MASON HAYES & CURRAN

ISSUE 7, JANUARY 2026

# Digital Health

## Annual Review 2025

Dublin London New York San Francisco

MHC.ie

MASON HAYES & CURRAN

# *Welcome*
# Digital Health Annual Review 2025

2025 has proven to be another landmark year for Digital Health regulatory developments leading to continued uncertainty and new challenges for stakeholders working to adapt their business systems to keep pace with what is still a dynamic and evolving regulatory landscape in the EU.

While 2025 was a year full of significant developments, 2026 is now set to be a year of continuing challenge for stakeholders striving to ensure compliance in an evolving regulatory landscape that is itself changing to accommodate increasingly novel and innovative products and business models. In this edition of our Annual Digital Health Review, we cover various key legal developments from the last year:

- The future obligations which the European Health Data Space Regulation will impose on digital health businesses and how best to prepare.
- The EU Commission's guidelines to assist in defining an AI system under the AI Act.
- The impact of a recent Court of Justice of the EU decision interpreting the concept of 'telemedicine'.
- The key implications of the NIS2 Directive on the life sciences sector and the resulting challenges for businesses in managing and enhancing their cyber security systems into the future.
- The EU Commission's landmark proposal for reform of the Medical Device and In Vitro Diagnostic Device Regulations.

As we enter 2026, we cover these issues and much more with the aim of providing a useful reference for stakeholders navigating an increasingly sophisticated EU Digital Health regulatory landscape. We hope you enjoy this latest edition of our Annual Digital Health Review.

## EDITORS


MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie


Michaela is Head of Life Sciences. She advises clients in the pharmaceutical, healthcare, medical device, digital health, cosmetic, video game, software and general consumer products sectors on various regulatory compliance matters. Michaela has particular expertise in wearables and software medical devices. She frequently advises clients on applicable regulatory frameworks, regulatory approvals, labelling, packaging, traceability, safety and liability issues. Michaela also represents manufacturers in product liability claims and enforcement action by regulators.


JAMIE GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie


Jamie is a Partner in the Life Sciences team. He advises a variety of international clients in the life sciences, consumer products and technology sectors on the application of domestic and EU regulatory regimes throughout the life cycles of their products. He regularly advises clients on matters such as the applicability of regulatory frameworks, regulatory approval, labelling, packaging, traceability, recalls, safety and liability.


BRIAN MCELLIGOTT
*Partner, Head of Artificial Intelligence*
brianmcelligott@mhc.ie


Brian is Head of our Artificial Intelligence (AI) team. Brian re-joined us in January of 2023 having spent time in-house as Chief Intellectual Property counsel with an Irish AI fintech start-up. During that time, he gained significant experience in operationalising and commercialising AI platforms and solutions. He led AI invention harvesting and international patent and trademark portfolio filing projects. He was also part of a team that conceived and developed a bespoke inhouse software invention and R&D tagging tool that has applications in the trade secret space.

# Contents

*Latest Digital Health insights from our Team*

01

# European Health Data Space

*Preparing for secondary use obligations*

BRIAN JOHNSTON
*Partner, Data & Technology*
bjohnston@mhc.ie

The European Health Data Space Regulation (EHDS) is a significant piece of legislation. We have previously written about how the EHDS is "a major step forward in digital healthcare".

In this article, we examine the secondary use provisions contained in the EHDS, which will significantly affect how digital health businesses will need to share valuable data for research, innovation and public interest uses with third parties.

Most of these provisions will not take effect until 2029. However, compliance will require very substantial investment by businesses, meaning preparation should begin now.

## What data is in scope?

EHDS sets out an extensive list of electronic health data categories that health data holders must make available for secondary use through health data access bodies. Categories of relevant data include, among other things:

- Electronic health data from electronic health records
- Aggregated data on healthcare needs, resources allocated to healthcare, the provision of and access to healthcare, healthcare expenditure and financing
- Healthcare-related administrative data, including on dispensations, reimbursement claims and reimbursements
- Personal electronic health data automatically generated through medical devices
- Data from wellness applications
- Data from clinical trials
- Other health data from medical devices
- Data from research cohorts, questionnaires and surveys related to health, after the first publication of the related results, and
- Health data from biobanks and associated databases

Member States may also provide in their national law that additional categories of electronic health data are to be made available.

