MASON HAYES & CURRAN

Digital Health Annual Review 2023

ISSUE 4 – DECEMBER 2023

Welcome to Mason Hayes & Curran LLP's Digital Health Annual Review 2023

2023 was another eventful year for digital health in the EU. For example, in the six months since the publication of our Mid-Year Review we have seen:

- The start of trilogue negotiations to agree the final text of the EU AI Act
- Reflection papers issued by the Food and Drug Administration (FDA) and European Medicines Agency (EMA) on the use of AI in drug development
- Updates to the Manual on Borderline Classification for Medical Devices
- 'Principles for Machine Learning in Medtech' published jointly by the Medicines and Healthcare products Regulatory Agency (MHRA), FDA and Health Canada
- Further delays to the operationalisation of the EUDAMED system
- Updated MDCG guidance on hardware/software combinations and Article 120 'significant changes'
- A MedTech Europe statement calling for a major rethink of the features of the revised EU Product Liability Directive
- An open letter from MedTech Europe to the EU Commissioner for Health calling for comprehensive structural reform of the European regulatory framework for medical technologies made up of the MDR and IVDR.

Meanwhile, a lacklustre H1 for digital health funding was followed by a 14% drop in quarter-on-quarter funding in Q3 to $3B – its lowest level since 2016 – with the majority share of top deals going to AI-enabled startups.

As we now enter 2024, we discuss these and a number of other issues that arose during 2023 for digital health stakeholders in the EU. As we prepare for another significant year, we look ahead to topics including:

- The step up in preparations for the coming into effect of the EU AI Act
- Enhanced awareness around the need to guard against product liability claims involving software products and software medical devices
- Increased adoption of at-home diagnostics and biometric tracking using wearable devices, especially in areas like agetech, femtech and mental health, and as part of decentralised clinical trials
- Further developments in the use and regulation of generative AI in healthcare
- The continued focus on cybersecurity and data privacy

We hope you enjoy the fourth edition of our Annual Digital Health Review.

Editors

Michaela Herron
Partner,
Head of Products
mherron@mhc.ie

Michaela is Head of the Products practice. She advises clients in the pharmaceutical, healthcare, medical device, digital health, cosmetic, video game, software and general consumer product sectors on various regulatory compliance matters. She has particular expertise in wearables and software medical devices. She frequently advises clients on the applicable regulatory framework, regulatory approval, labelling, packaging, traceability, safety and liability issues.

Michaela also represents manufacturers in product liability claims and enforcement action by regulators.

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

James is a Partner in the Products practice. 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 AI
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 also.

Contents

WHO on AI in Health: Key Regulatory Considerations 4

The EU Data Act: Spotlight on Digital Health 7

AI Model Contractual Clauses for High-Risk Systems 10

EU Borderline Manual for Medical Devices - Key Updates 12

Medtech Europe Calls for Major Rethink on Revision of Product Liability Directive 14

Product Liability for Consumer Healthcare Products in the EU 16

MedTech Europe's Open Letter to EU Commissioner for Health 20

Required Reading: Key Digital Health Documents 22

EUDAMED Delayed (Again) 23

First Harmonised Electronic Product Information for Medicines Published 25

Recent MHC Events, Articles & Publications 26

WHO on AI in Health: Key Regulatory Considerations

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Brian McElligott
Partner,
Head of AI
brianmcelligott@mhc.ie

Artificial intelligence (AI) is already having a significant impact on the way that healthcare services are designed and delivered across the globe. However, ongoing debate and discussion relating to issues like data integrity and security, transparency, risk management and bias that are relevant to the use of AI more generally can become particularly nuanced when looking at AI deployed in a healthcare context. A recently published World Health Organisation (WHO) publication therefore aims to outline key healthcare-specific principles that governments and regulatory authorities can follow to develop new guidance or adapt existing guidance on AI at national or regional levels.

The WHO publication focusses on a number of key areas, for example:

Documentation and transparency

Documenting all aspects of AI systems – throughout the AI system's lifecycle – is an essential way of establishing trust, guarding against bias and minimising risks which may be associated with a given AI system. Effective documentation of AI in healthcare should include, at a minimum, the identification of the purpose of the particular AI system in its clinical context. Beyond that, the level or degree of documentation required should be determined on a risk-based approach. In certain circumstances it may even be appropriate to publish a version of the training data set on which the AI system is developed for external, independent validation.

Risk management

The EU's proposed AI Act embodies a risk-based approach to the regulation of AI, which is traditionally associated with product safety legislation. The WHO's regulatory guidelines are aligned with this style of approach. In addition to documentation, a central feature of a risk-based approach to regulating AI involves monitoring and managing the development and use of an AI system. An integral part of such a risk-management approach is the need to determine the level of scrutiny required based on the risk-level or categorisation of the AI system.

Some AI systems will be riskier than others and vice versa. In general, all AI systems should be subject to a system of pre- and post-market monitoring. This is done through data collection and evaluation, with a view to minimising known risks and adapting to emerging or unforeseen risks going forward. These processes should be more intense for high-risk AI systems and correspondingly less intense in scenarios involving low-risk AI systems.

Data privacy

Given the vast amounts of data involved in the development and use of many AI systems, privacy and data protection will remain a significant focus area for governments and regulators. This is particularly the case where personal data will be necessary for the effective operation of the AI system.

