MASON HAYES & CURRAN

Wearables and the Evolving Regulatory Landscape

We explore rapid advancements in the field of Wearable technology and the new and evolving EU regulatory challenges that this can present for manufacturers and industry stakeholders.

This article highlights the importance of seeking expert legal guidance to stay informed on developing EU regulations. It also emphasises the need for maintaining effective strategies to ensure ongoing compliance in this dynamic regulatory environment.

Today, the interface between humans and technology is becoming more complex than ever. One of the most significant developments is the rise of Wearable technology, which is now a category made up of basic lifestyle trackers right through to advanced exoskeletons.

While consumer demand continues to drive manufacturers to constantly innovate and improve Wearable product functionality and performance, this can also result in increased regulatory complexity and compliance burden. We examine the Wearables regulatory ecosystem in light of several relevant legislative updates and what this means for securing and maintaining compliance with EU product requirements and by extension, access to the EU market.

We have reviewed a broad spectrum of factors influencing the Wearable industry in previous insights including:

- Wearable Medical Devices: Current Challenges and Emerging Issues, and
- Fitness Trackers & Wearables – What are the Regulatory Risks?

We focus on how the legal landscape has evolved further in light of a number of important legislative developments.

Industry

The global fitness tracker market size continues to grow, with a recent valuation of $54 billion last year and a projected rise to $290.85 billion by 2032. Meanwhile, since they have entered the market, Wearables have evolved from the original basic recording of activity levels like step counts, to much more advanced physiological indicators like oxygen levels, respiratory rate, HRV and heart rate.

As the Wearable market continues to evolve, consumers now expect advanced capabilities and features. As a result, manufacturers and developers have needed to continually innovate and push product boundaries so that devices remain relevant and desirable to consumers. As a result, this has resulted in Wearables falling in scope of a much broader legal ecosystem than when these devices first entered the consumer market.

We look at each of the potential legal frameworks and flag some of the key considerations that Wearable industry stakeholders need to be mindful of. Given the various nuances under each legal regime, a careful assessment is required to determine what legal frameworks and more importantly what applicable obligations, are triggered by each specific Wearable.

What product safety framework applies?

Probably the most important initial assessment for a Wearable is its classification, which will dictate what product safety and compliance legislative framework it will need to comply with. For certain categories of products such as electrical equipment and Bluetooth / Wi-Fi enabled equipment, which would cover most Wearables, there are specific EU Directives such as the Radio Equipment Directive which will set out requisite product safety and compliance requirements. In the event that the Wearable does not utilise Bluetooth or Wi-Fi and does not engage any of the other sector specific legislation, which would seem unlikely, then the General Product Safety Regulation will apply to the product.

This replaces the General Product Safety Directive and comes into full effect from mid-December of this year.

While assessing whether the Wearable uses electronics or Wi-Fi or Bluetooth is straightforward, another question regularly arises and that is whether the Wearable could qualify as a medical device.

Is it a 'medical device'?

Wearables associated with lifestyle or fitness tracking do not routinely fall within the scope of the medical device regulatory frameworks and more specifically under the EU Medical Devices Regulation (MDR). However, these products do require a thorough assessment in terms of their accessories, hardware, and software to determine if their specifications and features have brought them within the ambit of the EU medical device regulatory regime.

In determining whether a product falls within scope of the MDR (for the purposes of this article we are not examining the possible triggering of the IVDR), we need to assess the product against the definition of a medical device found in Article 2(1) which states that a medical device is:

"... any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations[...]"*

In order to answer this question, an assessment must be carried out as to whether the device is intended to be used for a medical purpose i.e. diagnosis, treatment, etc.? In addition to the device's intended purpose, consideration must also be given to the product's functionality and the claims the manufacturer intends to make about the product.

In practical terms, this means that regardless of the manufacturer's stated intended use, products presented in a way that create an impression that they are to be used for medical purposes can also result in MDR applicability. For example, if a Wearable makes claims regarding medical benefits or diagnosis, then the device will most likely trigger MDR requirements.

Examples of Wearables that can qualify as medical devices in the EU are:

- Blood pressure monitors
- Glucose meters that help manage blood sugar levels for diabetics, and
- Heart rate monitors intended to detect irregular heart rhythms requiring further medical investigations.

