MASON HAYES & CURRAN

Digital Health Mid-Year Review 2023

ISSUE 4 – JUNE 2023

Welcome to Mason Hayes & Curran's Digital Health Mid-Year Review 2023

Welcome to the fourth edition of the MHC Mid-year Digital Health Review, your guide to the ever-evolving landscape of digital health regulation in the EU.

As EU policymakers strive to foster innovation while ensuring high levels of patient safety, data privacy and cybersecurity, and health systems continue to invest in technologies that will allow them to provide care to growing populations of patients with complex and changing needs, we cover various key legal developments from the last 6 months:

- After a long running saga, and in order to avoid the possible removal of essential medical devices from the EU market, an amendment to the Medical Device Regulation (MDR) extending the Medical Device Directive (MDD) transition timelines has now been adopted. We provide the background to this development and set out the key take aways for businesses
- We take a closer look at the planned changes to EU product liability legislation that are set to have a significant impact on software developers including digital health stakeholders
- Further analysis for stakeholders in the sector is provided in our article providing an overview of some key considerations when seeking to set up decentralised trials in the EU
- We provide an overview and some updates on the status of the EU AI Act and its expected impact on the regulation of certain digital health products
- We also highlight some of the intellectual property risks involved in packaging software and hardware products together as part of a digital health offering

The MHC Digital Health Review serves as a trusted resource for keeping up with the latest trends, regulatory updates, and emerging policies in EU digital health. Whether you are a healthcare professional, a technology developer, an investor, or a policymaker, we aim to provide you with the actionable insights necessary to navigate regulatory challenges and seize the opportunities in this rapidly evolving sector. We hope you enjoy this edition of the Review.

Editors

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

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

Brian McElligott
Partner,
Head of AI
brianmcelligott@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.

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.

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

Update: Product Liability for Digital Health Products in the EU

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

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

Digital health products and services delivered using technologies such as wearable devices, telemedicine platforms and health apps continue to transform the way people access healthcare and manage their wellbeing. However, use of these technologies to monitor health and deliver care have created new risks that challenge some of the core rules and concepts underpinning the current product liability regime provided for under EU law.

In this article we summarise the key changes to the EU product liability landscape being brought about by three key pieces of legislation:

- A revised Product Liability Directive
- An AI Liability Directive
- The Directive on Representative Actions ("the Collective Redress Directive")

A Revised Product Liability Directive

Why?

The current EU Product Liability Directive (PLD) has been in force for nearly 40 years. In that time, technological advances and increased awareness and concern around environmental sustainability and circularity 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 European Union by a consumer

What?

The changes contained in the draft text of a proposal for a revised PLD (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. The PLD Proposal is particularly relevant to digital health stakeholders given the references to innovative and life-sustaining medical devices, software products, AI techniques and cybersecurity within the text.

How?

Some noteworthy features of the PLD Proposal include:

- **'Product':** The concept of medical device software is a well-established concept in EU product safety legislation under the EU Medical Devices Regulation (EU) 2017/745 (MDR) and In-vitro Diagnostic Device Regulation (EU) 2017/746 (IVDR).

The definition of a 'product' under the PLD Proposal would now also include software and digital manufacturing files within scope for product liability claims.

- **Terminology:** The Proposal would bring EU product liability and product safety rules into closer alignment by adopting various terms and definitions, such as 'manufacturer' and 'placing on the market', that are already in use in EU product safety legislation under the NLF, including the MDR and IVDR.
- **'Damage':** The notion of compensatable damage would be extended to include corruption of data and recognised forms of psychological injury. The €500 minimum threshold for property damage would also be removed.
- **'Defectiveness':**The PLD Proposal would add the following factors to a list of non-exhaustive criteria that can be considered when determining whether a product *"provides the safety which the public at large is entitled to expect"*:
  - The effect on the product of any ability to continue to learn after deployment
  - The effect on the product of other products that can reasonably be expected to be used together with the product
  - Product safety requirements, including safety-relevant cybersecurity requirements, and interventions related to product safety, and
  - The specific expectations of the end-users for whom the product is intended

The express inclusion of product safety requirements, cybersecurity and product safety interventions in a list of criteria for 'defectiveness' for product liability purposes is particularly important for manufacturers of products regulated under the MDR and IVDR. Indeed, the recitals to the PLD Proposal specifically mention the full product lifecycle requirements set out under the MDR in calling for liability for damage caused by *"failure to supply software security updates or upgrades that are necessary to address the product's vulnerabilities in response to evolving cybersecurity risks."*

Another particularly important feature of the PLD Proposal is a rebuttable presumption of defectiveness that could arise in circumstances where:

- The claimant establishes that the product does not comply with mandatory safety requirements laid down in EU law or national law that are intended to protect against the risk of the damage that has occurred
- The claimant establishes that the damage was caused by an "obvious malfunction" of the product during normal use or under ordinary circumstances, or
- A national court were to consider that a claimant faced "excessive difficulties" in proving defectiveness and/or causation owing to the technical or scientific complexity of a product

Again, 'innovative medical devices' and complex technologies such as machine learning are called out in the recitals to the PLD Proposal as the types of complex products warranting this type of new approach.

- **Causation:** claimants would also be able to avail of a rebuttable presumption that a defective product caused damage where:
  - He or she faced *"excessive difficulties"* in proving same owing to the technical or scientific complexity of a product, as above in relation to defectiveness, or
  - It could be 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 (which would now include software products). 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.

- **Defences:** regarding the defence currently available under the PLD that allows a defendant to escape liability if it can be proved that it is probable that the defect that caused the damage did not exist when the product was put into circulation, the PLD Proposal would close off this possible defence in cases where the defect is due to a 'related service' or software. This includes updates or upgrades or lack thereof that are required to maintain safety that is within the control of the manufacturer.
- **Limitation periods:** the 10-year longstop period would be extended to 15 years in certain cases involving latent personal injuries, another significant development for healthcare products, particularly screening and diagnostic systems. Time could also be determined to start running from the date that a product had been substantially modified (i.e. at a point after it had been placed on the market or put into service) which could give rise to new issues in the context of updates and new versions of software products.

When?

As of May 2023, a briefing published by the European Parliamentary Research Service (EPRS) noted that the EP and Council are currently working on establishing their respective positions on the draft legislation under the EU Ordinary Legislative Procedure. Most recently, the EP Committee on Internal Market and Consumer Protection (IMCO) and the Committee on Legal Affairs (JURI) have released a joint draft report on 5 April 2023 that proposes a number of changes to the draft text. It is currently not clear when the legislative text will be adopted and enter into force, however the EP committee report will need to be adopted before the EP can vote on its first reading position in a plenary sitting. Meanwhile in the Council, the Working Party on Civil Law Matters discussed a compromise text of the legislation on dates in March and April 2023. Work to reach agreement on a final text is expected to intensify throughout 2023, with the possibility of the adoption of a text before the end of the year.