Not only must data be of a certain quality to ensure that AI in healthcare really works, but it must also be secure and respect the fundamental rights of data subjects. While transparency contributes to privacy, the WHO believes that developers of AI for healthcare should consider privacy and data protection norms when developing and deploying their AI systems. This might involve the adoption of a separate and distinct compliance programme in relation to privacy and data protection.

Recommendations

This WHO publication is a useful summary and restatement of some of the most prominent issues and considerations that governments and regulators are seeking to address in new AI regulations and legislative frameworks worldwide. Given the focus on AI in healthcare, digital health stakeholders should be aware of its contents.

In particular, the publication finishes with a set of key recommendations arranged under 6 headings which are useful as guiding principles when developing digital health products containing or comprised entirely of AI technologies:

1. Documentation and transparency

- Consider pre-specifying and documenting the intended medical purpose and development process, such as the selection and use of datasets, reference standards, parameters, metrics, deviations from original plans, and updates/changes during the phases of development. These should be considered in a manner that allows for the tracing of the development steps, as appropriate
- Consider a risk-based approach also for the level of documentation and record-keeping utilized for the development and validation of AI systems

2. Risk management

- Consider a total product lifecycle approach throughout all phases in the life of a medical device: premarket development management, post-market management/surveillance, and change management
- Consider a risk management approach that addresses risks associated with AI systems, such as cybersecurity threats and vulnerabilities, underfitting, algorithmic bias etc

3. Intended use and validation

- Consider providing transparent documentation of the intended use of the AI system. Details of the training dataset composition underpinning an AI system – including size, setting and population, input and output data and demographic composition – should be transparently documented and provided to users
- Consider demonstrating performance beyond the training dataset through external, analytical validation in an independent dataset. This external validation dataset should be representative of the population and setting in which the AI system is intended to be deployed and transparent documentation of the external validation dataset and performance metrics should be provided. This external validation dataset should be appropriately independent of the dataset used for the development of the AI model during training and testing
- Consider a graded set of requirements for clinical validation based on risk. Randomized clinical trials are the gold standard for the evaluation of comparative clinical performance and could be appropriate for the highest risk tools or where the highest standard of evidence is required. In other situations, consider prospective validation in a real-world deployment and implementation trial which includes a relevant comparator using accepted relevant groups

- Consider a period of more intense post-deployment monitoring through post-market management and market surveillance for high-risk AI systems

4. Data quality

- Consider whether available data are of sufficient quality to support the development of the AI system that can achieve the intended purpose
- Consider deploying rigorous pre-release evaluations for AI systems to ensure that they will not amplify any of relevant issues, such as biases and errors
- Consider careful design or prompt troubleshooting to help early identification of data quality issues, which could potentially prevent or mitigate possible resulting harm
- Consider mitigating data quality issues that arise in health-care data and the associated risks
- Consider working with other stakeholders to create data ecosystems that can facilitate the sharing of good-quality data sources

5. Data privacy

- Consider privacy and data protection during the design and deployment of AI systems
- Consider gaining a good understanding of applicable data protection regulations and privacy laws early in the development process and ensure that the development process meets or exceeds such legal requirements
- Consider implementing a compliance programme that addresses risks and develop privacy and cybersecurity practices and priorities that take into account potential harm and the enforcement environment

6. Engagement and collaboration

- Consider the development of accessible and informative platforms that facilitate engagement and collaboration, where applicable and appropriate, among key stakeholders of the AI innovation and deployment roadmap and collaboration
- Consider streamlining the oversight process for AI regulation through engagement and collaboration in order to potentially accelerate practice-changing advances in AI

The EU Data Act: Spotlight on Digital Health

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Brian Johnston
Partner,
Privacy & Data Security
bjohnston@mhc.ie

The EU Data Act (Regulation (EU) 2023/2854) entered into force on 11 January 2024, putting into place new rules for the fair access to and use of data. We look at the impact this new legislation will have on those in the digital health sector when it applies from 12 September 2025.

What is the Data Act?

The Data Act is a key pillar of the EU Data Strategy. It will operate alongside the EU Data Governance Act and sectoral legislation to develop common European data spaces such as the European Health Data Space. The goal of the Data Act - and the wider EU Data Strategy - is to facilitate reliable and secure access to data, fostering its use in key economic sectors and areas of public interest.

The Data Act provides for new rights and obligations regarding the sharing of "data generated by the use of a product or related service". This includes any data recorded intentionally by the "user", for example weight and height in a fitness tracker. Information recorded passively like location and heart-rate in a fitness tracker when the product is in standby mode also comes within scope.

The right to access and/or trigger the sharing of data will be attributed to a "user" of the product or service, who is defined as "the natural or legal person that owns, rents or leases a product or receives a service". Meanwhile, the "data holder" will be the company that has the control of the technical design of the product and/or the related service and has the ability to share certain data.

Relevance for digital health

Any connected Internet of Things (IoT) device or wearable that obtains, generates or collects data of the person using the wearable, or regarding their environment, will be under the scope of the Data Act. Medical and health devices are expressly mentioned and most digital health stakeholders, such as manufacturers of software medical devices and wearables, as well as suppliers of related services, will be subject to the Data Act where the product or service is placed on the market in the European Union.