Given the value of the data potentially in scope, and the impact of that data being treated as subject to the EHDS secondary-use provisions, businesses need to take particular care in identifying and classifying what is and is not captured. The classification exercise is a critical task in preparing for EHDS compliance.

## How is data shared and facilitated?

Sharing of data will be facilitated by dedicated bodies set up under the EHDS, called health data access bodies. Health data access bodies will be responsible for considering requests for data and issuing permits to third parties, called health data users. Health data holders will have a limited ability to prevent this highly valuable data from being made available.

The health data holder must communicate to the health data access body a description of the dataset it holds. At a minimum on an annual basis, this must be checked to ensure it is accurate and up to date. Health data access bodies must make available publicly a description of the available datasets and their characteristics.

This should include information concerning the source, scope, main characteristics, and nature of the electronic health data in the dataset and the conditions for making the data available. This will enable health data users to request relevant data.

On request, health data holders must make relevant data available to the health data access body within a reasonable time period, i.e. no later than three months, which can be extended by a further three months, if required.

Requests for data cannot be made to:

- Take decisions detrimental to individuals based on their electronic health data
- Taking decisions regarding individuals in the context of job offers, offering less favourable terms in the provision of goods or services, or which result in discrimination against them
- Carrying out advertising or marketing activities
- Developing products or services that may harm individuals, public health or society at large, and
- Carrying out activities in conflict with ethical provisions

This affords health data users with very significant scope to access and use data for their own commercial purposes.

Businesses should have rigorous processes in place to ensure health data access bodies are properly assessing applications for data from health data users, that all the necessary conditions are met, and that any invalid requests are being challenged appropriately.

### What format does data need to be in?

The EHDS provides that data must be shared with health data access bodies in standardised, interoperable, machine-readable formats.

The European Commission will set out the technical formats in implementing acts, likely referencing EU-recognised standards like HL7 FHIR, SNOMED CT, ICD or LOINC. These must be adopted before 2029, so businesses should monitor for developments between 2026 and 2028. Aligning systems and records with these standards will be a very significant undertaking. Businesses will need to update their infrastructure to meet EHDS requirements and ensure interoperability.

### What exceptions apply?

The exceptions available to health data holders are relatively limited, given the nature of the data. Even if data is protected by intellectual property rights or trade secrets, it cannot necessarily be withheld by the health data holder.

Health data holders may only refuse to disclose if doing so would cause serious harm to trade secrets and where no safeguards could sufficiently mitigate the risk. If data requested falls into this category, it is for the health data holders to bring this to the attention of health data access bodies dealing with the request.

To maximise their chances of protecting their data, businesses should:

- Identify and classify datasets containing trade secrets or intellectual property
- Document the concrete commercial harm caused by disclosure
- Prescribe the necessary confidentiality safeguards that need to be in-place before access can be granted, and
- Establish an internal escalation and objection workflow in case requests for protected data are received

### Can a fee be charged?

The EHDS seeks to eliminate charges that could be a barrier to the flow of data.

Health data access bodies may charge fees for making electronic health data available for secondary use. The fees should be in proportion to the cost of making the data available and they shall not restrict competition. The fees charged may include compensation for the costs incurred by the health data holder for compiling and preparing the electronic health data to be made available for secondary use, provided the holder has provided an estimate for these costs.

Licensing fees cannot be charged and there is no ability to be compensated for the use of trade secrets and intellectual property.

Health data holders should be ready to explain the costs involved in facilitating any request and be able to defend and justify these costs.