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

An AI Liability Directive

Why?

As stated in the text of the relevant proposal, current national liability rules are ill-equipped to handle cases involving AI-enabled products and services. Hallmark characteristics of AI systems like opacity, complexity and autonomy can make it particularly difficult and expensive for claimants to establish who to sue and then prove how that liable person is to blame for the damage they have suffered. In response, national courts in EU Member States need to adapt how they apply existing civil liability rules in order to achieve a just result in certain cases involving AI. Several EU Member States are already pursuing their own AI civil liability strategies. Without EU-level legislation there is a risk of fragmentation, with different rules and procedures for AI cases in different Member States. This has the potential to result in increasing levels of legal uncertainty for businesses which could in turn lead to increased costs, especially for SMEs trading across borders with limited access to in-house legal and technical expertise.

What?

A proposal for an EU Artificial Intelligence Liability Directive (the AILD Proposal) therefore aims to harmonise certain aspects of fault-based EU civil liability frameworks as they apply to AI. The AILD Proposal is intended to complement planned revisions to the EU's non-fault based (strict liability) regime provided for under the Product Liability Directive and does not seek to alter well established concepts forming part of existing national civil liability systems such as 'fault' or 'damage'. Instead, it seeks to address the burden-of-proof issue in a way that interferes as little as possible with different national liability regimes.

How?

The AILD Proposal contains two key features that are particularly relevant to digital health stakeholders:

- **Access to evidence:** claimants seeking compensation would have an opportunity to obtain information on 'high-risk AI systems' (a category defined under the EU AI Act that is expected to include devices regulated under the MDR) that must be recorded and documented under the AI Act. These requests would need to be *"supported by facts and evidence sufficient to establish the plausibility of the contemplated claim for damages"*. The requested evidence would also need to be at the addressee's disposal. This measure would be open to 'potential claimants' who could request a court to order the disclosure of relevant evidence in advance of submitting a claim for damages.
- **Rebuttable presumption of causation**: the AILD Proposal also makes provision for a presumption of a causal link in the case of fault, which can trigger if a number of criteria are satisfied:
  - Firstly, the claimant needs to demonstrate a fault on the part of the defendant. This can be an instance of non-compliance with a duty of care laid down in EU or national law. In the case of 'high-risk AI systems', non-compliance with the requirements of the AI Act would constitute such a fault.
  - Secondly, the claimant would need to show that it was 'reasonably likely' that the fault had influenced the AI-system output in question, or lack thereof.
  - Thirdly, the claimant would still need to demonstrate that the output, or lack of an output, caused the damage complained of. The presumption also distinguishes between claims brought against providers and users of high-risk AI systems, and defendants may prevent the presumption from triggering in cases involving high-risk AI systems where they could demonstrate that the evidence and expertise needed for the claimant to prove a causal link is already available.

When?

Like the PLD, the Proposal AILD Proposal is currently undergoing review by the EP and the Council as part of the EU Ordinary Legislative Procedure. It is not clear when a settled text will be agreed however once adopted, the AI Liability Directive will also need to be transposed into national law. The AILD Proposal provides that Member States would be required to transpose the new legislation within 2 years of its entry into force.

The Directive on Representative Actions

Why?

Prior to the Collective Redress Directive (CRD) coming into effect, member states had different legal systems and procedures regarding collective actions, making it challenging for consumers to exercise their rights across borders. With the growth of e-commerce and the digital economy, consumer harm increasingly transcended national boundaries. Calls for updated legislation recognized the need for a unified approach to collective redress to tackle these types of cross-border consumer issues more effectively.

What?

The CRD harmonized the rules and procedures for representative actions, ensuring consistency and facilitating cross-border consumer claims while providing safeguards to prevent frivolous claims against traders. It seeks to streamline legal processes by allowing representative actions to be brought on behalf of a group of consumers with similar claims, thus reducing the burden on individuals to initiate separate legal proceedings and making the process more efficient and cost-effective. To distinguish the EU regime from the more litigious US class action procedure, the criteria required in the Directive to bring a redress action are relatively strict.

How?

- **Qualified entities:** The CRD requires each Member State to designate at least one 'qualified entity' to bring actions on behalf of consumers. A list of qualified entities will be maintained by the European Commission. Qualified entities, such as consumer organisations, will be empowered to bring collective action cases on behalf of consumers for breaches of a wide range of EU Directives and Regulations including the MDR, the GDPR and the Product Liability Directive. In order to bring a cross-border representative action, the qualified entity will have to meet certain criteria:
  - Be a non-profit organisation in the area of consumer protection
  - Be independent
  - Have a legitimate interest in ensuring that there is compliance with the provisions of the Directive

  Qualified entities will also be able to apply for injunctive relief and other redress, with injunctions potentially being granted on a preventative or prohibitive basis. In addition, qualified entities may seek redress on behalf of consumers in the form of compensation, repair, replacement, price reduction, contract termination or reimbursement. The redress awarded could vary among consumers in the group or could be the same for all consumers involved in the action. Member States will be given some flexibility as to how this will operate, and will be able to decide to either opt-in, i.e. consumers actively opt-in to being represented, or to opt-out, i.e. a consumer must express their desire not to be represented by a qualified entity. For cross-border actions, only the opt-in basis will be available.
- **Safeguards:** One of the important features of the Directive on representative actions are the safeguards which were introduced in order to ensure the system does not encourage frivolous lawsuits. These include:
  - **Loser pays principle:** The costs of the proceedings should be borne by the unsuccessful party.
  - **Dismissal of manifestly unfounded cases:** Courts will also be willing to dismiss manifestly unfounded cases at the earliest possible stage of the proceedings.
  - **Settlement:** There is also the possibility that a claim can be settled. However, such a settlement requires the approval of the court.
  - **Third party funding:** A qualified entity will be required to publicly disclose information about its sources of funding for the representative actions it brings. It is important to note that at present, third party funding in Ireland is prohibited.
  - **Multiple claims by individual consumers:** Member States will be required to lay down rules preventing consumers from bringing an individual action or being involved in another collective action against the same trader for the same infringement. Furthermore, Member States must ensure that consumers do not receive compensation more than once for the same cause of action against the same trader.

When?