Important features

Some features of the Data Act that are particularly relevant to digital health products include:

Transparency

Before concluding a contract involving the supply of a connected medical device or health wearable, a user will need to be provided with information on:

- The nature and volume of the data likely to be generated by the use of the product
- How the user may go about accessing that data
- Whether the manufacturer/service provider intends to use the data itself or allow a third party to use the data and, if so, the purposes for which the data will be used

Right of access/obligation to share

The user will have a right to access data and/or require the data holder (subject to some limited exceptions) to share it with a third party. Where the recipient of the data is a third party, it can process the data for the purposes and under the conditions agreed with the user in a "sharing agreement", and subject to the privacy rights of the data subject. Users/third parties receiving data would not be permitted to use the data to develop a product that competes with the product from which the accessed data originates. Data may also be made available to public sector bodies in cases of public emergencies (e.g. major cybersecurity incidents), subject to national rules to be set down at Member States level.

Data protection

Sharing of health data with a third party will qualify as processing of a special category of data requiring a legal basis under Article 6 GDPR and a derogation under Article 9 GDPR.

The sharing will ordinarily not be carried out for the purposes of preventive or occupational medicine, medical diagnosis, etc. The usual derogation for the disclosure of health data will be the data subject's consent, although other legal bases, performance of an agreement, legitimate interest, etc. may also be appropriate in certain circumstances and where a derogation under Article 9 GDPR will apply.

Key issues

While the Data Act has now formally entered into force, questions remain about how it will be applied in practice and impact on other legislative frameworks.

Towards the end of 2023, MedTech Europe and COCIR (the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries) issued a joint statement on the final agreement of the Data Act). The statement aimed to raise awareness around the Data Act's impact on the medical technology sector.

It highlighted the importance of guidance that includes the necessary clarifications and references to the safety, health, and performance of connected products. It also looks ahead to future sector-specific legislation, such as the European Health Data Space (EHDS). The concerns highlighted by MedTech Europe and COCIR on behalf of industry remain relevant following the Data Act entering into force. Those concerns are as follows:

Data sharing obligations

- The obligation to share data under the Data Act should in no way contradict or compromise the obligations for medical technologies required under other EU legislation. This may have implications on patient or device safety
- The Data Act needs to be interpreted in a way that recognises the safety, performance, and efficacy requirements of medical technologies, given their direct impact on the health and safety of patients
- More clarity on the Data Act's interplay with GDPR, MDR and IVDR cybersecurity, safety, and efficacy requirements, as well as privacy requirements, is crucial to mitigate unintended risks
- A better understanding of the interplay with upcoming sectoral data legislation, namely the EHDS, is needed

Intellectual property and trade secrets

- Strict interpretation of which data is readily available along with the alignment with the existing legislative framework on the protection of IP and trade secrets as well as international agreements is important

International data flows

- Any risk of imposing data localisation and possible counter-reactions of third countries must be avoided

Interoperability

- Preference should be given to already successfully implemented fit-for-purpose and consensus balloted healthcare interoperability standards, including HL7, SNOMED, etc
- The Data Act should encourage the creation of data repositories, consortia, or other mechanisms that allow companies to access and utilise anonymised, aggregated healthcare data for research and development, like HealthData@EU. These initiatives should prioritise maintaining the privacy and security of individuals while providing an environment conducive to innovation and breakthrough discoveries

Conclusion

The EU Data Act entered into force on 11 January 2024. The requirements of the Data Act will apply from 12 September 2025 .

Those in the digital health sector should therefore familiarise themselves with the Data Act, assess how it might impact on their respective business models, and put in place necessary measures to ensure compliance.

AI Model Contractual Clauses for High-Risk Systems

Brian McElligott
Partner,
Head of AI
brianmcelligott@mhc.ie

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Ensuring contractual certainty in agreements related to innovative technologies with complex and changing regulatory requirements is a challenge for in-house counsel and their external advisers. Contracting for software medical devices currently regulated under the EU Medical Device Regulation (MDR), and soon to be regulated under an EU AI Act, is a good example. Model clauses from a credible source can often be particularly helpful.

Against this backdrop, a multi-stakeholder group within the European Commission has published a draft proposal for standard contractual clauses (SCCs) for the procurement of AI by public organisations. One of the template SCCs that has been developed deals specifically with high-risk AI systems, which are a major focus of the requirements in the proposed AI Act due to be passed by the end of this year. These SCCs will be particularly relevant to digital health stakeholders operating in the EU because the majority of software medical devices incorporating AI are expected to be regulated as high-risk AI systems under the AI Act. The SCCs are intended for use by public organisations but are a useful reference for developers of medical device software incorporating AI who are reviewing and drafting their own contractual provisions.

What do they do?

The goal with the SCCs is to make provision for compliance with the EU AI Act in existing agreements. It is hoped that the SCCs will also ensure that the respective rights and responsibilities of the parties to agreements involving AI systems are clear. They are not standalone sets of template contractual provisions, however. They are drafted in such a way that they can be attached as a schedule to an existing agreement. Given the variety among AI-systems, the SCCs also contain a number of Annexes relating to system-specific features that can be populated in accordance with the system the subject of the agreement. These include:

- Descriptions of the system itself and its intended purpose (Annex A)
- Data sets used for training of the system (Annex B), and
- Measures taken to meet transparency requirements (Annex E).

