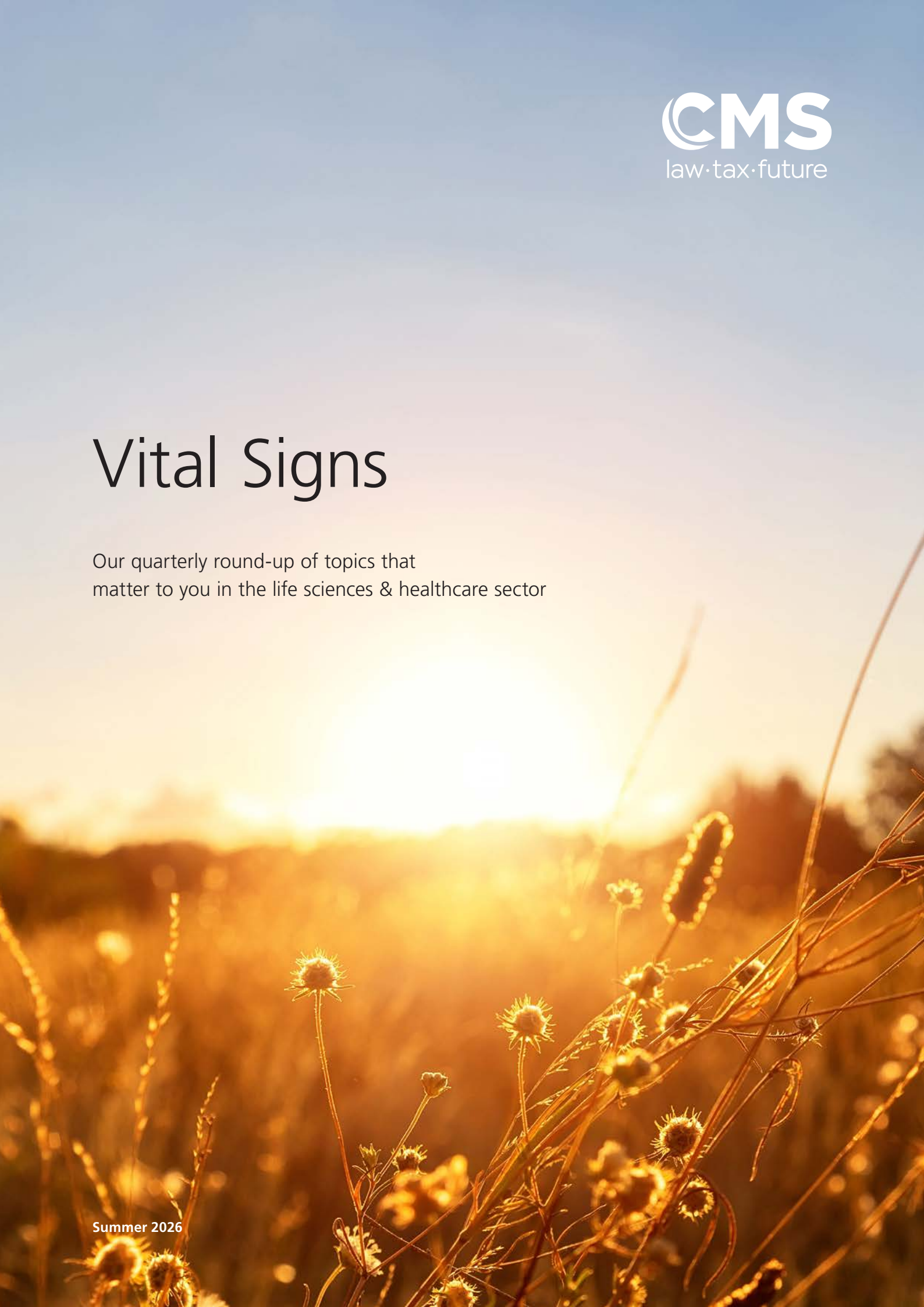
CMS
law·tax·future

Vital Signs

Our quarterly round-up of topics that
matter to you in the life sciences & healthcare sector



Summer 2026

Contents

Introduction

We are pleased to bring you the summer edition of Vital Signs, our quarterly round-up of legal and regulatory developments shaping the life sciences and healthcare sector.

