Data Act and Medical Devices: data interoperability or regulatory risk?

In recent years, medical devices have become increasingly connected, interoperable and data-dependent. Wearables, remote monitoring systems, cloud platforms and medical software generate large volumes of clinical and technical information every day, creating new opportunities for innovation and for the digital transformation of healthcare.

Against this backdrop, **Regulation (EU) 2023/2854**, better known as the **Data Act**, forms part of the broader European strategy aimed at promoting the circulation and value creation of data within the digital single market.

Interest in this Regulation is set to increase further in the coming months. **12 September 2026** will be a particularly important date for manufacturers of connected devices, as from that point the **obligations under Article 3** of the Data Act concerning the accessibility of data generated by connected products and related services will begin to apply.

In the medical device sector, however, the issue is not limited to data availability. Making a device "*data accessible*" may require software changes, updates to communication architectures, the introduction of new APIs or a review of cybersecurity mechanisms. And in the MDR context, where software directly contributes to the safety and clinical performance of the device, such changes may have non-negligible regulatory relevance.

This article therefore examines the relationship between the Data Act and the MDR, highlighting the main areas of overlap and the potential design and regulatory implications for manufacturers of connected medical devices.

The Data Act: why it was introduced and what it brings

In recent years, the European Union has launched a broad regulatory strategy to support the creation of a single market for data. The objective is to promote innovation, interoperability and competitiveness by facilitating access to, and reuse of, information generated by digital products and services.

In many sectors, large volumes of data are generated every day by connected devices, yet they often remain in practice under the exclusive control of manufacturers or digital platform providers. This limits the ability of users, companies and organisations to use that information to develop new services, integrate different technological solutions or foster innovation.

It is precisely in this context that the Data Act was introduced, published on 13 December 2023 as part of the broader *European Data Strategy*.

The Regulation mainly applies to so-called **connected products** and their related services, meaning products capable of collecting, generating or transmitting data through electronic communications. In other words, a large part of the IoT ecosystem (*Internet of Things*), which today includes not only consumer and industrial devices, but also many connected medical devices.

The core of the Data Act concerns the accessibility of data generated by those products. The Regulation introduces specific obligations to ensure that such data can be made available to users in a simple, secure and interoperable manner.

To better understand how the Regulation works, it is useful to introduce some of the main roles defined in Article 2:

- **User**: the person or entity that uses a connected product or related service;
- **Data Holder**: the person or entity that has the right or obligation to make available the data generated by the product or service;
- **Data Recipient**: the third party to whom the data is transferred at the user's request.

Once these roles are defined, the principle underlying the Data Act can be summarised as follows: data generated through the use of connected products must not remain confined within manufacturers' platforms; instead, the Data Holder must ensure access to the User or to the Data Recipient designated by the User, in accordance with the procedures set out in the Regulation.

For this purpose, Article 3 introduces design obligations requiring connected products to be built so that data is accessible by default, while Article 4 governs users' right to access and use such data, including through third parties designated by them.

The effect of the Data Act on medical devices

The application of the Data Act is not limited to traditional consumer or industrial IoT devices. The Regulation also affects the healthcare sector and, more specifically, connected medical devices.

This reference is made explicit in Recital 14 of the Regulation, where medical and health devices are included among the examples of connected products falling within the scope of the Data Act:

"*Connected products are found in all aspects of the economy and society, including [...] medical and health devices [...].*"

This is a particularly relevant point when considering the technological evolution currently taking place in the medical sector. Today, many medical devices are designed to collect, process and transmit data in real time through cloud platforms, mobile applications or connected hospital infrastructures.

Common examples include:

- remote patient monitoring devices;

- medical wearables;
- connected diagnostic systems;
- smart infusion pumps;
- medical software integrated with cloud services.

In this scenario, data generated by the device has central value not only from a clinical standpoint, but also from a technological and operational perspective. Making that data accessible to users or to designated third parties, as required by the Data Act, may therefore require direct intervention on the software architecture and communication mechanisms of the device itself.

This is precisely where the point of contact with the MDR emerges.

In the medical device sector, software is not a mere ancillary component; it often constitutes an essential element for ensuring safety, clinical performance and risk management. As a result, changes introduced to meet the data accessibility requirements laid down by the Data Act may also have significant regulatory relevance from an MDR perspective.