SCCs replicate the AI Act

The SCCs are largely based on the requirements of high-risk AI systems under the proposed AI Act. They essentially mimic the terms of the AI Act regarding certain core definitions, such as the "intended purpose", "reasonably foreseeable misuse" and "substantial modification" of an AI system. They also address the key requirements for AI systems, such as:

- The implementation of a risk management system
- The development of technical documentation and instructions for use, maintaining adequate records, and
- The requirement that AI systems are sufficiently transparent to enable the user to reasonably understand the system's functioning

The obligations of high-risk AI system providers under the AI Act are also provided for in the SCCs. These include the obligation that a quality management system is implemented, and that the AI system undergoes a conformity assessment.

Rights to use data sets

The SCCs aim to ensure clarity regarding the rights of parties in the use of data when training and operating high-risk AI systems. For instance, in the case of public organisations employing these clauses, all rights, including intellectual property rights, pertaining to the datasets of public organisations should be vested in those bodies. The supplier of an AI system is prohibited from utilising these datasets for purposes beyond those explicitly permitted by the public organisation. However, suppliers retain entitlement to all these rights concerning their own datasets but are obliged to grant public organisations a non-exclusive right to use these datasets for the purpose of employing the AI system. The SCCs also propose the inclusion of provisions for public organisations and suppliers to indemnify each other in case of any infringement of their intellectual property, privacy, and related rights concerning their datasets.

What's missing?

As well as the planned AI Act, AI systems tend to be regulated under various EU regulatory frameworks. The SCCs are specifically addressed to AI systems as regulated under the AI Act only, however. In other words, the SCCs do not incorporate requirements and obligations that may arise under other EU frameworks such as the GDPR or the MDR.

It is also common for public procurement contracts to incorporate certain more extensive and onerous terms and impose additional obligations on technology suppliers than would otherwise be seen in traditional commercial contracts. For example, additional obligations around sustainability requirements and human rights protections are increasingly common. The European Parliament's proposed revisions to the text of the AI Act were marked by their addition of human rights due diligence and other obligations. For the time being however, these types of obligations have not been provided for in the SCCs.

What to do?

Digital health stakeholders should review the SCCs and consider them as a useful benchmark for assessing and possibly updating their own internal contractual provisions dealing with AI systems in the EU. They do not amount to a template for a "complete agreement" solution, but they do offer important insights when it comes to recognising and providing for sophisticated EU regulatory requirements as part of contracting processes.

The versions currently available are still in draft form and have been published with a view to collecting initial feedback from stakeholders. Digital health stakeholders can also read them and consider whether there are any unique features of AI systems that are also regulated as medical devices in the EU that could or should be provided for in a final version of the SCCs.

EU Borderline Manual for Medical Devices – Key Updates

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Aisling Morrough
Senior Associate,
Product Regulatory & Liability
amorrough@mhc.ie

The European Commission's Medical Device Coordination Group (MDCG) recently published an updated version of its Manual on Borderline and Classification for Medical Devices (the Manual). The Manual records the decisions made by the MDCG's Borderline and Classification Working Group (BCWG) under the Helsinki Procedure as provided for in the Medical Device Regulation (MDR) and the In Vitro Diagnostics Regulation (IVDR).

While not legally binding, the Manual serves as an important guide on the qualification and classification of 'borderline' cases under the European regulatory framework for medical devices. This is particularly helpful for digital health and medical device software products where qualification and classification issues are common.

The Manual contains a number of worked examples of borderline qualification and classification cases. However, it is a work in progress and will continue to be populated as cases are finalised by the BCWG under the Helsinki Procedure. While the old version of the Manual, which related to Directive 93/42/EEC on medical devices (MDD) and Directive 98/79/EC on in vitro diagnostic medical devices (IVDD), had an entire section covering the classification of software and mobile applications.

The Manual currently contains a limited number of digital health-related examples:

- Temperature sensors embedded in orthopaedic devices for compliance tracking, for example scoliosis braces. These devices are not considered an accessory to a medical device as the sensor does not specifically and directly assist the medical functionality of the orthopaedic device. They are also not considered a medical device in their own right because the orthopaedic device can function without it
- Medical calculators to facilitate routine medical calculations at the point of care for multiple clinical disciplines through an app or webpage. For example, the calculation of stroke risk for patients with atrial fibrillation. Given their intended use for a medical purpose, these devices are considered a medical device in accordance with the MDR. As classification rule 11 applies, software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes, they are classified as at least class IIa
- Smartphone application for STI prevention strategies intended to prevent STI by the exchange of information between different sexual partners. The risk calculation is considered an epidemiologic tool rather than a prevention tool within the meaning of the medical device definition and so, the product is not considered a medical device under the MDR

Conclusion

The Manual will be updated as more decisions are made regarding borderline qualification and classification cases. While not legally binding, it is highly recommended that manufacturers of medical devices and in vitro diagnostics (IVDs) familiarise themselves with the views expressed by the MDCG in the Manual. It should be read in conjunction with other MDCG documents providing guidance on borderline cases and the classification of medical devices and IVDs.

The up-to-date version of Manual can be accessed online.

Medtech Europe Calls for Major Rethink on Revision of Product Liability Directive

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Aisling Morrough
Senior Associate,
Product Regulatory & Liability
amorrough@mhc.ie

MedTech Europe, along with 11 other European industry associations, has published a statement on the progress of the revision of the Product Liability Directive (PLD).