Examples of Wearables that do not ordinarily qualify as medical devices in the EU can include:

- Fitness trackers that record steps and heart rate for wellness purposes
- Smart watches that record sleep habits for wellness purposes (and which don't check for any sleep disorders).

If the product triggers the definition of a medical device, its risk class will then need to be determined with reference to the MDR Classification Rules set out in Annex VIII and it will be required to conform with the Essential Requirements in Annex 1.

Software as a medical device (SaMD)

With the integration of technology into Wearable devices, it's not just the physical hardware that might be regulated as a medical device.

The integrated software can also potentially invoke the medical device frameworks where the software is considered to be a medical device in its own right. Furthermore, depending on functionality, where there is a mobile app operating alongside the Wearable, this could also potentially fall within scope of the MDR.

Assessing whether software qualifies as a medical device can be difficult because software and its integration with a given Wearable device varies in complexity, functionality, and risk. Helpfully, various pieces of guidance have been published to assist in assessing whether software is a medical device, classification of software medical devices as well as the relationship between hardware and software making up 'systems' regulated under the MDR.

Are data protection laws applicable?

The next key consideration is the data protection legislative framework.

Wearables, regardless of whether they fall in scope of the medical device regime, will almost always trigger the application of the GDPR. This is because Wearables collect, process, store and share a considerable amount of personal data. Often this can include sensitive data such as precise geolocation data or "special category data" under GDPR such as health data. For this reason, complying with GDPR can be challenging.

Some of the main obligations include:

Data protection by design

Manufacturers (as controllers under the GDPR) have an obligation to incorporate compliance with GDPR principles at the product development stage. GDPR principles include processing personal data fairly and transparently, processing personal data only for specified and explicit purposes (purpose limitation), processing only the personal data that is necessary for those purposes (data minimisation) and keeping data only as long as is necessary.

Manufacturers and developers will be expected to have given due regard to these principles when designing the Wearable and when processing the personal data generated by the Wearable. The onus is on the manufacturer to demonstrate compliance with this obligation. This can be demonstrated through carrying out privacy assessments such as a 'data protection impact assessment' (DPIA), where necessary. A DPIA helps to assess the level of risk associated with the Wearable's processing and identify appropriate safeguards and measures that should be in place.

To properly assess such risks and ensure compliance, it is very important that cross-functional teams work closely to understand the following issues:

- What data is processed?
- For how long is it retained?
- Who has access to the data?
- How is the data secured?
- With whom is the data shared?

Compliance cannot be treated as a last-minute consideration or an afterthought at the end of a product's development. It must be 'baked in' during the product design and development process.

Lawfulness

Processing must also be lawful. There are six lawful bases set out in the GDPR which may apply to different aspects of the processing. In the context of Wearables, the most relevant bases for data processing are likely to include:

- Processing necessary for the performance of a contract with the user. This could include things like setting up a user's account and providing the core functionality to the user, such as integrating the Wearable with other apps and services, and where requested by the user
- Processing necessary for the purpose of pursuing "legitimate interests". This could be for product improvement purposes or research and development.
- Obtaining the consent of the user, such as for processing of health data (where explicit consent is often needed) or for advertising.

Understanding the nature of the data being processed is important to determine the appropriate legal bases. The correct determination is the responsibility of the manufacturer and will need to be relied on by a manufacturer.

Transparency

Users must have been provided with transparent information about the processing prior to any processing taking place. This means ensuring there is an appropriate privacy policy which explains what personal data is being collected and processed, the purposes of that processing (and the legal bases), how long the data is being kept and the third parties with which it is being shared. Steps must also be taken to ensure the privacy policy is accessible to users in an appropriate manner, such as surfacing it as part of the account creation flow or by way of email or in-app notification whenever there is a material update to the privacy policy.

Achieving compliance with lawfulness and transparency principles is also closely linked to the principle of fairness. Manufacturers should provide data subjects with clear and informative information which is not overly technical in nature to allow them to readily understand how their personal data will be processed. This means that information should be presented in straightforward language and be easily accessible.