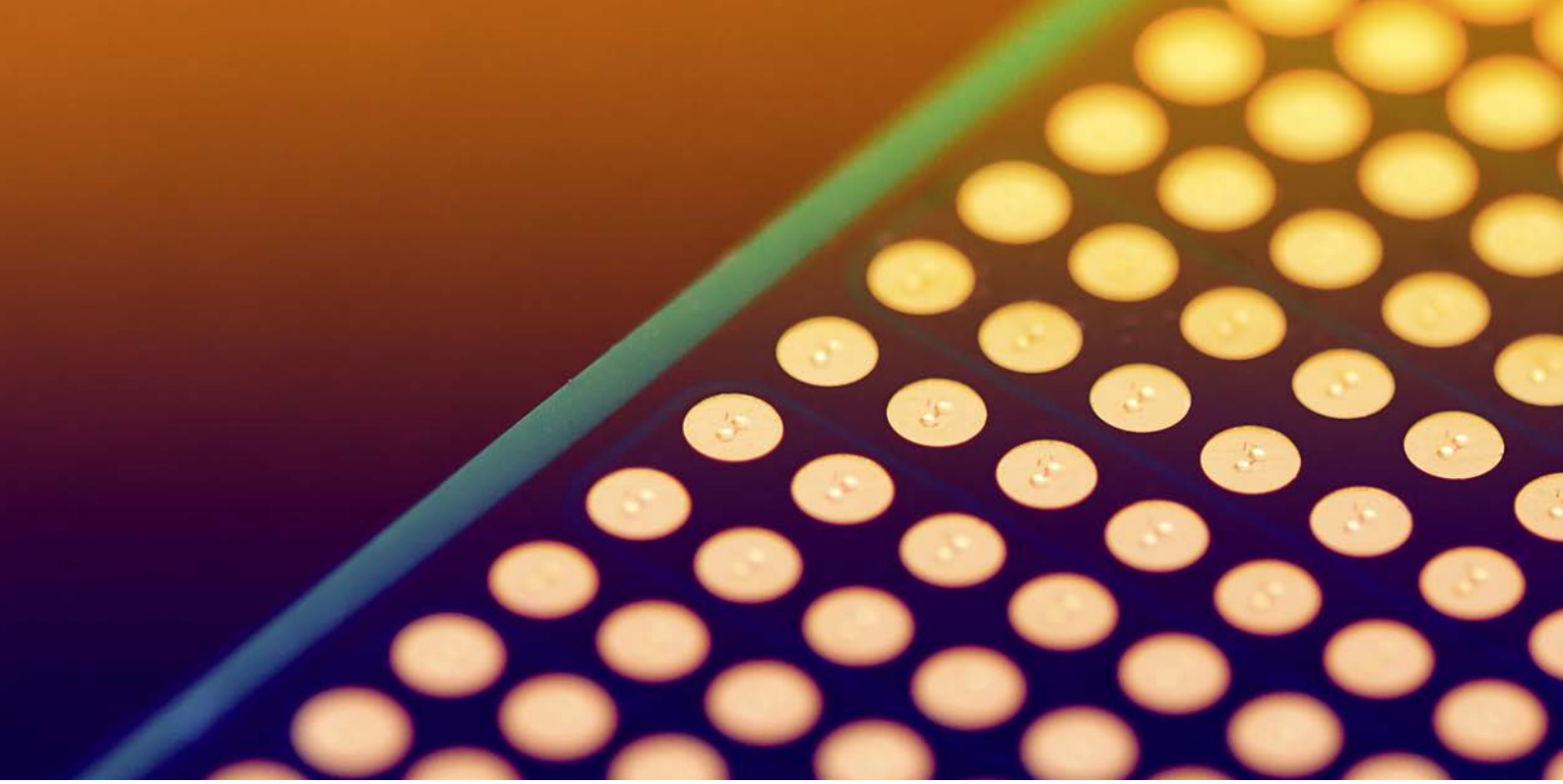
In this issue, we consider the growing cyber threat facing life sciences and healthcare organisations, including recent incidents affecting Novo Nordisk's clinical trial data and the Synnovis ransomware attack, and why boards and executive leadership must now treat cyber preparedness as a leadership priority rather than solely an IT matter.