### What action to take now?

EDHS represents a very substantial change to the way in which digital health businesses will need to make available very valuable data. While obligations will not apply until 2029, being in a position to achieve compliance while strongly protecting your organisation's rights will require multi-year preparation.

Businesses should start to consider the following steps:

- Map all datasets and distinguish clearly between data that is and out of scope of EHDS secondary use provisions
- Prepare to provide health data access bodies with the necessary detailed descriptions of in-scope data
- Assess current standards and formats ahead of implementing acts to be adopted by the European Commission
- Develop a robust trade secret and intellectual property protection framework to defend interests when data is requested
- Establish measures to ensure maximum cost recovery when requests are compiled with

02

# Defining AI

## *Commission guidelines on AI systems*

BRIAN MCELLIGOTT
*Partner, Head of Artificial Intelligence*
brianmcelligott@mhc.ie

SADHBH MURPHY
*Associate, Data & Technology*
sadhbhmurphy@mhc.ie

The EU Commission published their much anticipated guidelines on the definition of an artificial intelligence system on 6 February 2025. The guidelines explain how the legally defined term *"artificial intelligence system"* is applied in practice.

In particular, the guidelines aim to assist providers in determining whether a software system constitutes an AI system.

In this article, we provide an overview of the guidelines.

### WHAT YOU NEED TO KNOW

- The EU Commission published non-binding guidelines on how to interpret the definition of an AI system under the AI Act on 6 February 2025
- The definition is broken into seven elements, including autonomy, inference, and the ability to influence environments, highlighting inference as an important aspect
- Techniques such as machine learning, and logic and knowledge based approaches are in scope, while techniques such as basic data processing and simple prediction systems are out of scope
- The guidelines recommend first classifying an AI system in accordance with its risk category under the AI Act to determine if it is out of scope, before considering whether it meets the definition of an AI system

### Scope of application

The guidelines specifically state that they are designed as a guide only and do not provide an exhaustive list of all AI systems that may be covered. They are not legally binding, and any authoritative interpretation of the AI Act can ultimately only be provided by the Court of Justice of the European Union.

### Breaking out the definition

Essentially, the guidelines break down the definition into its seven main elements and provide detailed explanations for each. The seven elements are that the system is:

1. *a machine-based system;*
2. *that is designed to operate with varying levels of autonomy;*
3. *that may exhibit adaptiveness after deployment;*
4. *and that, for explicit or implicit objectives;*
5. *infers, from the input it receives, how to generate outputs;*
6. *such as predictions, content, recommendations, or decisions;*
7. *that can influence physical or virtual environments.*

### Pre and post-deployment included

Importantly, the guidelines note that the definition adopts a lifecycle-based perspective encompassing two main phases:

1. The pre-deployment or 'building' phase of the system, and
2. The post-deployment or 'use' phase of the system, referencing a recent OECD paper[1] on the same topic

This approach is highlighted to clarify that the seven elements of the definition are not required to be present continuously throughout both phases of that lifecycle. Instead, the definition acknowledges that specific elements may appear at one phase, but may not persist across both phases. This is an important point for those looking to make precise scoping arguments. It reflects a means of analysis deployed in recent data protection supervisory authority guidelines.

### In-scope and out-of-scope

Prior to the guidelines' publication, most commentators focused on two or three crucial aspects of the definition that go to the heart of what does and does not constitute an AI system. The most important aspects were seen as autonomy and inference, with many also including adaptiveness.

Reading between the lines, it seems the Commission has zoned in on inference as the key aspect of the definition. Almost six of the thirteen pages of the guidelines are devoted to this topic and the majority of the guidelines focus on listing the AI techniques that fall within the scope of the definition. It also outlines techniques that may fall outside the scope, such as comparing AI software with simple execution or rules-based software.