Regulators take compliance with data protection principles, such as transparency and lawfulness, very seriously. Regulatory enforcement related to this aspect of the GDPR has often resulted in significant fines and remains an area of focus in the EU.

Data sharing and transfers

Manufacturers and developers who share personal data with third parties such as advertisers, or other third-party apps, must ensure that this data sharing is done in an informed and compliant manner. This means manufacturers must be clear with users about how their personal data will be shared with any third parties and the purposes for the sharing. In most cases, manufacturers might need to offer users a choice about whether such sharing takes place. Manufacturers and developers should also consider their relationships with such third parties. Where there is a significant data sharing, it is often appropriate to put in place a contract governing the relationship which clearly states the role of the parties, how personal data can be used, and how data subjects' personal data is fully protected. In cases where parties are jointly making decisions on how personal data is to be processed, they will be considered "joint controllers". This can trigger additional obligations under GDPR, including the need to enter into a joint control arrangement and make the essence of this arrangement available to users.

If the manufacturer is transferring personal data of EU users to a third country, whether to an affiliate or a third party, then an assessment must also be completed to determine the appropriate transferring mechanism. If the recipient of the data is based in a country that is not deemed adequate by the EU, then in most cases, the manufacturer will need to put in place Standard Contractual Clauses (SCCs) or seek to rely on any certifications obtaining under the EU-US Data Privacy Framework.

Security considerations

Ensuring there is appropriate security in place to protect data being processed is critical. This involves ensuring data is appropriately stored securely, appropriate measures are in place to prevent unauthorised access and, access internally is limited to authorised employees and those who have a need to access such data, e.g. product improvement employees etc. It also involves regular testing to ensure safeguards and protections are robust.

The threat posed by criminals is significant with attacks on companies' IT infrastructure becoming increasingly sophisticated, such as through ransomware attacks or phishing. It is critical that manufacturers ensure the measures in place are up to date and appropriate to its specific risks. This can include ensuring data is encrypted, ensuring the data is securely stored, and conducting regular software updates to ensure newly discovered vulnerabilities are addressed. For example, if Wearable products are caught by NACE Code C26, then the NIS2 Directive would apply if the relevant company has at least 50 employees and over €10m in annual turnover.

In addition to having appropriate security in place, manufacturers should have appropriate policies in place to react to any security incidents if and when they arise. This involves implementing an incident response plan, developing policies and procedures which personnel can follow and understanding the various breach reporting and notification obligations that apply.

Will the Data Act apply?

The EU Data Act will also generate additional data obligations. This new legal framework applies to manufacturers of "connected products or related services" and so many Wearable manufacturers will fall in scope. Connected products could include pacemakers, continuous glucose monitors and smart insulin pens, as well as various Wearables, ingestible sensors, MRI and X-ray scanners.

The EU Data Act covers non-personal data and personal data and so, it is broader than the GDPR. As a result, the rules prescribed by the EU Data Act apply to data generated through use of the Wearable and its connected interface or integrated application. This encompasses data that users intentionally record, such as entering their menstrual cycle dates into the device's interface, as well as data that is indirectly generated during periods of inactivity, for instance, when the device is in standby mode or even when it is turned off.

The EU Data Act creates rights and obligations for different parties.

In summary:

- The EU Data Act applies to manufacturer/providers of connected products and related services.
- It creates onerous new obligations to make data directly accessible or at least readily available to users, third parties (where requested by the user) and public bodies (in exceptional cases).
- It imposes obligations that impact how products and services must be designed.
- It requires transparency to be given upfront to users about the data that will be generated through the connected products and related services.
- It requires manufacturers to make arrangements to share data with third parties (where requested by a user). This means manufacturers/providers need to consider measures (technical and contractual) to protect their interests and rights, such as IP/trade secrets.
- It gives users the right to make a complaint in the event there is non-compliance.

This EU Data Act is now in force; however, a transitional period of 20 months has been afforded meaning that it does not take effect until September 2025.