The CRD was published in the Official Journal of European Union on 4 December 2020. Member States are required to adopt implementing measures by 25 December 2022 and the measures will apply from 25 June 2023. However, at the time of writing only a small number of Member States had notified the EC of implementation. The EC has therefore issued 'formal letters' to 24 Member States in relation to a failure to transpose the CRD.

Conclusion

On one hand, manufacturers of products regulated under the EU Medical Devices Regulation (EU) 2017/745 (MDR) and In-vitro Diagnostic Device Regulation (EU) 2017/746 (IVDR) may be uniquely well placed to adapt to these changes given the existing need to comply with these modern and sophisticated pieces of product safety legislation. On the other hand, however, the move to bring the EU product liability regime up to speed with updated product safety legislation is likely to give rise to increased litigation risks that will require careful management. To prepare for these incoming changes digital health stakeholders with products on the EU market should:

- Assess how the revisions contained in the current text of the Proposal would impact their product portfolios were they to become law
- Consider the impact of these proposed changes alongside other new EU legislation designed to safeguard the interests of consumers, especially the Collective Redress Directive, and
- Where necessary, identify opportunities to become involved in policy debates relating to proposed changes that could have a significant impact on particular product lines or product categories.

Learn more:

- PLD Proposal
- EC Q&As on the revision of the PLD
- EP Draft Committee Report on the PLD Proposal (April 2023)
- EPRS Briefing: New Product Liability Directive (May 2023)
- AILD Proposal
- MHC Insights: Class Actions in Ireland?

Regulatory Snapshot: MDR Transition Timelines Extended

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

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

Even before coming into effect on 26 May 2021, calls for extensions to transitional timelines provided for under Article 120 of the Medical Devices Regulation (EU) 2017/745 (MDR) were growing. In the nearly two years since, and just over a year out from the original deadline of 26 May 2024, EU legislators have recognised the pressing need to address the imminent risk of shortages of essential medical devices in the EU by publishing a new Implementing Regulation. This amends the MDR and provides manufacturers with more time to certify their devices as MDR-compliant.

Conditions

Although the extended timelines do provide extra breathing room to manufacturers and notified bodies, effective transitioning to the MDR remains the objective. Accordingly, extra time is only available to manufacturers who satisfy various specific conditions.

Extended timelines

Device class under MDR	Deadline
Class III custom-made implantable devices	26 May 2026
Class III, or Class IIb implantable devices excluding 'well-established technologies' (WET)	31 December 2027
Class IIb devices, excluding Class IIb implantable non-WET, or Class IIa devices, or Class I sterile devices or Class I devices with a measuring function	31 December 2028
Devices that did not require Notified Body certification under the Medical Device Directive (MDD) and for which the declaration of conformity was drawn up prior to 26 May 2021, but now require Notified Body certification under the MDR. Example: the majority of software medical devices, now classified under MDR, Annex VIII, Rule 11	31 December 2028

Manufacturers availing of the extended timelines must:

1. Lodge an MDR conformity assessment application and sign a formal agreement for conformity assessment services with a notified body by 26 May 2024 and 26 September 2024 respectively
2. Have an MDR-compliant quality management system in place on or before 26 May 2024, and
3. Ensure that the relevant device(s) continue to comply with the requirements of the MDD or the Active Implantable Medical Devices Directive 90/385/EEC (AIMDD)
4. Ensure that no significant changes are made to the design or intended purpose of the relevant device(s)
5. Ensure that the relevant device(s) do not present an unacceptable risk to the health or safety of patients, users or other persons, or to other aspects of the protection of public health

MDR post-market surveillance, market surveillance, vigilance and registration requirements also continue to apply to devices subject to transitional provisions.

Sell off provisions

As an added step to ensure a continued supply of essential medical devices on the EU market, 'sell-off' provisions in both the MDR (and In Vitro Diagnostic Regulation (EU) 2017/746 (IVDR)) have also now been removed. These provisions previously prevented devices already placed on the market from remaining on the market beyond a certain point. With the recent amendments, these devices can now continue to be made available until the revised expiry of the device certificate or the shelf life of the device.

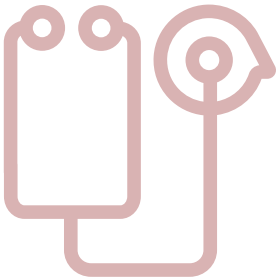
Notified bodies

Enhancing the capacity of a limited number of designated notified bodies processing a surge in demand for conformity assessment services has been identified as a key part of completing the transition to the MDR. The EU Medical Device Coordination Group (MDCG) has proposed various solutions and actions in a position paper published in August 2022 (MDCG 2022-14). The European Commission has recently acted on one of these proposals by publishing a Delegated Regulation that resets the frequency that notified bodies themselves are reassessed under the MDR to five years.

UK, Northern Ireland and Switzerland

The UK Medicines and Healthcare products Regulatory Agency (MHRA) has issued a statement regarding the extension of EU certification timelines and CE-marking, which confirms that:

- The changes to the MDR will apply automatically in Northern Ireland under the terms of the Northern Ireland Protocol
- MDD and AIMD certificates that have been extended will also be recognised as valid for placing CE marked devices on the Great British market and MHRA registration guidance will be updated to reflect this change
- The Swiss Federal Council also intends to update relevant Swiss legislation in order to maintain alignment with the updated MDR provisions. These amendments to the Medical Devices Ordinance (MedDO) and the Ordinance on In Vitro Diagnostic Medical Devices (IvDO) are currently planned for Autumn 2023.



Conclusion

Although extended timelines are a welcome development, manufacturers should maintain their efforts to certify their devices under the MDR as soon as possible. It is important to remember that extra time has only been provided to accommodate an existing backlog, and many notified bodies already have heavily oversubscribed application processes for both existing and new clients, as well as growing lead times for allocation of suitably qualified reviewers carrying out assessment projects to tight deadlines.

Manufacturers therefore need to proactively engage with their planned or existing notified body regarding quality management systems certification and the lodging of an application for conformity assessment services before May 2024, and ready their MDR technical documentation for assessment while maintaining compliance with transitional requirements in the meantime.

Learn more:

- Regulation (EU) 2023/607
- EU Commission Q&A on implementation of Regulation (EU) 2023/607
- MDCG 2022-14
- Commission Delegated Regulation (EU) 2023/502
- MHRA Notice
- Swiss Federal Council Press Release
- MHC Regulatory Snapshot: MDR Transition Timelines to be Extended (January 2023)

Update: Substantial Changes Proposed to EU AI Act

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

Conor Califf
Associate,
Product Regulatory & Liability
ccaliff@mhc.ie

MEPs in the European Parliament's Internal Market Committee and the Civil Liberties Committee recently voted on amendments to the European Commission's proposal on the EU Artificial Intelligence Act aiming to ensure that AI systems are overseen by people, and are safe, transparent, traceable, non-discriminatory and environmentally friendly. Passage of these amendments set the Act up for plenary adoption in the coming months.