The existing text of the PLD has been in force for nearly 40 years and has been due an upgrade. It provides for a system of 'strict liability' for claims involving injuries caused by defective products, including medical devices. This means that claimants do not have to prove that manufacturers:

- Did something they should not have done, or
- Failed to do something they should have

Instead, they are required to prove that the product was 'defective' and that that defect caused their injury. 'Defectiveness' is assessed with reference to a set of broad criteria. The ultimate legal test is whether the product provides the level of safety that the consumer is entitled to expect in the circumstances. The PLD is designed to make it easier for consumers to claim for injuries suffered. However, as products have become more technologically sophisticated it has become harder for consumers to prove their 'defectiveness'. The proposed changes to the PLD seek to address this and other challenges for consumers when bringing claims.

In terms of digital health and software/AI medical devices, a key point is that the current PLD only covers hardware products. This means you can't use the PLD to claim for injuries caused by standalone software. The revisions would change this and bring software within scope for product liability claims. This is likely to have huge implications for digital health stakeholders. This is especially the case when viewed alongside other EU developments like the Collective Redress Directive.

The MedTech Europe statement claims that:

"...the revision would sweep away existing checks and balances and create a one-sided, litigation-friendly regime. The impact of the changes will significantly raise litigation risk, legal complexity and uncertainty for European businesses. Companies will have to decide whether to expend significant resources to defend against potentially unmeritorious claims or settle to limit litigation costs and reputational risk.

Ultimately, the primary beneficiaries of this far-reaching change to the PLD will likely be lawyers and litigation funders rather than European consumers."

The EU Council and Parliament have adopted their negotiating positions on the text of the Commission's proposal for the revisions. Inter-institutional negotiations, also referred to as 'trilogues', to agree the final text of the legislation are about to begin.

Against this backdrop, MedTech Europe makes several recommendations in its statement:

- **Limit the alleviation of the burden of proof:** Under the current PLD, the claimant must prove the damage, the defect and the causal link between the two. The new rules would make it easier for claimants to do this with reference to various undefined terms such as "obvious malfunction", "excessive difficulties" and damage that is "typically consistent" with a product defect. The scope of these new allowances for claimants should be significantly narrowed. In addition, clarification should be provided as to what claimants must do and prove before any liability can be presumed
- **Safeguards for disclosure of evidence:** New disclosure rules lack sufficient safeguards to protect businesses against abusive discovery exercises or disclosure of commercially sensitive data or trade secrets. Disclosure of evidence must therefore be limited to only what is strictly necessary and proportionate. Similarly, there should also be a right for defendants to request relevant information from the claimant
- **Scope to be fit for purpose:** Software being included in a strict liability regime brings new questions, such as how to apply the concept of defectiveness. More investigation into the impact of this extension is needed, as there is now greater legal exposure for software developers

Conclusion

How soon could this all be happening? It is expected that a final text of the revised PLD will be adopted at some point during the first half of 2024. This may then have to be transposed by all EU Member States within 12 months.

For more information on the revisions to the PLD, see our short insight piece here.

A useful briefing note issued by the European Parliamentary Research Service (EPRS) with a bit more detail about the proposed revisions is also available here.

Product Liability for Consumer Healthcare Products in the EU

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Aisling Morrough
Senior Associate,
Product Regulatory & Liability
amorrough@mhc.ie

The transition to a digital and circular economy continues to transform various aspects of the healthcare sector. This undoubtedly has many positive economic and social impacts. However, the changing nature of healthcare products in the digital age has challenged some of the core rules and concepts underpinning the current product liability regime provided for under EU law. Notable recent changes include the interconnectedness and self-learning functions of products, and the emergence of new actors such as online platforms.

A revised Product Liability Directive

The current EU Product Liability Directive (PLD) has been in force for nearly 40 years. A 2018 evaluation of the PLD by the European Commission identified several shortcomings, largely driven by significant changes since the PLD was adopted in 1985. These include the modernisation of product safety and market surveillance rules. In particular, technological advances and increased awareness around environmental sustainability and the circular economy have led to the creation of a new generation of products that have made it more difficult to:

- Consistently apply the definitions and legal tests contained in the PLD
- Effectively prove that a defect in a product caused the damage suffered
- Allocate responsibility and liability when a business substantially modifies a product that is already on the market, or when a product has been directly imported from outside the EU by a consumer

In light of these concerns, in September 2022, the European Commission published its proposal for a new Product Liability Directive (PLD Proposal). The changes contained in the PLD Proposal are designed to address these challenges and provide the EU with an extra-contractual product liability regime updated to deal with the 21st century product landscape.

Noteworthy features

Some noteworthy features of the PLD Proposal include:

- **Alignment of Terminology:** the PLD Proposal would bring EU product liability and product safety rules into closer alignment by adopting various terms and definitions that are already used in EU product safety legislation. For example, 'manufacturer', 'placing on the market' and 'making available on the market'
- **Expanded definition of a 'product':** the PLD Proposal expands the definition of a 'product' to include software and digital manufacturing files. The proposed new definition clarifies when a related service, ie a digital service that is integrated into, or inter-connected with, a product is to be treated as a component of that product

- **Defectiveness:** the PLD Proposal adds additional factors to be considered when determining whether a product is defective. These factors include interconnectedness, self-learning functionality and a product's cybersecurity vulnerabilities
- **Burden of proof:** there is a proposed rebuttable presumption of defectiveness where:
  - The claimant establishes that the product does not comply with mandatory safety requirements
  - The claimant establishes that the damage was caused by an "obvious malfunction" during normal use or under ordinary circumstances
  - A defendant fails to comply with an order to disclose the evidence necessary for the claimant to understand how a product was produced and how it operates

The PLD Proposal also includes a rebuttable presumption that a defective product caused damage where it has been established that the product is defective, and the damage caused is of a kind typically consistent with the defect in question.