While manufacturers have some time before these rules become effective, now is the time to determine how compliance can be achieved given the scale of the new obligations and also how this new framework will co-exist with overlapping legislative regimes already in full force. Assessing how design and data access rules can be complied with, including how they interplay with the GDPR, and its associated cybersecurity obligations will be a difficult exercise for many. Similarly, if Wearables designated as a medical device undergo significant modifications so as to comply with this new regime; this could result in adverse knock-on implications with respect to its compliance with the MDR or IVDR. As a result, manufacturers will need to carefully map the various regimes that may apply to its Wearables. From there, it will need to develop a well-structured and considered compliance plan.

Will the AI Act apply?

Another legislative regime that requires careful consideration is the recently enacted EU AI Act. This new legislative instrument is like many of the aforementioned regimes, in that it is far-reaching and onerous on certain uses of AI systems. As a result, manufacturers and developers incorporating the capabilities of AI must now determine whether the AI Act is applicable.

The AI Act is intended to be industry-agnostic, applying across a wide range of sectors including life sciences, healthcare, financial services and consumer products. It also applies to a broad array of economic operators active in the AI supply chain, including providers, importers, distributors, and deployers of AI systems as well as AI product manufacturers.

Each of the Wearables economic operators, if applicable, in the supply chain will have responsibilities. In this case the manufacturer / developers will be designated the providers of the AI system. Like many products, Wearables, including medical device Wearables, have integrated AI solutions into their devices' development. As a result, the AI Act will be applied.

The next consideration is determining the level of risk associated with the intended use of the AI system. There are four risk categories prescribed by the AI Act:

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

Unacceptable risk includes AI systems which are considered a serious threat and will be banned from the EU market by 2 February 2025. An example would include Wearables whose specific purpose is to categorise individuals by using their biometric data to infer an individual's race, religion, or sexual orientation.

High-risk AI systems is the broader risk category and one which prescribes the most obligations. Wearables incorporating AI which are classified as a medical device under either the MDR (or the IVDR) and which require Notified Body certification will fall within this category.

If a Wearable falls within the high-risk AI system category, a significant compliance undertaking will be required (including a pre-market launch conformity assessment and post-market monitoring regime). Specifically, seven detailed requirements require manufacturers and developers to substantially revise their processes and device procedures to ensure compliance with this regime. These are:

1. Risk management
2. Accuracy, robustness and cybersecurity
3. Data and data governance
4. Human oversight
5. Transparency and provision of information to users
6. Record keeping, and
7. Technical documentation

Some of these requirements are already provided for under the MDR (and IVDR). Manufacturers of Wearables in scope of these regimes are not required to carry out two distinct assessments. However, they must map the additional obligations required under the AI Act as part of a combined conformity assessment with the same market surveillance authority. While this is helpful, completing this gap assessment between the AI Act and the MDR / IVDR will require careful consideration and cross sector expert analysis.

Does the EU Batteries Regulation apply?

Again, as with most of the legislation referenced in this article, the new EU Batteries Regulation[1] is much wider reaching than that of its predecessor. This new regulation applies to all batteries as well as battery management systems, including those placed in or used for Wearables.

Like with the AI Act, the Batteries Regulation imposes obligations to entities across the economic chain including manufacturers, importers, and distributors of batteries and of medical devices that incorporate batteries. This includes those companies who produce these products. It also applies to companies who have the products produced for them and then sell the products under their own name or trademark.

The primary obligation under the Batteries Regulation is that batteries placed on the market or put into service shall not present a risk to human health, to the safety of persons, to property, or to the environment. However, the Batteries Regulation outlines more detailed obligations concerning sustainability, safety requirements, as well as labelling and information standards. Read more on the application of the Batteries Regulation to MedTech in our dedicated insight.

Consumer protection considerations

EU Consumer Protection laws have undergone significant reform over the last number of years to ensure more appropriate safeguards for consumers in today's digital world. While there are too many to include here, by way of example, the Modernisation and Enforcement Directive 2019/2161, or 'Omnibus Directive', seeks to update and strengthen existing consumer protection laws through a range of measures. These include improved transparency and outcomes for consumers buying goods and services online and the identification and regulation of fake customer reviews and hidden paid-for advertising. The most significant feature of the Omnibus Directive is the increased enforcement for breaches of consumer law. The Omnibus Directive seeks to impose fines of not less than 4% of the trader's annual turnover, or at least €2 million when information on turnover cannot be obtained.