Staying with Novo Nordisk, we examine the High Court's landmark decision to order internet service providers to block websites selling counterfeit and unlicensed semaglutide products such as Ozempic and Wegovy — the first ruling of its kind to extend website blocking injunctions into the field of public health, together with the follow-up dynamic blocking order and what both mean for pharmaceutical companies facing online counterfeiting threats.

We then turn to Poland, where a recent amendment to the rules on medicinal product advertising now permits pharmaceutical companies to provide mandatory information to healthcare professionals via QR codes or hyperlinks, rather than reproducing it in full within advertising materials themselves. It's a modest change on paper, but one that promises a meaningful practical impact for companies in the sector operating in Poland. We also take a broader look across the region, surveying the key regulatory developments facing life sciences and healthcare companies in Central and Eastern Europe and the Adriatic region in 2026 — from the transposition of the cybersecurity EU NIS2 Directive, to shifting market access and reimbursement rules, tightening anti-corruption frameworks, and the approaching deadline for implementation of the new EU Product Liability Directive.

We hope this summer edition offers useful perspectives as you navigate these developments, and as always, our team remains on hand to discuss any of the topics covered.

David Bridge
Partner, Solicitor Advocate,
Co-Head Life Sciences & Healthcare
T +44 20 7367 3021
E david.bridge@cms-cmno.com



Cyber Security in Healthcare and Life Sciences: A Leadership Priority

Cyber threats are escalating across every sector. For healthcare and life sciences organisations, a cyber incident can disrupt critical services, compromise sensitive patient data and undermine public trust, creating financial, legal, operational, regulatory and reputational consequences that reach far beyond the IT function. As a result, cyber preparedness is no longer simply an operational concern. It is a leadership priority.