- **Defendants:** the PLD Proposal expands the pool of defendants that can potentially be held liable for damage caused by a defective product. As well as manufacturers, importers and in some cases distributors, the PLD Proposal would also permit no-fault liability claims to be brought against authorised representatives, fulfilment service providers, third parties making substantial modifications to products already placed on the market, and certain online platforms. This proposed change highlights the growing significance of products manufactured outside the EU and is designed to ensure that there is always an economic operator in the Union against whom a claim for compensation can be made. In the case of online platforms, the PLD Proposal makes it clear that it does not affect the conditional liability exemption available under the Digital Services Act. This is because the PLD Proposal is geared towards liability in cases where: an online platform cannot benefit from that exemption; and a person is harmed by a defective product and seeks compensation
- **Scope of 'damage':** the PLD Proposal seeks to extend the concept of 'compensable damage' to include corruption of data and recognised forms of psychological injury. It is also proposed to remove the €500 minimum threshold for property damage
- **Scope of liability:** the PLD Proposal seeks to expand the scope of liability from the previous reference to when a product was put into circulation to possibly include the time after circulation, including once the product has been placed on the market, if a manufacturer retains control of the product, for example through software updates
- **Longstop provision:** the PLD Proposal suggests two modifications to the 10-year longstop provision. First, an extension to 15 years in certain cases involving latent personal injuries. Second, calculation of time running from the date that a product has been substantially modified, at a point after it has been placed on the market or put into service

When?

Now that the European Council and the European Parliament have approved their negotiation positions on the PLD Proposal prepared by the European Commission, trilogue negotiations will commence to agree the final text of the legislation. This is with a view to having the legislation passed in advance of the European Parliament elections in June 2024.

As the table overleaf illustrates, while there is some consensus between the three institutions, there remain significant differences in their positions. These will have to be addressed before political consensus is achieved. After this, the legislative text will be formally adopted by the Parliament and Council before publication and entering into force on the 20th day following its publication in the Official Journal of the European Union.

Once adopted, the revised Product Liability Directive will also need to be transposed into national law. The PLD Proposal provides that the current Directive would be repealed, and Member States would be required to transpose the new legislation into national law within 12 months of its entry into force.

Snapshot: Respective positions of the EU Institutions on the revised Product Liability Directive

	Product	Defectiveness	Damage	Causation	Limitation Periods
European Commission	Should include 'software' and 'digital manufacturing files'. Proposed treatment of a 'related service', a digital service that is integrated into, or inter-connected with a product, a component of that product.	Should be assessed with reference to: • A product's ability to learn after its deployment • Its effect on other products that can reasonably be expected to be used together • Product safety requirements and cybersecurity vulnerability Introduction of a rebuttable presumption of defectiveness in certain cases.	The notion of compensable damage should include corruption of data and recognised forms of psychological injury. Removal of the €500 minimum threshold for property damage.	Introduction of a rebuttable presumption that a defective product caused the damage where: • Claimants face "excessive difficulties" in proving defectiveness owing to the product's technical or scientific complexity • It can be established that the product is defective, and the damage caused is of a kind "typically consistent" with the defect in question	Proposed extension of 10-year longstop to 15 years in certain cases involving latent personal injuries. The limitation period could also reset and restart from the date that a product had been substantially modified.
European Council	Definition should cover raw materials.	When assessing defectiveness: • Warnings or other product information cannot, by themselves, make an otherwise defective product safe • A product's 'reasonably foreseeable use' should include foreseeable instances of misuse	Compensation for pure economic loss, privacy infringements or discrimination should not by themselves trigger liability under the revised Directive. However, this should not affect the right to compensation for any damages, including non-material damages, under other liability regimes.	Presumption of a causal link between a product's defectiveness and the damage suffered where the claimant has established that a product is defective and similar cases have shown that the damage suffered is typically caused by the defect in question.	Proposed extension of longstop period to 20 years in certain cases involving latent personal injuries. A new limitation period after a product has been substantially modified and has subsequently been made available on the market or put into service.
European Parliament	Agrees with the inclusion of raw materials. Recognition of the increasing prevalence of inter-connected as well as integrated products.	A product's 'reasonably foreseeable use' should consider its expected lifespan. Defectiveness should consider a product's ability to acquire new features or knowledge after its deployment.	The definition of 'damage' should include material losses resulting from: • Medically recognised damage to psychological health • Damage to or destruction of property subject to certain specific exceptions, and • Destruction or irreversible corruption of data not used for professional purposes. provided the material loss exceeds €1000.	The presumption of a causal link where a product belonging to the same production series as a product already proven to be defective. Empowerment of national consumer protection bodies to gather the evidence necessary to prove defectiveness, damage and the causal link between the two, on behalf of groups of consumers.	Proposed extension of longstop period to 30 years in certain cases involving latent personal injuries.