In addition, the Unfair Commercial Practices Directive (UCPD) underwent significant overhaul, last updated in March 2024[2]. The Directive empowers consumers with a right to receive better protection against misleading information and commercial practices. As a result, not only must manufacturers be extremely careful of their claims and labelling so that they don't inadvertently trigger the application of the medical devices regulatory regime, but they must also ensure that they don't mislead consumers under the UCPD. Recent updates to the UCPD, inserted using the Green Transition Directive, have focused on combating misleading 'green claims' for instance, however, any false and inaccurate information which consumers rely upon to enter into a transaction to purchase products can result in adverse consequences for manufacturers.

[1] *Regulation (EU) 2023/1542*

[2] *Directive (EU) 2024/825 of the European Parliament and of the Council of 28 February 2024 amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and through better information.*

Liability considerations

To compliment the aforementioned consumer protection framework, reform is also underway regarding the rules governing EU product liability claims, which enable consumers to issue proceedings in relation to damage caused by defective products. A revised Product Liability Directive (the PLD) has now been adopted by the European Council which, amongst other things, extends the definition of product to include software and standalone software. Given that software is an integral part of Wearables, and that Wearables tend to be accompanied by apps, the revised PLD will have significant implications for manufacturers. In addition, for Wearables using AI, an AI Liability Directive is currently under consideration, which would seek to harmonise fault-based liability rules in National Member States and if adopted, would change the liability rules applicable to such devices.

The coming into force of other pieces of EU legislation like the Collective Redress Directive also brings with it an increased potential for litigation and class action-style claims brought by groups of EU consumers. This in turn increases the likelihood of a whole new body of case law forming across the EU concerning liability for defective Wearable devices and the software connected to them.

Sustainability legislative issues to be considered?

Ecodesign and Right to Repair

The EU is introducing a range of legislative measures aimed at achieving a more circular economy by encouraging consumers to choose repair over replacement. For example, the new Ecodesign for Sustainable Products Regulation entered into force on 18 July 2024. The new Right to Repair Directive entered into force on 30 July 2024, and Member States will be required to adopt national measures giving effect to this Directive by 31 July 2026 at the latest.

The Ecodesign Regulation applies to "any physical goods" placed on the EU market. The Regulation itself does not specify sustainability requirements for certain products. Rather, it creates a framework for the Commission to adopt information and/or performance requirements in the context of product durability, repairability, energy efficiency, carbon footprint, etc. The Commission will initially focus on setting requirements for certain sectors including electronics and information and communications technology. The first of these eco-design requirements are expected to apply from 2027/2028.

The Right to Repair Directive imposes repair obligations on manufacturers "of tangible movable items" across all industry sectors, whether they are established inside or outside the European Union. The scope of the repair obligation is currently limited to goods for which 'repairability requirements' are provided by another European Union Act listed in Annex II of the Directive. The repair obligation is also limited to circumstances where repair is technically possible. The Directive introduces a "right to repair" for consumers, even beyond the expiry of the warranty period. This is to make it easier and more cost-effective for consumers to repair products to keep them in circulation for longer.

Consumers will have the right to request that the manufacturer (or their repair sub-contractor) carry out a repair within a reasonable period of time, either free of charge or at a reasonable price. Further, the Directive prohibits manufacturers from using contractual clauses, hardware or software techniques that impede the repair of goods unless these are justified by legitimate and objective factors.

This new eco-design and repair legislation will likely have a particular impact on manufacturers of products from the consumer and technology sectors. In particular, the Right to Repair Directive will open the aftersales markets for these products, although this will be subject to the requirement to offer repair either free of charge or at a reasonable cost. Manufacturers will likely face competition from independent repairers who may fix products at lower costs.

WEEE

The EU's WEEE Directive aims to achieve collection, recycling, and recovery targets for waste electrical and electronic equipment (WEEE) by establishing extended producer responsibility (EPR) requirements. Broadly speaking, any entity placing EEE on the Irish market that is manufactured in its own name, imports EEE or sells EEE by distance sales is required to register as an EEE producer. Producers must file returns on the quantity of EEE they place on the market, contribute to the cost of the safe collection of WEEE from consumers, and display certain information regarding the hazardous properties of WEEE.