### In-scope techniques are:

1. Machine learning approaches including:
   - Supervised learning
   - Unsupervised learning
   - Self-supervised learning
   - Reinforcement learning
   - Deep learning
2. Logic and knowledge based approaches including:
   - Knowledge representation
   - Inductive (logic) programming knowledge bases
   - Inference and deductive engines
   - Symbolic reasoning
   - Expert systems, and
   - Search and optimisation methods

### Out-of-scope techniques are:

- Systems for improving mathematical optimisation, including linear or logistic regression methods
- Basic data processing
- Systems based on classical heuristics, and
- Simple prediction systems

### How to use these guidelines

In the final section, the guidelines explain how they should be used when determining whether a system is considered an AI system under the AI Act. According to the guidelines, this assessment should be based on the specific design and function of the system taking into account the seven key elements of the definition.

In our view, the guidelines are most helpful to those with AI systems that are founded on a technique specifically identified as out-of-scope, or those who have a very specific query on scope. Organisations looking to make a quick big picture call on "*in v out of scope*" of the AI Act are not best served by beginning with assessing their technology against these guidelines, given how broadly the guidelines interpret the AI systems definition.

As recommended in the guidelines, the optimal approach for assessing whether your organisation may be subject to the AI Act is to take the following steps. First, consider how the use of the technology might be classified under the AI Act, such as whether it could fall into a high-risk category. It may be the case that there will be no compliance lift, for example if it is a minimal risk AI system. If it is likely to fall under one of the higher risk categories such as high-risk AI, the second step is to consider whether the system is excluded from the scope of the AI Act altogether on the basis that it does not meet the definition of an AI system in the first place.

1. OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system", OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, https://doi.org/10.1787/623da898-en, p.7.

03

# NIS2 Considerations for the Life Sciences Sector

*Key changes and practical steps to ensure compliance*


JULIE AUSTIN
*Partner, Data & Technology*
jaustin@mhc.ie

MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie

JAMIE GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie


Cyber security is critical to every aspect of a Life Sciences business. It safeguards sensitive data and systems, and is essential for maintaining regulatory compliance and stakeholder trust. Emerging laws and legislative reform make compliance a moving target.

In this article, we:

1. Highlight the key provisions of the NIS2 Directive
2. Examine its application to the Life Sciences sector, and
3. Outline the practical steps organisations should take to ensure compliance

### What is NIS2?

NIS2 forms part of a package of measures to improve the cyber security and resilience of critical public and private sector organisations. NIS2 will require an overhaul of how organisations approach cyber security and puts leadership accountability at its core. NIS2 is currently being transposed into the national law of each EU Member State, meaning the exact application of the rules will vary from country to country. As a result, this will create a compliance challenge for multinational organisations.

## Application to the Life Sciences sector

In basic terms, subject to meeting certain size criteria, NIS2 will apply to entities in sectors which are considered critical to the EU's security and the functioning of its economy. These include the health, food and manufacturing sectors. In particular, for Life Sciences companies, again subject to meeting certain size criteria, NIS2 will apply to the following activities:

- Healthcare providers
- EU reference labs
- R&D of medicinal products
- Manufacturing basic pharmaceutical products / preparations
- Manufacturing medical devices and in vitro diagnostic medical devices
- Manufacturing medical devices considered to be critical during a public health emergency
- Manufacturing, production and distribution of chemicals
- Manufacturing of electronic products
- Food business

Generally, organisations in the Life Sciences sector will be subject to the separate and concurrent jurisdiction of each Member State in which they are established. These various national rules are causing significant headaches for multinational organisations, as the rules can vary significantly from Member State to Member State. For example, in some countries, the definition of the health sector has been expanded to include the distribution and importation of medical products, while in other jurisdictions these sectors are out of scope.

The rules mean that multinational organisations must comply with all local laws transposing NIS2 in every Member State where they are established. They must also register with the relevant competent authority in each Member State. In addition, they are required to report significant cross-border cyber security incidents to the relevant competent authorities. Senior management of organisations in each Member State are responsible for compliance. The stakes are high, as boards and senior management can be held directly accountable for compliance failings. This is causing particular issues for multinational Life Sciences organisations. Traditionally, cyber security is the responsibility of the head office or parent company, with affiliates simply relying on the measures adopted by the parent organisation.