MedTech Europe's Open Letter to EU Commissioner for Health

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Aisling Morrough
Senior Associate,
Product Regulatory & Liability
amorrough@mhc.ie

Both the Medical Devices Regulation (EU) 2017/745 (MDR) and the In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR) aim to provide "a robust, transparent, predictable and sustainable regulatory framework that ensures a high level of safety and health while supporting innovation". However, despite more than six years of implementation, the European and Swiss medical technology industry say that the IVDR and MDR have not achieved their intended objectives. Importantly, they say that there are structural issues in the Regulations that cannot be overcome by their implementation.

In their open letter to European Commissioner for Health & Food Safety, Stella Kyriakides, the representative associations have called for comprehensive structural reform of the European regulatory framework for medical technologies. They say that it is urgently needed to address systemic issues encountered by patients and health systems alike in accessing medical technology throughout Europe.

Systemic regulatory issues

Among the systemic issues identified by the representative organisations are that the regulatory framework is unpredictable, complex, slow and costly. They claim that this:

- Impacts access by European patients and health systems to medical technologies, both those already on the market and future innovations
- Slows the pace of innovation in Europe, with medical technology innovations available in other regions not available in Europe, and
- Causes certain products to no longer be available for medical care in Europe

Proposed solutions

The representative organisations have called for:

- An efficient CE marking system: A more efficient and resource-effective CE marking system would improve predictability, reduce the administrative burden, and flexibly adapt to external changes. Examples of measures suggested include:
  - Predictable and transparent deadlines and costs for all regulatory processes
  - Removing the limited validity of certificates, and
  - Bringing the EU into the Medical Device Single Audit Program (MDSAP) programme

- Support for innovation: The inclusion of an innovation principle to quickly connect the latest medical technologies to European patients and health systems through dedicated assessment pathways and early dialogues with developers
- An accountable governance structure: The establishment of a single, dedicated structure to oversee and manage the regulatory system, including the designation and oversight of Notified Bodies, with the authority to make system-level decisions

Conclusion

MedTech Europe and the other signatories to the letter are highly critical in their assessment of the current EU regulatory position. However, the representative organisations have indicated their willingness to work with Commissioner Kyriakides and the European Commission to deliver the desired structural reform. A response from Commissioner Kyriakides and the European Commission is awaited.

This adds to mounting pressure from the medical technology industry following the publication in June 2023 of a similarly critical White Paper by German medical technology associations on the future development of the MDR and IVDR.

For further information, please see the MedTech article and the open letter.

Required Reading: Key Digital Health Documents

1. Artificial Intelligence for healthcare and well-being during exceptional times: A recent landscape from a European perspective. European Commission Technical Report
2. Reflection paper on the use of artificial intelligence in the lifecycle of medicines. European Medicines Agency (EMA)
3. Discussion paper on the use of Artificial Intelligence and Machine Learning in the Development of Drug and Biological Products. Food and Drug Agency (FDA)
4. Briefing on the new Product Liability Directive, European Parliamentary Research Service
5. MDCG 2023-4
   Medical Device Software (MDSW) – Hardware combinations: Guidance on MDSW intended to work in combination with hardware or hardware components
6. Manual on borderline and classification for medical devices under the MDR and the IVDR, European Borderline Classification Working Group
7. Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles. MHRA, FDA and Health Canada
8. Cybersecurity of Artificial Intelligence in the AI Act: Guiding principles to address the cybersecurity requirement for high-risk AI systems. European Commission Technical Report
9. Regulatory considerations on artificial intelligence for health. World Health Organization
10. Digital Health Reimbursement Strategies of 8 European Countries and Israel: Scoping Review and Policy Mapping. Van Kessel et al. JMIR Mhealth Uhealth. 2023 Sep 29:11

EUDAMED Delayed (Again)

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Michaela Herron
Partner,
Head of Products
mherron@mhc.ie

EUDAMED is the secure, web-based European portal for medical devices, provided for under the Medical Device Regulation (MDR). It acts as a central database of information exchanged between national competent authorities and the European Commission. EU and non-EU device manufacturers, importers, system and procedure pack producers and authorised representatives must also register and provide information via this system. This approach ensures greater transparency across the life cycle of devices placed on the EU. Parts of the system will be publicly accessible.

Composition

EUDAMED is made up of six interconnected modules on a public site:

1. Actor – user registration and management (operational)
2. UDI database and registration of devices (operational)
3. Certificates and Notified Bodies (operational)
4. Clinical investigation and performance studies (coming soon)
5. Vigilance and post-market surveillance (coming soon)
6. Market surveillance (coming soon)

It will not become fully operational until all of the modules are up and running. While work to do that continues at EU level, stakeholders are being encouraged to familiarise themselves with the modules that are operational, in order to be ready to use the full system in due course. Some updated guidance and information has been published which stakeholders should remain up to date with:

- EUDAMED user guide: Economic Operators – Actor module
- Guidelines on Data Exchange with EUDAMED
- EUDAMED Release notes

There is also Medical Device Coordination Group (MDCG) guidance, entitled MDCG 2021-1 Rev. 1, which sets out workarounds for how stakeholders are to register with and notify information to Member State competent authorities until EUDAMED is fully functional.

Timeline

The big question for EUDAMED is when will it be ready? The European Commission said in 2019 that it would be completely functional only when all its modules are available and after confirmation of the functional specifications by an independent audit. It was originally scheduled to be launched in 2020. By mid-2023, the new 'go-live' date was expected to be some time in Q2 2024.