Packaging and packaging waste

The packaging of products also attracts environmental obligations. The EU's Packaging Directive aims to achieve collection, recycling, and recovery targets for glass, plastic, paper, board, metal, and wood. Broadly speaking, businesses that sell or otherwise supply to other persons packaging material, packaging or packaged products above certain thresholds must join an EPR compliance scheme.

Obligations include reporting on the quantity of packaging placed on the market, financing the take-back of waste packaging, and ensuring minimum recovery targets are met.

Comment

Wearables have evolved significantly from their initial basic pedometer functionality to revolutionary tools that can transform lives. This evolution reflects a continued demand for enhanced functionality and innovative new features amongst a growing number of consumers of Wearable technologies. However, ground-breaking technological advancements can often come with an increased regulatory burden.

New legislative developments such as the Data Act, the AI Act and the proposed Product Liability Directive mean that manufacturers and developers must now consider a unique array of overlapping regulatory frameworks in respect of any given product.

Assessing which modern day Wearables trigger which frameworks can be challenging, seeing as many new laws now introduce novel and complex requirements. Additionally, understanding how each law aligns with the other is not always straightforward.

As a result, cross-sector specialist legal advice should be obtained by manufactures, developers and other industry stakeholders in order to determine what regimes are applicable and to construct a compliance strategy that satisfies the requirements of the various in scope frameworks in respect of any given product.

For more information and expert advice please contact a member of our dedicated Life Sciences team.

About Us

We are a business law firm with 120 partners and offices in Dublin, London, New York and San Francisco.

Our legal services are grounded in deep expertise and informed by practical experience. We tailor our advice to our clients' business and strategic objectives, giving them clear recommendations. This allows clients to make good, informed decisions and to anticipate and successfully navigate even the most complex matters.

Our service is award-winning and innovative. This approach is how we make a valuable and practical contribution to each client's objectives.

Life Sciences at Mason Hayes & Curran

Ireland is a globally recognised centre of excellence for life sciences, pharma and medtech companies, ranging from global multinationals to an increasing number of vibrant indigenous companies.

Our Life Sciences team, drawn from specialist practice areas across the firm, offers commercial and practical advice to global players and emerging companies alike. Our key strength is our industry knowledge and expertise. Many of our lawyers have backgrounds in industry, science and medicine.

Life sciences companies require a special blend of legal advice and industry knowledge. We advise on a variety of issues from the development, protection and licensing of intellectual property to clinical and regulatory matters.

We also advise on a number of other areas affecting the life sciences sector. In particular, we have deep expertise on the intersection of technology and healthcare law and are one of the few advisors in Ireland with this expertise.

Recent Awards & Recognition

Client Choice Awards 2024 Winner

Michaela Herron was recently named the sole winner of the 'Life Sciences in Ireland' award at the Lexology Client Choice Awards 2024.

Learn more

2024 WWL Life Sciences Rankings

Following the publication of Who's Who Legal's 2024 research, we continue to be the only Irish law firm with a 'recommended' lawyer ranked in all four specialist areas for Life Sciences including Patent Litigation, Transactional, Product Liability, and Regulatory.

Learn more

What others say about us

Our Life Sciences Team

"They are solution-focused, collaborative and responsive and they get to grips with complex matters very quickly."

Chambers & Partners, 2024

Our Life Sciences Team

"The firm is notably engaged, both intellectually and pragmatically, in the analysis and management of clients' positions and interests."

Chambers & Partners, 2024

Our Life Sciences Team

"Michaela and her team have a culture of customer service in her organization that is unmatched by other firms we've worked with."

Lexology Client Choice

Key Contacts

Michaela Herron
Head of Products & Head of Life Sciences
+353 86 607 6005
mherron@mhc.ie

Jamie Gallagher
Partner, Life Sciences Regulatory
+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 Artificial Intelligence
+353 86 150 4771
brianmcelligott@mhc.ie

Jay Sattin
Partner, ESG & Governance
+353 86 078 8295
jsattin@mhc.ie