurity. The SBOM is a list of all of the software components included in a medical device along with associated information, and can help mitigate against the potential for patient harm caused by cybersecurity issues. This guidance document provides recommendations for medical device manufacturers in SBOM generation, management, and distribution. This document does not address SBOM-related recommendations related to cloud services, but they may be considered in future documents.

5. EU Legislation on Cybersecurity and Data Protection

While the IVDR is the principal means of ensuring safe, effective and cybersecure IVDs, the medical device industry must also be aware of additional EU legislation outside of the medical devices regulations which may impact cybersecurity. These include laws surrounding data protection as well as international standards and regulations on cybersecurity.

The NIS2 Directive[8], whose aim is to achieve a high level of cybersecurity across the Union, includes a range of cybersecurity requirements across the entirety of a medical device's lifecycle. Included in Annex I of the NIS2 Directive, under sectors of high criticality, are EU reference laboratories and medical devices considered to be critical during a public health emergency, while manufacturers of medical devices and in vitro diagnostic medical devices are listed in Annex II. All impacted entities must now "take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems.” Stringent security and incident reporting requirements have been introduced and entities are required to manage cyber risks, and report significant cyber incidents to national authorities within 24 hours of becoming aware. Member States have until 17 October 2024 to adopt and publish the measures necessary to comply with this Directive. The new laws shall apply from 18 October 2024.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, General Data Protection Regulation (GDPR)[9], is not specific to medical devices but covers patient health information and therefore must be taken into consideration by manufacturers of medical devices or medical software that deal with patient data. Medical devices and especially software often store and process personal health data, as defined in the GDPR. As per Article 9 on processing of special categories of personal data; “1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.” Therefore, if a medical device or medical device software collects personal data, GDPR compliance is required.

6. Conclusion

The IVDR is now in effect, and while its implementation is an important step in guaranteeing safe and effective IVDs, it has also highlighted certain challenges for all involved.

Many concerns remain, including those surrounding cybersecurity risks of new devices on the European market. Cyber-attacks and personal data leaks can have significant impact, leading to revenue loss and most significantly, potential patient harm.

It is therefore imperative that IVD manufacturers integrate cybersecurity considerations into their design and development processes and perform vulnerability assessments throughout the product's lifecycle. It is also critical to consider the impact of data privacy laws and regulations on device development. Companies that fail to comply with data privacy and cybersecurity laws may face serious consequences, highlighting the importance of prioritizing compliance with these important regulations.

7. References

1. Regulation (EU) 2017/746 of the European Parliament and of the council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU
2. MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices
3. MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software
4. MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR
5. Principles and Practices for Medical Device Cybersecurity, 2020
6. Principles and Practices for the Cybersecurity of Legacy Medical Devices, 2023
7. Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity, 2023
8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

9. 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)