We have set out below some of the key proposed changes to the Act by the Committee.

Definition of AI systems

Under Article 3(1) of the AI Act, an AI system:

"means a machine-based system designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments".

This definition was adopted by MEPs in line with the OECD's definition of an AI system and differs from the original Commission draft.[1] This definition is narrower in scope than the Commission's original proposal and is in line with what conservative political groupings in the European Parliament had been advocating for in the draft stages of the Act, left-of-centre politicians have been pushing for a broader, more encompassing understanding of the technology and its outputs. However, it should be noted the definition may yet change as the Act continues through the legislative process.

Prohibited practices under Article 5

The EU AI Act sets out several prohibited applications of AI Systems which are considered harmful, such as *"manipulative or deceptive techniques"* and social scoring. The Committee has also proposed substantially amending the list to include bans on other practices which it considers intrusive and discriminatory such as:

- "Real-time" remote biometric identification systems in publicly accessible spaces
- "Post" remote biometric identification systems, with the only exception being the ability for law enforcement to use the system for the prosecution of serious crimes and only after judicial authorization
- Biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation)
- Predictive policing systems (based on profiling, location or past criminal behaviour)

1. *Which read: "'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;"*

- Emotion recognition systems in law enforcement, border management, workplace, and educational institutions, and
- Indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases, violating human rights and right to privacy

This outright ban on several uses of biometric data follows intense lobbying from civil society groups and other EU bodies, who pushed for amendments to bolster protections for fundamental rights, with the EDPB and the EDPS among those who called for a total ban on biometric surveillance in public.

High risk categorisations and obligations under Annex III

The Act is designed to regulate AI systems on a sliding scale of risk, with four risk categories:

- Unacceptable risk
- High risk
- Limited risk
- Minimal or no risk

The Committee have made amendments to expand the category of high-risk areas to include harm to people's health, safety, fundamental rights or the environment. AI systems deployed which seek to influence voters in elections/political campaigns, and in recommender systems used by social media platforms (known as VLOPs under the Digital Services Act) have also been added to the high-risk list.

The previous draft of the Act contained significant compliance challenges for providers of those systems. The Committee has attempted to ensure that obligations for high-risk AI providers are now much more prescriptive, notably in risk management, data governance, technical documentation and record keeping. The Committee has also introduced a completely new requirement that deployers (previously called users) of high-risk AI solutions must conduct a fundamental rights impact assessment considering aspects such as the potential negative impact on the environment and on marginalised groups.

Transparency measures

Following the recent explosion of ChatGPT on to the marketplace, it is unsurprising that the Committee has included obligations for providers of foundation models to attempt to guarantee robust protection of fundamental rights, health and safety and the environment, democracy and the rule of law. This includes placing an obligation on those providers to take steps towards mitigating risks, complying with design, information and environmental requests, and registering in an EU database.

There will be additional transparency requirements for generative foundation models, such as Chat GPT or Google Bard, for example, disclosing the content was generated by AI, designing the model to prevent it from generating illegal content and publishing summaries of copyrighted data used for training.

In order to boost AI innovation, the Act also proposed to promote so-called "regulatory sandboxes", which will be exceptions to the more onerous requirements for AI providers. This will include research activities and AI components which are provided under open-source licenses.

Next steps

Finally, MEPs reformed the role for the EU AI office, which will be the regulator for the Act, giving it more powers and which will supplement decentralised oversight of the regulation at EU level.

Before negotiations with the Council and Commission on the final form of the law can begin, this draft negotiating mandate needs to be endorsed by the whole Parliament, with the vote expected during the 12-15 June session.

Learn more:

- EU AI Act: Risk Categories
- Regulating AI in the EU

Decentralised Clinical Trials in the EU: Key Considerations

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

Decentralised trials (DCTs) utilise digital and remote technologies to facilitate clinical trials and collect data from trial subjects outside of trial sites located in traditional clinical settings such as hospitals and laboratories. They can involve the use of digital tools, telemedicine and more mobile and local forms of healthcare such as home health visits, remote monitoring and diagnostics, direct-to-patient shipment of study drugs and electronic informed consent.

While the potential recruitment, retention, time and cost benefits are significant, implementing DCTs in the EU requires careful management of a number of added regulatory challenges.

In this article, we break down some important EU guidance aimed at providing clarity to stakeholders designing and conducting DCTs in the EU.

DCTs: Benefits and challenges

Although they have the potential to address many practical challenges that traditional clinical trials can give rise to, the possible benefits offered by DCTs come with their own set of unique regulatory considerations.

Benefits:

- **Improved participation:** DCTs can reduce travel burden on patients by allowing them to participate in the trial from their homes, thus increasing participation rates. This can also potentially lead to a more varied pool of potential participants located further away from a hospital or lab where investigators are based.
- **New sources of data:** DCTs can allow fewer study personnel to gather objective data in real time, reducing reliance on a larger number of investigators to perform participant evaluations. Effectively managed, this has the potential to reduce variability of data collected and allow for faster responses to safety issues.
- **Reduced costs:** DCTs have the potential to reduce the overall costs of clinical trials by reducing reliance on fixed physical sites, reducing the number of site visits, and decreasing the need for on-site monitoring.
- **Improved efficiency:** DCTs offer the possibility of accelerating trial timelines in appropriate cases by eliminating travel time, reducing data entry time and allowing for real-time monitoring.

Challenges:

- **Patient safety and data integrity:** DCTs must have robust systems in place to ensure that patient safety and data integrity are maintained, including appropriate oversight, monitoring, and data management systems.
- **Adequate oversight:** Regulators must ensure that DCTs are appropriately designed and executed, and that sufficient oversight is provided to ensure that the trial meets regulatory requirements.
- **Data privacy:** DCTs must adhere to strict data privacy regulations, including GDPR compliance, to protect patient privacy and ensure that patient data is not compromised.
- **Trial consistency:** DCTs may introduce additional sources of variability, such as differences in digital tools and devices or internet connectivity, which may impact trial results and the credibility of trial results.