It is now expected to be fully operational by 2027, as the implementation of the clinical investigation module will not be ready until then. All other modules will be finished by Q2 of 2024. This means that the 6 and 24-month timelines for the transitional period of EUDAMED obligations are now expected to start in 2027.

Comment

Although these continued delays are not a welcome development, medical device manufacturers should continue to familiarise themselves with the existing guidance and the various modules making up the database as they are introduced. Given the detailed information to be entered, and the care required to provide data in an organised and accessible format, learning how to navigate the various parts of the database as they come on stream will also assist in managing the resources required to ensure full adherence with this new system.

First Harmonised Electronic Product Information for Medicines Published

James Gallagher
Partner,
Product Regulatory & Liability
jamesgallagher@mhc.ie

Michaela Herron
Partner,
Head of Products
mherron@mhc.ie

The Heads of Medicines Agencies (HMA), the European Commission (EC) and the European Medicines Agency (EMA) have published the first electronic product information (ePI) for 25 human medicines harmonised across the European Union (EU). This is part of a one-year pilot project exploring how to integrate ePIs into common practice and expand their use across the EU.

What is ePI?

ePI refers to the authorised, statutory product information for medicines (such as the summary of product characteristics, package leaflet and labelling) adapted for handling in electronic format and dissemination via the web, e-platforms and in print. Ordinarily these documents would be found, often as a PDF document, on the websites of EU regulators, with a printed package leaflet also provided in the medicine's box. Digital platforms open new possibilities to share this information electronically. It also allows for information to be continuously updated and made more accessible to end users such as healthcare professionals and patients.

A transition to ePI is therefore expected to provide various advantages including improved accessibility, searchability and multilingual capabilities for product safety information. ePI also has the potential to integrate with electronic healthcare systems, enabling healthcare professionals and patients to access accurate and up-to-date product information more conveniently.

Pilot project

EMA and a group of EU national competent authorities, including Denmark, the Netherlands, Spain and Sweden, are testing the use of ePI in a one-year pilot project from July 2023. This initiative is an action under the Pharmaceutical Strategy for Europe supported by the EU funding programme EU4Health. The pilot will conclude in July 2024.

Published ePIs

The 25 published ePIs are for medicines evaluated by EMA or national authorities of Member States taking part in the pilot project. They were created following the EU ePI Common Standard adopted by the European medicines regulatory network, to provide a consistent structure throughout all Member States and ensure the information works across different e-health platforms. Companies participating in the pilot create and submit the ePI as part of their regulatory application and the ePIs can be viewed at the Product Lifecycle Management Portal in English for centrally approved medicines and in the local language for nationally approved ones. Testing is ongoing to allow access to ePIs in all EU languages.

In addition, ePI data can be accessed via a public application programming interface where developers can explore the potential of this new format within existing digital platforms.

More information on the announcement is available here.

Recent MHC Events, Articles & Publications

Events & Webinars

- MedTech Summit 2023: Medical Device Software and AI Medical Devices – Liability through a wider lens
- HealthTech Ireland Breakfast Briefing Series: The AI Act and what it means for your organisation
- RAPS Ireland: Substantiation, Advertising & Promotion for Medical Devices
- Bio€quity Europe 2023
- Future Health Summit 2023
- Technology Conference – Talent, Funding and the Future

Publications

- A question of liability: Who is responsible when an AI medical device leads to patient harm? (Journal of Medical Device Regulation - November 2023)
- Medical Devices: Sources of Regulation (Thomson Reuters Practical Law Series)
- Product Liability Law in Ireland (Lexology Getting the Deal Through Series)
- Medical Devices and the Risk of Trademark Infringement
- Decentralised Clinical Trials in the EU: Key Considerations
- The EU AI Act – Imaging and Diagnostics

About us

Mason Hayes & Curran is a business law firm with 119 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 to give our clients clear explanations of complex issues, robustly defend their interests and devise practical value-adding solutions for them whenever possible.

What others say about us

Our Products Team

"The law firm has a superb team, easy to work with, supportive and fully understands the complexity of cases."

Chambers & Partners, 2023

Our Privacy & Data Security Team

"Vast experience in dealing with technology companies headquartered in Ireland."

"They remain the "go to" firm for privacy matters."

Legal 500, 2023

Our Life Science & Healthcare Team

"They assess complex situations in a balanced manner with an intuitive ability to recognise and understand the cases. They get the job done efficiently but always in a warm and friendly way."

Chambers & Partners, 2023

Our Technology Team

""...always go over and above, no matter the issue. They have a wonderful ability to turn advice on complex points around quickly and concisely."

Chambers & Partners, 2023

Key contacts

Michaela Herron
Partner,
Head of Products
+353 1 614 2878
mherron@mhc.ie

James Gallagher
Partner, Product
Regulatory & Liability
+353 86 068 9361
jamesgallagher@mhc.ie

Brian Johnston
Partner,
Privacy & Data Security
+353 86 776 1771
bjohnston@mhc.ie

Brian McElligott
Partner,
Head of AI
+353 86 150 4771
brianmcelligott@mhc.ie

Aisling Morrough
Senior Associate, Product
Regulatory & Liability
+353 86 083 2044
amorrough@mhc.ie

For more information and expert advice, visit:

MHC.ie/DigitalHealth

Dublin London New York San Francisco

MHC BRIEF

Your Insights & Events Community

Join now at MHC.ie/BRIEF