## Key issues for Life Sciences businesses

- **Registration:** In-scope entities will need to register with their national competent authority in each Member State in which they are established. Member States have each imposed different registration deadlines and procedures for registering, which can be complex.
- **Risk management measures:** Under NIS2, each Member State will establish a set of risk management measures (RMMs) that organisations will be required to implement, as appropriate. The management body of each organisation, such as the board of directors, must approve the RMMs of their own organisation. They must also oversee the implementation of the RMMs. In certain jurisdictions, members of the management body risk being held personally liable for any infringements. The RMMs vary across each Member State, with different assessment and certification frameworks being introduced. These circumstances will inevitably lead to inconsistent approaches across the EU. For example, there is a requirement in Hungary and Romania to appoint a specified local auditor to assess compliance. However, this requirement doesn't exist in other Member States at present.
- **Supply chain due diligence:** As part of their risk management measures, NIS2 requires entities to carry out due diligence of their supply chain security. Organisations will have to ensure that they have confidence in the network and information systems of their suppliers, in addition to their own network and information systems.
- **Incident reporting:** In-scope Life Sciences organisations will be obliged to report significant cyber security incidents to the relevant competent authority. An initial report must be made within 24 hours of the organisation becoming aware of the incident. Follow up reports must be made within 72 hours, with the final report to be made in 30 days. Each country will have different reporting mechanisms and reporting requirements. As a result, handling a cross-border incident will be challenging. Multinational organisations should ensure that they have internal reporting procedures in place so if a cross-border incident occurs, there is an established process to follow. These procedures should be tested through the use of tabletop exercises.
- **Training:** Training must also be provided to management bodies to equip them to meet their obligations to approve and implement RMMs. Cyber security training should also be provided to all staff.

> *NIS2 makes cyber security a board-level responsibility for Life Sciences firms, with cross-border compliance, supplier checks, and rapid incident reporting now non-negotiable.*

## KEY DATES

EU Member States are each at different stages in their transposition of the NIS2 Directive into national law.

**NIS2 is expected to come into effect in Ireland in early 2026.** We recommend that Life Sciences organisations based in Ireland begin their preparations for the coming into force of NIS2 sooner rather than later.

# *10 Practical steps* **for compliance**

01

Identify the Member State(s) where your organisation is established.

02

Assess whether your entity falls within the scope of NIS2 in each of those Member States, taking account of the local law transposing NIS2.

03

Register with the relevant competent authority in each Member State where the organisation is established, keeping in mind the deadlines for registration varies across countries.

04

Identify key variations in approaches across jurisdictions where your organisation is subject to NIS2. Align risk management measures accordingly.

05

Work with teams on the ground in each of your locations to assess your existing cyber security infrastructure. Also, run risk assessments identifying any weaknesses in your network or your processes.

06

Consider whether you will adopt any certifications such as ISO 27001.

07

Identify your direct suppliers and carry out due diligence of their cyber security practices.

08

Develop your incident reporting plans which set out the flow of how your organisation will respond to and report a significant incident. Test these plans through tabletop exercises.

09

Ensure that you have plans in place for business continuity in case of a significant incident including back up management, disaster recovery and crisis management.

10

Develop a single approach for the management body. Also, deploy and staff training that works across Member States.

04

# CJEU Clarifies Telemedicine Rules

*Understanding which national rules apply to your business*

MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie

JAMIE GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie

A recent judgment from the Court of Justice of the European Union (CJEU) has provided added clarity on which national rules apply to telemedicine services offered and delivered across various EU member states.

The legal analysis and conclusions set out in this judgment are useful for businesses offering telemedicine services in the EU and seeking to understand which national rules apply to their business models.

### WHAT YOU NEED TO KNOW

- Only services delivered entirely remotely via information and communication technologies qualify as *"cross-border healthcare provided in the case of telemedicine"* under the Patient Rights Directive.
- In the EU, telemedicine services are governed by the law of the country where the health care provider is established.