DCTs in the EU

Assessing the appropriateness of decentralised elements as well as detailed planning regarding their actual use require sponsors and investigators to carefully consider various new and unique factors, adherence to EU and national member state laws and regulations, as well as established EU and international standards, guidance and principles related to clinical trials. For example:

- The Clinical Trial Regulation (EU) 536/2014 (CTR) or Clinical Trials Directive 2001/20/EC (CTD) (as applicable)
- ICH E6 (R2) Guideline for Good Clinical Practice (ICH E6)[1]
- EudraLex – Volume 4 – Good Manufacturing Practice (GMP) Guidelines (in particular Annex 13 on manufacture of investigational medicinal products (IMPs))
- Guidelines on Good Distribution Practice (GDP) of Medicinal Products for Human Use
- Guidelines on Good Pharmacovigilance Practices (GVP)
- World Medical Association Declaration of Helsinki: ethical principles for medical research involving human subjects (2013)
- General Data Protection Regulation (EU) 2016/679 (GDPR)

In December 2022, the European Medicines Agency (EMA) and Heads of Medicines Agency (HMA) published a Recommendation Paper on Decentralised Elements in Clinical Trials (the Recommendation Paper) which aims to deliver a non-binding but harmonised perspective on the use of decentralised elements in clinical trials in the EU/EEA.

The Recommendation Paper builds on previous guidance issued during the COVID-19 pandemic and sets out the joint recommendations of the EMA and HMA under a number of headings:

General considerations

Risk assessment: Where decentralised elements are likely to have a significant impact on scientific validity, data integrity, benefit-risk ratio or impact on trial participants' rights, this should form the basis of a separate documented risk-benefit assessment, with any resulting mitigation actions clearly described in the clinical trial protocol. A summary of the decentralised elements proposed as part of a study should be set out in the cover letter of the clinical trial application to assist in assessment by regulators and ethics committees.

Contingency plans: These should be in place to account for the possible failure of any critical-to-quality decentralised element of the trial such as malfunction of a digital tool or disruption of a planned decentralised visit.

Use of ICT and medical devices: The use of IT devices and systems for the creation and capture of electronic clinical data should be fit for purpose and compliant with the 'Guideline on computerised systems and electronic data in clinical trials' EMA/226170/2021.[2] Use of medical devices and IVDs in a clinical trial must ensure compliance with the Medical Devices Regulation (EU) 2017/745 (MDR) and In-vitro Diagnostic Device Regulation (EU) 2017/746 (IVDR) respectively.

Data management: data generated as part of trials using decentralised elements is subject to the same requirements as data from trials using on-site procedures. In order to ensure the scientific quality of data collected, sponsors should carefully scope potential challenges and how they plan to address any challenges introduced via the use of decentralised elements. This becomes particularly important in the case of trials identified as pivotal in marketing authorisation applications.

1. *A draft version of ICH E6 (R3), including an Annex 1 addressing interventional trials, was published in May 2023. Work has also begun on an Annex 2 to this guidance which is intended to address additional considerations for "non-traditional" interventional trials including decentralized studies. ICH expects to be in a position to publish a draft of Annex 2 in the next 12 – 18 months.*

2. *A revised version of this guidance was published by the Good Clinical Practice Inspectors Working Group (GCP IWG) on 9 March 2023 and will come into force on 10 September 2023.*

The role of clinicians: Investigators and healthcare professionals should be involved in study design to ensure the conduct of a DCT in a way that is safe, effective and takes into full account the consequences of having less personal contact with participants and how to best manage related issues around data collection, quality and integrity.

The role of the trial participant: Sponsors and investigators should also involve potential trial participants in the design, development and implementation of a clinical trial involving decentralised elements. This type of consultative approach can lead to enhanced decision making around choice of decentralised elements in a trial, measurement of endpoints that are meaningful to patients and appropriate trial population selection. Any transfer of burden for trial relation procedures to participants that result from the use of decentralised elements must be carefully weighed against the benefits generated.

Informed consent

Although a remote process can be justified in appropriate circumstances, in general, informed consent should be sought during a physical meeting between the investigator and the potential trial participant. Regardless of whether or not all or part of the informed consent process is carried out remotely, the entire procedure for obtaining informed consent still needs to:

- Comply with the relevant principles laid down in the CTR or CTD, ICH E6, the GDPR and national legislation
- Be described in detail in the clinical trial application and the clinical trial protocol

Informed consent interviews: If a potential trial participant will not be attending a physical meeting for the informed consent interview, the clinical trial application should address the following:

- The meeting should still take place face-to-face and in real time. Deviation from this convention should be dealt with in the clinical trial application and attending issues like verification of the identity of the parties involved and sufficient understanding of study information should be addressed and justified
- Trial participants and investigators should retain an option to conduct the informed consent interview on-site if requested or deemed necessary by either party. The removal of this on-site option may be justified in certain cases
- As part of the interview process, the investigator should asses the suitability of the use of the decentralised elements of the trial with reference to the proposed participant's individual circumstances
- Decisions on the format of information relating to the trial that is provided to the potential participant (e.g. use of a digital information leaflet) should be carefully assessed and justified in the clinical trial application, again with reference to the potential participants' level of comprehension. Likewise, information should be provided to the participant in a storable and retrievable format
- Use of electronic signatures should follow national requirements and guidance on use of e-signatures. Trial participants should be able to download and print a copy of the signed and dated consent form and adapted procedures should be in place to provide for re-consent and follow-up steps via electronic means where necessary
- Where delivery of the IMP to the proposed trial participant forms part of the trial protocol (see below), it should be made clear as part of the informed consent process that contact details will be used for delivery purposes, with further information on use of contact details for this purpose to be set out in participant information materials

Trial procedures at home

The use of a trial participant's home as a location for carrying out clinical trial activities gives rise to various novel issues that need to be considered by the sponsor and investigator, for example:

- Is a given trial participant's home suitable? Are there personal or social circumstances that exclude home visits? What type of inclusion/exclusion criteria need to be developed?
- Does the performance of trial related activities in a trial participant's home give rise to additional risks? Could there be an impact on the reliability of data collected and what type of training and support might the trial participant need to mitigate this?
- The insurance or indemnity covered required by the CTR/CTD should cover any damage resulting from trial related procedures that take place at home
- Because of the reduced number of in-person visits and trial personnel, how will the investigator monitor trial participants and compliance? Trial participants should have the option to meet in-person if needed and should have a direct contact line for when they need instructions, advice or other supports
- Adverse event reporting and management procedures need to be carefully designed and implemented in order to pick up on any safety incidents taking place in the trial participant's home
- The sponsor should provide alternatives where a trial participant is unable or unwilling to use his or her own smartphone or tablet to collect data

Clinical trial oversight

DCTs will tend to effectively involve an extension of the trial site into participants' homes potentially using additional service providers such as home-visit nurses and the use of various technologies collecting and delivering data via a number of different routes.