Overlap with the MDR

Probably the most relevant aspect of the Data Act for medical device manufacturers concerns the design obligations introduced by Article 3 of the Regulation.

The provision states that connected products must be designed and manufactured in such a way that the data generated by their use, including the metadata necessary to interpret them, is accessible to the user in a simple, secure and free-of-charge manner, and in a machine-readable format.

In other words, the Data Act introduces an approach that could be described as "**data accessibility by design**": data accessibility is no longer treated as an optional feature, but as a requirement to be taken into account from the product design stage.

In the context of connected medical devices, this could translate into the need to:

- introduce new APIs or data export interfaces;
- modify device software or firmware;
- update communication architectures;
- implement new authentication and access management mechanisms;
- review interoperability arrangements with external platforms or cloud services.

In the medical sector, however, these interventions are not simply IT changes.

The MDR regards software as an integral part of a medical device when it contributes to the device's performance, patient safety or risk management. Consequently, changes introduced to comply with Data Act obligations could have a direct impact on the device's regulatory profile.

For example, the introduction of new data access functionalities could affect:

- the integrity of medical software;
- device cybersecurity;
- access management;
- data confidentiality and availability;
- the system's operational behaviour;
- the risk analysis performed under ISO 14971.

In some cases, such changes could even qualify as "*significant changes*" under the MDR, requiring a regulatory reassessment and the possible involvement of the Notified Body.

It is at this point that one of the main areas of overlap between the Data Act and the MDR becomes apparent. On the one hand, the Data Act promotes greater accessibility, interoperability and data sharing; on the other, the medical device regulatory framework imposes strict requirements in terms of safety, cybersecurity, software integrity and change control.

For manufacturers of connected medical devices, the challenge will therefore be to strike a balance between these apparently competing needs: making data more accessible without compromising the device's safety, clinical performance and regulatory compliance.

Implications for manufacturers

In light of these considerations, alignment with the Data Act should not be approached solely as a matter of data access or documentary compliance.

For manufacturers of connected medical devices, the new obligations introduced by the Regulation may have direct impacts on software architecture, cybersecurity, risk management and, more broadly, the entire device lifecycle.

For this reason, analysis of the requirements laid down by the Data Act will most likely require a multidisciplinary approach capable of involving, at the same time:

- regulatory professionals;
- software and cybersecurity teams;
- risk management specialists;
- quality managers;
- designers of interoperable systems.

In many cases, it will be necessary to carefully assess whether the technical solutions adopted to ensure data accessibility may affect elements already covered by MDR documentation, such as:

- software architecture;

- risk analysis;
- cybersecurity requirements;
- interoperability;
- software validation;
- device performance.

This aspect may become particularly relevant for manufacturers of legacy devices or for products already placed on the market, where updates aimed at alignment with the Data Act may require additional regulatory assessments.

In this context, preliminary activities such as technical and regulatory gap assessments, data architecture analyses and preventive evaluations of MDR impact could play an increasingly strategic role from the early stages of update design and planning.

Conclusion

The entry into application of the obligations laid down by the Data Act will represent an important step for the entire ecosystem of connected products and, consequently, also for the medical device sector.

In the medical context, however, data accessibility cannot be viewed solely as a question of interoperability or data valorisation. The changes required to make a device compliant with the Data Act may have direct impacts on software, cybersecurity, risk management and MDR compliance.

For this reason, the relationship between the Data Act and medical devices should not be interpreted as a simple regulatory overlap, but as a new design and regulatory scenario that will require manufacturers to adopt an increasingly integrated approach between technology development, risk management and compliance.

The real challenge in the coming years will probably be precisely this: enabling greater accessibility and circulation of data without compromising safety, clinical reliability and patient protection.

With the 12 September 2026 deadline approaching, for many manufacturers of connected medical devices this may be the right time to start assessing the concrete impact of the Data Act on their products, software architectures and regulatory change management processes.

Sources:

1. *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act),* *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32023R2854* .

2. *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices (Medical Device Regulation - MDR), https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32017R0745*

Keywords: Data Act, MDR, data interoperability, connected medical devices, digital health compliance

Author: Antonio Cancilla, R&D Product Specialist