## Background

The case originated from a request for a preliminary ruling from the Austrian Supreme Court. The request related to a dispute between the Österreichische Zahnärztekammer (ÖZ), the Austrian Dental Chamber, and UJ, an Austrian dentist. UJ was contracted by Deutsche Zahnklinik GmbH (DZK), a German-based provider of remote aesthetic dental treatments, to perform dental examinations on its behalf in Austria. ÖZ applied for an interim injunction prohibiting UJ from carrying out dental activities in Austria on behalf of foreign companies that do not hold certain professional licences required under Austrian law.

The request sought a determination on a number of questions, including:

- Is telemedicine limited solely to digital services, or can telemedicine include physical elements, for example exams and treatment?
- Is a foreign provider of telemedicine services required to comply with the professional rules of the host Member State?
- In the case of telemedicine, does the scope of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare (the Patient Rights Directive) apply only to the reimbursement of costs?

## Judgment

*Is telemedicine solely digital?*

In answering the first question, the CJEU concluded that the provision of an in-person health service is not covered by the concept of 'cross-border healthcare provided in the case of telemedicine' under the Patient Rights Directive. This means that the concept is limited to healthcare provided exclusively via ICT, to a patient by a healthcare provider established in a Member State other than that patient's Member State, without that patient and that provider being simultaneously physically present in the same location.

*A country-of-origin principle for telemedicine services?*

In order to answer the second question, the CJEU also analysed the provisions of the Patient Rights Directive alongside Directive 2000/31/EC, also known as the E-Commerce Directive. It determined that telemedicine services must be provided in accordance with the laws of the Member State where that telemedicine provider is established, not where the patient receiving the service is located.

*Scope of telemedicine rules?*

On the third question, the CJEU decided that the relevant provisions of the Patient Rights Directive must be interpreted as applying to all the fields governed by that directive, including the quality and safety of services provided, and not only to the reimbursement of the costs of cross-border healthcare.

**Comment**

The most important feature of this judgment is that it clarifies how 'telemedicine' is to be viewed, and which national laws should apply to 'telemedicine' services under EU law. It is also particularly useful when looking at complex healthcare business models with in-person and digital components spread across different EU Member States. A key question is now: where is the provider of the telemedicine service established? Telemedicine providers should check that their services are compliant with the rules in that EU member state.

> *The CJEU clarifies that telemedicine must be delivered exclusively via digital technologies, governed by the laws of the provider's home member state, rather than where the patient is located.*

05

# Medical and In Vitro Device Regulations

*EU Commission proposes reform*


MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie

JAMIE GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie

HUGH HORAN
*Associate, Product Regulatory & Liability*
hhoran@mhc.ie


Following the identification of several key challenges in the application of the Medical Device Regulation (MDR) and In Vitro Diagnostic Devices Regulation (IVDR), the EU Commission has now published its proposal setting out various targeted revisions to both frameworks. In this article, our Life Sciences Regulatory team provides an overview of the proposed amendments.

### WHAT YOU NEED TO KNOW

- The EU Commission's proposal to simplify the rules for medical devices and IVDs forms part of a package of measures to improve the health of EU citizens, while ensuring the long-term resilience and competitiveness of the health sector.
- The proposal introduces reforms that seek to simplify regulatory requirements, reduce costs and the administrative burden, and promote innovation and digitalisation in the medical device sector.
- The proposed amendments will now be submitted to the European Parliament and Council for consideration and may be revised further in advance of adoption.

The EU Commission published a proposal for a targeted revision of the MDR and IVDR on 16 December 2025. The proposal follows a call for evidence launched earlier this year seeking feedback from industry stakeholders regarding the key issues faced under the current regulations. This feedback identified unpredictable certification timelines, disproportionate conformity assessment requirements and unnecessarily high costs and burdens as core areas for improvement. In light of this feedback, the proposal aims to streamline and future-proof these EU regulatory frameworks by simplifying the applicable rules, easing the administrative burden on manufacturers and improving the predictability and cost efficiency of the certification process by notified bodies.