These added variables can lead to an added burden in ensuring that the specific roles and responsibilities of the sponsor, investigator and other parties are clearly defined and that the sponsor and investigator can fulfil their legal obligations under the CTR or CTD, ICH E6 and GDPR.

Service providers: Although some DCTs may involve home visits by healthcare professionals, in accordance with ICH E6 all clinical trial related tasks are the responsibility of either the sponsor or the investigator. Therefore:

- Trial specific tasks that are delegated by a responsible party (investigator or sponsor) to a service provider should be captured in a written agreement
- Delegation of trial specific tasks to additional service providers (including the rationale underpinning same) should also be clearly documented in the trial protocol using a general workflow, with more detail on the extent of their involvement to be included in a protocol related document

Data collection and management

A key feature of DCTs is the increased involvement of trial participants, their caregivers and service providers such as home nurses in data collection activities. However, the addition of these parties as well as the systems needed to ensure that data recorded remains credible, reliable and verifiable (in accordance with ICH E6) adds to the onus on the sponsor to provide for adequate oversight:

- All parties involved in the trial should be provided with an overview of the data flow with the inclusion of a data flow diagram and associated information in the protocol being recommended
- Data acquisition tools should be configured and validated in accordance with their intended use

- Control and complete and continuous access by the investigator to both source data generated either on-site or off-site, as well as source data reported to the lab sponsor (e.g. central lab data) should be ensured
- Have in place adequate security and data integrity measures including use of encryption, firewalls, defined user rights and methods of access, and preservation of metadata

More data to manage: DCTs also create a potential for significantly increased volumes of incoming data, received via a variety of routes and from an increased pool of sources (be they participants, investigators or service providers). Management of this data needs to be informed by a risk-based perspective to effectively identify serious adverse events in a timely manner.

In addition:

- Everyone involved in the trial needs to be properly trained on any digital tools that are to be used, and how to identify, report and manage adverse events that may arise during a trial. Procedures should be developed to deal with the potential for the same adverse event to be reported through several different routes
- Where the generation of critical safety data using digital tools and the use of notifications and alerts is envisaged, the handling of these alerts should be addressed in the trial protocol. Use of a schematic overview of the information flow and respective duties of the parties involved is recommended. The tool that generates the alerts should be tested and validated. A risk mitigation plan needs to be put in place in case the tool does not work as intended

Delivery/administration of investigational medicinal products (IMPs)

Another decentralised element of a clinical trial that can be deployed in appropriate cases involves the delivery and administration of the IMP to the trial participant at home. This gives rise to a further set of issues that need to be factored into design of the trial and which should form the basis of a structured risk assessment.

Delivery: The Sponsor retains overall responsibility for the delivery process (which should be described in the clinical trial protocol or the IMP Dossier) and the various contracts or agreements defining the roles and responsibilities of the parties involved:

- From a risk management perspective, the number of separate transportation steps should be minimised and IMP should only be handed over to the trial participant or their representative or healthcare professional as the case may be, with procedures in place to confirm and record what has been despatched has been successfully delivered
- Vendors used in the delivery process should be authorised to distribute and dispense medicinal products
- The delivery process is subject to national requirements and can take a number of forms, for example:
  - Delivery from the investigator site pharmacy, a delegated pharmacy or a depot
  - Dispensing from a local pharmacy, using a prescription issued by the investigator,, subject to national laws and provided that labelling requirements in respect of IMPs are complied with

Storage and administration: Not all IMPs will be appropriate for storage or administration in a trial participant's home e.g. where the IMP has specialist or complex storage requirements or requires specialist training and equipment to effectively administer or places a disproportionate burden on the trial participant to ensure compliance with the trial protocol. Generally speaking, if an IMP needs to be administered by a trained healthcare professional, storage and administration might not be possible.

Where storage and administration at home is possible:

- The Sponsor may need to provide trial participants with additional equipment for IMP storage. The investigator should also provide realistic and feasible instructions to the trial participants on use and storage of the IMP. The decentralised storage and administration process should be described in the clinical trial protocol or related documents such as pharmacy manuals and information provided to trial participants
- Where preparation and administration of the IMP by trial participants is envisaged, they will need to be instructed and trained in advance on how to carry out these steps in compliance with the trial protocol. These instructions may need to be tailored to the specific needs of individual patients, and depending on the safety profile of the IMP, the investigator may need to arrange to contact the participant to ensure proper handling during initial preparation and administration, as well as follow up contacts to ensure ongoing compliance with the protocol
- Procedures also need to be in place for return and destruction of unused IMP from trial participants, including in the context of recalls

Conclusion

Digitally-enabled DCTs have the potential to improve recruitment and retention rates among trial participants, streamline processes in appropriate cases, and possibly facilitate new research on conditions and treatments. However, maintaining necessary safety and ethical standards in a more dynamic DCT environment requires very careful planning and management. Given their potential benefits however, stakeholders are encouraged to explore the use of decentralised elements as part of their clinical research activities.

To this end, the Recommendation Paper, as well as draft guidance recently published by the FDA, contains useful information on the particular unique regulatory considerations that should be considered and captured as part of the clinical trial protocol and related documents including contracts and agreements.

Learn more:

- EMA/HMA Recommendation Paper on Decentralised Elements in Clinical Trials (Version 01, 13 December 2022)
- FDA Draft Guidance - Decentralized Clinical Trials for Drugs, Biological Products, and Devices: Guidance for Industry, Investigators, and Other Stakeholders (May 2023)

Top 10 Guidance for Digital Health

1. Q&A on practical aspects related to the implementation of Regulation (EU) 2023/607 amending Regulations (EU) 2017/745 and (EU) 2017/746 with regards to the transitional provisions for certain medical devices and in vitro diagnostic medical devices

2. MDCG 2020-3 Rev.1
Guidance on significant changes regarding the transitional provision under Article 120 of the MDR with regard to devices covered by certificates according to MDD or AIMDD

3. Template for NB –
Confirmation letter in the framework of Regulation (EU) 2023/607

4. MHRA Guidance:
Medical devices: software applications (apps)
(Updated May 2023)

5. MHRA Guidance for manufacturers on reporting adverse incidents involving Software as a Medical Device under the vigilance system (May 2023)

6. FDA Draft Guidance: Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/ Machine Learning (AI/ML)-Enabled Device Software Functions (April 2023)

7. FDA Guidance Document:
Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices and Related Systems Under Section 524B of the FD&C Act (March 2023)

8. FDA Framework for the Use of Digital Health Technologies in Drug and Biological Product Development (March 2023)

9. MDCG 2022-4 rev. 1 (December 2022)
Guidance on appropriate surveillance regarding the transitional provisions under Article 120 of the MDR with regard to devices covered by certificates according to the MDD or the AIMDD

10. Manual on borderline and classification under Regulations (EU) 2017/745 and 2017/746 v2 (December 2022)

Controllership in App Development

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

A recent opinion from the Advocate General in the NVCS case (Opinion) underscores that controllership is a broad concept and highlights the importance of carefully considering any engagements with third parties on projects involving data processing. Our data privacy team consider a recent opinion from the Advocate General considering the concept of controllership that will be relevant to anyone engaging third parties to develop apps or provide other services such as market research surveys or clinical trials.