The main features of the proposal are arranged under a number of topic headings, with important proposed measures including:

## Simplification and proportionality

- The removal of the maximum 5-year validity period for device certificates, with notified bodies empowered to carry out periodic reviews that are proportionate to the risk posed by the device, while the certificate remains valid.

- Updates to device classification rules, potentially resulting in lower classifications, and more proportionate regulatory requirements for certain devices. The proposal offers examples of reusable surgical instruments and accessories for active implantable devices as devices that would benefit from this reclassification under the revised text, and possible updates to classification rules applicable to software devices should be monitored closely by digital health stakeholders.
- The concept of the '*well-established technology device*' to be placed on a legislative footing using a formal MDR definition. Under the proposal, medical devices falling within this category would be subject to more proportionate requirements.

### Reduction of administrative burden

- A reduced scope for devices requiring a summary of safety and clinical performance (SS(C)P), and a less frequent obligation to update the periodic safety update report (PSUR) of a device.
- Streamlined change notification procedures with notified bodies.
- An extension of the period for the reporting of serious incidents from 15 to 30 days where these do not relate to any threat to public health, death or the serious deterioration of health.

### Innovation and availability of devices for special patient groups or situations

- The introduction of criteria for designation as breakthrough devices and orphan devices, with access to expert panel advice and priority/rolling reviews.
- Extended market access for certain orphan devices CE marked under the former Directives, subject to conditions.

### Predictability and cost-efficiency of certification

- The introduction of a legal basis for structured dialogues between notified bodies and manufacturers.
- Reduced involvement of notified bodies in the conformity assessment of devices falling into lower and medium-risk classes (device class IIa and IIB and IVD classes B and C) and allows notified bodies to conduct remote audits in place of on-site audits.

### Coordination within decentralised system

- Measures to provide for increased coordination among competent authorities regarding the qualification of a product and the classification of a device, such as the codification of the 'Helsinki procedure', and an enhanced role for expert panels.
- The composition and role of expert panels to be broadened to allow for increased capabilities to provide scientific, technical, clinical and regulatory advice to the Commission, Member States, the MDCG, notified bodies and where appropriate, manufacturers.

### Further digitalisation

- The digitalisation of several aspects of compliance. For example, manufacturers would be permitted to draw up their technical documentation in digital form, and the Declaration of Conformity and certain labelling information could also be provided in digital form.

### International cooperation

- New provisions recognising the importance of global regulatory harmonisation, and the roles of the International Medical Device Regulators Forum (IMDRF) and the Medical Device Single Audit Programme (MDSAP).

### Interplay with other EU frameworks

- The overlap with 'high-risk AI system' (HRAIS) requirements under the AI Act would be addressed further, with most HRAIS requirements not applying in the case of medical devices.
- Cybersecurity to be expressly referred to in Annex I (General Safety and Performance Requirements) of the MDR and IVDR, and enhanced reporting requirements for 'serious incidents' under the EU Cyber Resilience Act.

### Comment

These proposed new measures signal the potential for widespread reform of the EU device and IVD regulatory regime in the EU. The EU's proposal will now be submitted to the European Parliament and the Council for consideration and adoption under the ordinary legislative procedure, so further revisions are possible. Although likely welcomed by industry as a positive if not long awaited step towards a more efficient and proportionate regulatory system, these proposals also require further monitoring by manufacturers, with the planned end result being a set of new requirements that will require further investment to ensure compliance.

06

# Four Modules of EUDAMED Declared Fully Functional

*Full implementation outline and timeline*

MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie

JAMIE GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie

Four modules of EUDAMED are now fully functional following a recent declaration of the European Commission. This declaration triggers a six-month transition period, after which the modules will become mandatory for manufacturers of medical devices. Our Life Sciences Regulatory team discusses the update and reviews the timeline for the full implementation of EUDAMED.