Background to the case

The case related to an app called "Karantinas" that was designed to collect and monitor the personal data of individuals who had been in contact with COVID-19-infected patients. The Lithuanian Ministry of Health had instructed the National Public Health Centre (NVSC) to arrange for development of the app through a public tender process. NVSC in turn told a company called "IT sprendimai sėkmei' UAB" (ITSS) it has been selected to do the development.

The app was developed, and without authorisation, by NVSC. It was made available publicly including on the Google Play Store mentioning both NVSC and ITSS as controllers. This took place before NVSC had acquired it from ITSS as initially planned as part of the official tender process and without any agreement between the parties.

The negotiations for the acquisition of the app by NVSC ultimately fell through due to lack of funding at which point NVSC notified ITSS to not refer to NVSC publicly in respect of the app, which continued to be publicly available.

The Lithuanian supervisory authority ultimately ordered the app to be suspended and started an investigation into both NVCS and ITSS for infringements of GDPR as joint controllers in respect of their processing of data of the thousands of users who had used the app. NVCS had never processed any of this data and objected to this on grounds it was not a controller.

What the Advocate General said about controllership

The Lithuanian courts referred several questions to the Court of Justice of the European Union (CJEU). Those relevant to the concept of controllership were:

First, was NVCS a controller?

Yes - subject to the Lithuanian court verifying the facts. The AG looked at factual rather than formal indicators. The fact NVCS was formally identified as controller on Google Play Store and publicly was relevant but not conclusive nor was the fact NVCS wasn't the legal owner and didn't formally approve the launch.

The key factor was whether NVCS had factually influenced the actual data processing and consented (express or implied) to the release of the app.

In this case, the AG considered the fact NVCS had commissioned the design of the app was not in and of itself sufficient. However, the AG noted that NVCS had also been involved in determining the "means" of processing by determining the data categories to be collected, from which the data subjects and other keys aspects of the processing were determined. NVCS had also determined the "purpose" by setting the objective of the app, ie collection of COVID data, and regularly modifying its functionality. Subject to the national court verifying these facts, the AG considered NVCS was a controller.

Second, did the lack of formal agreement mean there was no joint controllership?

No. The AG said this was not a pre-requisite for joint controllerships nor is a common decision between the parties.

The AG said there are only two requirements. First, each entity must satisfy the criteria of controller under Article 4 GDPR. Second, there must be "a certain relationship" between them such that they influence the processing jointly ie they must jointly participate. The AG noted this was a substantive and functional assessment not a formalistic one.

Here the AG noted that whether the parties had a formal agreement or had coordinated in respect of the development and release of the app was not relevant to determining this point.

The test in this regard was whether *"the processing would not be possible without the participation of both parties because both have a tangible impact on the determination of the purposes and means of that processing"*.

What's the impact of the Opinion?

The key takeaways from the Opinion are:

- Assessing whether you are a controller is a substantive and functional assessment, not a formal one. Whether you are named in a set of terms or a privacy policy is not determinative.
- This means it is extremely difficult to contract out of controllership obligations where you want to retain influence over the underlying processing. Even if a contract states you are not a controller or making any decisions on purposes and means of processing, if in practice you have an influence on this, you may be found to be a controller.
- Involvement in the prior steps of a project before decisions are made on the purposes and means of processing is not enough to make you a controller. For example if NVCS had simply commissioned the app but had no role in determining the data categories and data subjects affected it may not have been found to be a controller.
- Joint controllership can arise inadvertently and organically through parties collaborating in a way that jointly influences processing. The fact you have no formal agreement – or a formal agreement that states you are not acting as joint controllers - will not be determinative.

With this in mind, it is critical that companies identify all the parties involved in the project at the outset, determine which parties are controllers, joint controllers and processors carefully and take the necessary steps to ensure compliance.

For companies that are controllers – even where they are not handling any actual data – this will be discharging obligations such as providing transparency and ensuring there is a valid legal basis. For joint controllers this will mean ensuring there is a joint controllership agreement in place and obligations are allocated appropriately. For companies engaging processors this will mean ensuring there are appropriate data processing agreements in place from the outset.

The EU AI Act – Imaging and Diagnostics

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

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

The EU AI Act is set to become law later this year and providers of imaging and diagnostic artificial intelligence technology (AI) need now begin to consider its potential impacts on the regulation of their technology. Many manufacturers in this space are only just getting to grips with recently updated medical/in vitro medical device law when fresh regulatory obligations appear on the horizon relating to the use of AI in those devices. Regulators and notified bodies in the same space will also need to sit up and take notice when considering their new obligations in what is a novel technical area.

AI's impact on the imaging and diagnostic market

AI has the power to significantly grow the imaging and diagnostic technology market. It brings into our homes and daily lives the power to track, monitor and detect a range of illnesses. Paired with appropriate treatment we may all live longer and healthier lives. For the same reasons, AI also has the power to democratise essential imaging and diagnostic technology with the potential effect of treating billions of people who would otherwise suffer.

The World Health Organization cites that two-thirds of the world's population do not have access to essential radiology services, including the most basic of x-rays. Pairing AI, like Samsung's S-Detect AI, with essential imaging and diagnostic tools is proving very successful for low-resource hospitals with significant shortages of medical professionals. S-Detect is a commercially available AI that has shown diagnostic accuracy in detecting breast cancer across many studies.

Increased compliance obligations and conformity thresholds under the EU AI Act

Manufacturers operating in this space, including in the software space, are well aware of their obligations under EU medical device legislation and plan well in advance of product launches for an arduous compliance program. The thresholds of those compliance programs are about to be ramped up under the EU AI Act.

Under the AI Act, imaging and diagnostic tools that are themselves AI systems or those deploying AI systems as safety components will likely be classed as high-risk. This means they will be subject to a new conformity assessment regime specific to AI.

Manufacturers must be able to demonstrate compliance with seven detailed requirements. These include:

- Record-keeping
- Transparency, and
- The provision of information for users and human oversight

This new compliance obligation will be in addition to general safety and performance requirements provided for in Annex I of the Medical Devices Regulation (EU) 2017/745) (MDR). This lays out general requirements related to software medical devices but remains silent on AI specifically.

Pivot required for manufacturers

Manufacturers will also need to pivot their existing competencies in preparing and maintaining technical documentation for medical devices towards meeting the new technical documentation requirements under the AI Act. For example, careful consideration will need to be given to:

- The description and presentation of the intended purpose of the AI system
- The methods and steps performed in the development of the AI system, and
- Data requirements in terms of description of training methodologies and techniques, as well as information about the provenance of those data sets, their scope, and main characteristics

Some solace can be found in the fact that the new laws won't require manufacturers to deal with a new regulator. The intention is that the existing regulator in each Member State will take on a new role of overseeing compliance of these AI medical devices with the new AI Act requirements.

Comment

The market approval process for software medical and in vitro medical devices such as imaging and diagnostic tools has always been a challenge. The proposed AI Act is increasing the scope of that challenge for both manufacturers and regulators in this space. All of this means costs and resource issues for all parties involved. The balancing motivation here is ensuring the trustworthiness of the use of AI technology in what is a high-end sophisticated sector where the risk of harm is significant. The EU is determined to set the global standard of safety in this space. While there is great potential to make this life-saving technology available to a far greater portion of the population, it is still necessary to ensure the safety of those using it.

Medical Devices and the Risk of Trade Mark Infringement

When using third party products under your own brand

Hazel McDwyer
Partner,
Intellectual Property
hmcdwyer@mhc.ie

In the MedTech industry, medical device products often comprise a number of separate third party hardware and software components. In the enthusiasm to brand and launch MedTech products, particularly by start ups in this space, companies need to be aware of the risk of potential trade mark infringement, if, for example, trade marks on original products are overlabelled or products are repackaged.

The exhaustion of the trade mark rights principle establishes that where trade marked goods are put on the market, eg the EEA, with the consent of the registered proprietor, the relevant trade mark rights cannot be used to prevent further trade in those goods within the relevant market, after the first sale. This is provided for under both Irish and EU law. For example, if a company buys a product sold in the EU with the trade mark owner's consent, then the trade mark owner cannot use its trade mark rights to object to the onsale of the product in the EEA. Exhaustion does not apply where goods were put on the market without the consent of the trade mark proprietor.

There is also an exception to the exhaustion rule where there are legitimate reasons for the proprietor to oppose further commercialisation of the goods in question, particularly where the goods have been changed or impaired after being put on the market.

This issue has often arisen for pharmaceuticals, with a number of cases being brought before the CJEU where trade marked goods have been repackaged or relabelled.

The same issue can potentially arise in the context of medical devices. For example, if a third party smart watch formed part of a package for a new medical device and was relabelled or overlabelled by the medical device company, using its own brand. This could give rise to the exception to the exhaustion of rights doctrine. Third-party proprietors may object to the further commercialisation of their goods where their trade marks have been removed and/or replaced with someone else's, particularly, if, for example, the smart watch was recalibrated in some way, impairing the original product.

Medical device companies could then find themselves on the receiving end of infringement proceedings where they repackage or relabel another proprietor's product without complying with the requirements imposed on parallel importers.

Repackaging / relabelling requirements

Parallel imports or grey goods, are genuine goods purchased outside a jurisdiction (eg, the EU) and imported into the EU by a third party. This often occurs in the pharmaceuticals space. Throughout case law, the CJEU has accumulated requirements which a parallel importer must abide by when repackaging and overstickering grey goods. These include:

(a) The importer must give the trade mark owner notice of the product being put for sale and provide a sample before it goes on sale

(b) The presentation of the repackaged product must not damage the reputation of the trade mark and of the proprietor

(c) The name of the manufacturer and repackager must be stated on the outer packaging

(d) The original condition of the product must not affected, and

(e) Overstickering must be necessary

The court has held that the following may damage the reputation of a trade mark: de-branding; co-branding overstickering in any way that obscures the trade mark; and printing the name of the parallel importer in capitals. The courts in each Member State will decide the damage to the reputation in question.

The use of a third-party's product as a component of a medical device could potentially also give rise to a passing off claim in Ireland, if used in a particular way. Passing off can arise where an entity can show goodwill or reputation in its trade mark, or where there is a misrepresentation, such as due to a different label being affixed to the genuine product, which causes or is likely to cause damage to it.

Conclusion

Medical device companies should ensure they comply with the relevant conditions if using third-party products as an element of their newly developed devices.

It would be best for medical device companies to engage with the original device manufacturer prior to using their product, and to enter into a licence agreement with that proprietor to reduce the risk of any infringement claims being brought against them. The last thing a medical device company needs is to have their innovation set back by infringement or passing off proceedings, particularly on the launch of a new product on the market.

Recent Events, Webinars & Publications

Events & Webinars

- Medtech Summit 2023 (Brussels)
- Bio€quity Europe 2023
- Future Health Summit 2023
- Technology Conference – Talent, Funding and the Future
- Webinar: Commercial Contracts: What's Market 2023?
- Seminar: Data Privacy In-House Counsel Masterclass

Publications

- Medical Devices: Sources of Regulation (Thomson Reuters Practical Law Series)
- Substantial Changes Proposed to EU AI Act
- Update on the European Accessibility Act in Ireland
- Special Category Data and Bias Monitoring Under the New EU AI Act
- Lexology Getting the Deal Through Digital Health 2023
- A "SAFE" Investment
- The EU AI Act – Imaging and Diagnostics
- ChatGPT and the EU AI Act
- Notice and Takedown Obligations Under the Digital Services Act
- Cybersecurity for Digital Health in the EU
- Who's Who Legal 2023: Life Sciences

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

Martin Kelleher
Partner,
Head of Life Sciences
+353 1 614 5206
mkelleher@mhc.ie

Brian Johnston
Partner,
Privacy & Data Security
+353 1 614 7746
bjohnston@mhc.ie

Brian McElligott
Partner,
Head of AI
+353 1 614 2199
bmcelligott@mhc.ie

Hazel McDwyer
Partner,
Intellectual Property
+353 86 108 3861
hmcdwyer@mhc.ie

Dublin London New York San Francisco