The European Commission published a Commission Decision in November 2025 declaring the functionality of four modules of EUDAMED, the EU's centralised database for information on medical devices and in vitro diagnostic devices on the EU market. This declaration follows an independent audit report from June 2025 which confirmed that these modules now meet the requirements set out by the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR).

### WHAT YOU NEED TO KNOW

- EUDAMED is a centralised European database used to collect information about medical devices and their manufacturers.
- EUDAMED was established by the Medical Devices Regulation and is currently undergoing a phased rollout.
- Four EUDAMED modules have recently been declared fully functional by the European Commission and will become mandatory from 28 May 2026.

## Operational EUDAMED modules

The four EUDAMED modules covered by this decision are:

- Actor registration
- Unique Device Identifier (UDI) / device registration
- Notified bodies and certificates
- Market surveillance

The actor registration, UDI and notified body modules have been available for voluntary use for several years. However, the announcement triggers a six-month transition period, after which the modules will shift to mandatory use from 28 May 2026.

New devices placed on the market after this date must be entered into the UDI/device registration module prior to their first placement on the market.

## Remaining modules

The final two modules, namely post-market surveillance and vigilance, and clinical investigation and performance studies, remain under development. According to a provisional timeline published by the European Commission, it is expected that the post-market surveillance module will be declared functional in late 2026, with mandatory use commencing in the second quarter of 2027. The timeline for the clinical investigation and performance studies module remains unclear.

## Comment

This Commission Decision marks an important step towards the implementation of EUDAMED. To date, the development of EUDAMED has experienced significant delays, with full functionality initially intended to begin from May 2020. Once fully operational, EUDAMED will occupy a central role in ensuring transparency across the EU by consolidating medical device information and making it more accessible to the public and healthcare professionals.

# TOP 10

# Digital Health recommended reading

01

**MDCG:** FAQ on Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)

02

**MDCG:** Guidance on the safe making available of medical device software (MDSW) apps on online platforms

03

**IMDRF:** Characterisation considerations for medical device software and software-specific risk

04

**IMDRF:** Good machine learning practice for medical device development: Guiding principles

05

**MHRA:** Digital mental health technology: qualification and classification

06

**Team NB:** Notified Body Perspective on Future Governance in the EU Medical Device Sector

07

**MedTech Europe:** Facts & Figures 2025

08

**MedTech Europe:** Position Paper - Digital label for Authorised Representative and Importer

09

**MedTech Europe:** Position Paper - The medical technology industry's views on simplification of EU digital legislation

10

**US FDA:** Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

MASON HAYES & CURRAN



## ABOUT US

Mason Hayes & Curran is a business law firm with 124 partners and offices in Dublin, London, New York and San Francisco.

We have significant expertise in product, privacy and commercial law, which are sectors at the forefront of Digital Health law. We help our clients devise practical and commercially driven solutions for products regulated under complex and ever changing EU health and technology regulatory frameworks.

Our approach has been honed through years of experience advising a wide range of clients in diverse sectors.

We offer an in-depth understanding of the Digital Health regulatory landscape, with a strong industry focus. We ensure our clients receive clear explanations of complex issues, robustly defend their interests and devise practical value-adding solutions for them whenever possible.

## KEY CONTACTS


MICHAELA HERRON
*Partner, Head of Life Sciences*
mherron@mhc.ie

JAMES GALLAGHER
*Partner, Product Regulatory & Liability*
jamesgallagher@mhc.ie

BRIAN MCELLIGOTT
*Partner, Head of AI Team, Technology*
brianmcelligott@mhc.ie

BRIAN JOHNSTON
*Partner, Data & Technology*
bjohnston@mhc.ie

ANNA LUNDY
*Of Counsel, Life Sciences Regulatory*
alundy@mhc.ie

JULIE AUSTN
*Partner, Data & Technology*
jaustin@mhc.ie


For more information and expert advice, visit:

**MHC.ie/DigitalHealth**