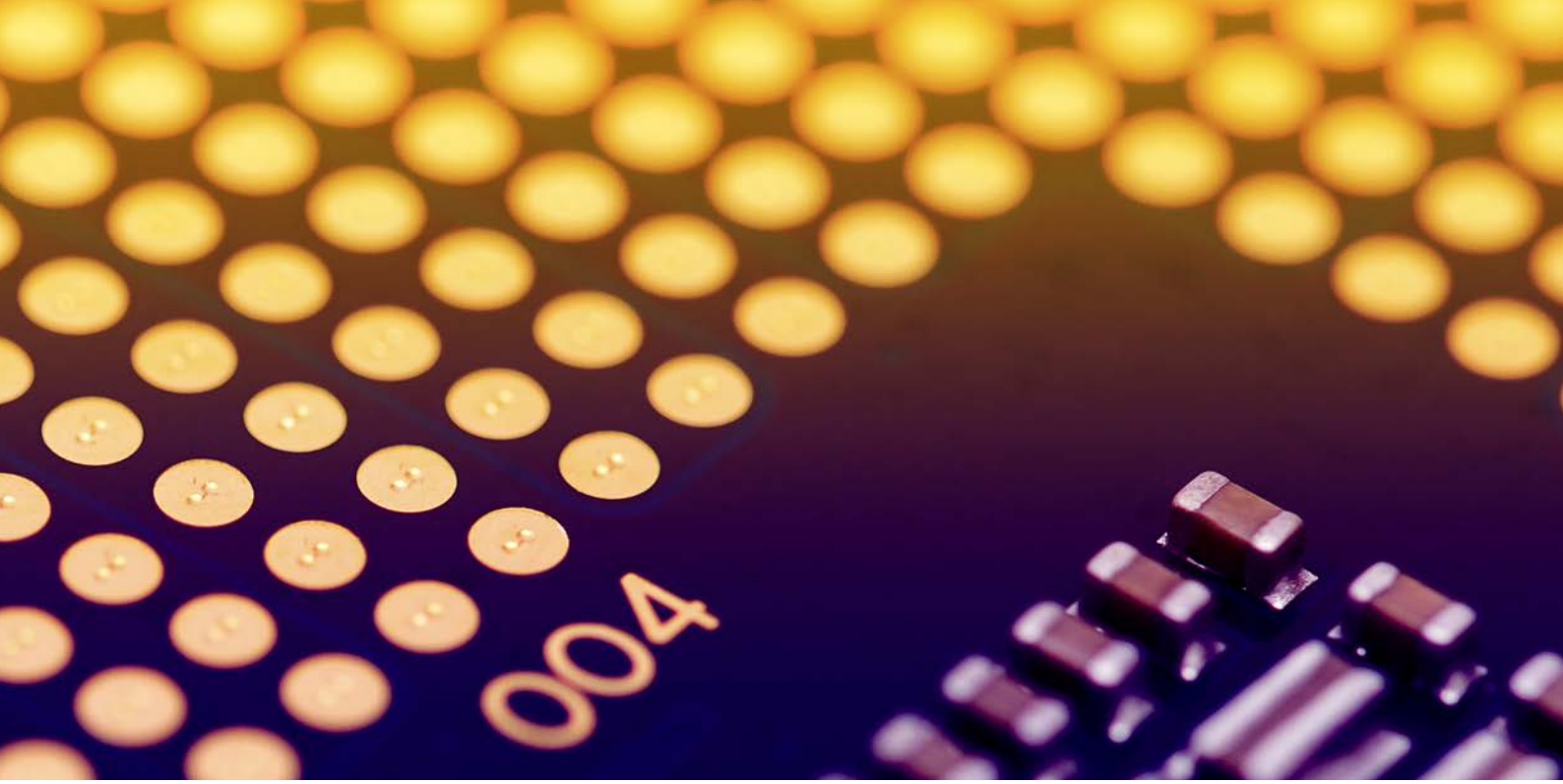
Risks

Recent incidents illustrate the scale of the threat facing the sectors. In June 2026, Novo Nordisk disclosed a cyber security incident involving unauthorised access to certain internal IT systems. The incident affected pseudonymised data relating to participants in some clinical trials, including patient identification numbers, sex, year of birth and certain health-related information.[1] In healthcare, the June 2024 ransomware attack on pathology service provider Synnovis demonstrates the potential widespread consequences. Sensitive patient data was stolen, servers across multiple NHS organisations were disrupted, more than 11,000 appointments and procedures were delayed and it has been confirmed that the attack was a contributing factor in the death of a patient.[2] [3]

Cyber security is a boardroom issue

Cyber preparedness cannot be delegated and ignored. While responsibility for day-to-day cyber security may sit within the IT or data team, ultimate accountability rests with the board and executive leadership. Senior leaders must understand the cyber risks facing their organisation, appreciate the potential impact of an attack on clinical and operational systems and ensure that appropriate safeguards, governance structures and incident response plans are in place.

Leadership responsibility is reinforced by law, not merely good practice. Under the Network and Information Systems Regulations 2018[4], NHS and certain independent healthcare providers are subject to cyber security and incident reporting obligations, with significant incidents requiring prompt reporting. These obligations sit alongside UK GDPR breach-reporting requirements and are expected to be strengthened by the proposed Cyber Security and Resilience Bill.[5]



The preparedness gap

Despite the scale of the threat, our report, *The Cyber Continuum: Ready, Resilient, Recovered,* published in May 2026, shows that confidence in cyber preparedness often outstrips actual readiness. Our report suggests that those in the life sciences and healthcare sectors would benefit from additional work on preparedness:

— In the life sciences and pharmaceutical sector, only 48% of businesses reported being very confident in their preparedness, compared with the cross-sector average of 64%; and

— Organisations providing health services are frequently reliant on third parties, which our report identified as something of a "blind spot" for boards when it comes to cyber security.

Steps to improve preparedness

Those in the life sciences and healthcare sectors can consider the report's four recommendations to improve the preparation for a cyber incident:

— **Audit and actively support suppliers:** only 37% of respondents had audited the cyber credentials of key suppliers in the past 12 months, even though 30% of breaches in 2025 were linked to third-party involvement;

— **Embed cybersecurity culture beyond basic communication:** although 99% of businesses claimed to have strong cybersecurity culture, only 48% had departmental cybersecurity ambassadors and just 41% offered employee incentives to promote good practice;

— **Prepare with simulation and training:** these are essential to test escalation protocol and build "muscle memory" for a real incident. Only 40% of respondents had run a breach simulation in the past 12 months;

— **Use cyber insurance as more than financial support:** while 82% of respondents held cyber insurance, only 52% had designated external cybersecurity breach legal counsel in place who should be involved in simulation exercises in advance so that working relationships are established before a real breach occurs.

Taken together, CMS report recommendations point to a clear message for healthcare and life sciences leaders: preparedness must be treated as a continuous, board-owned discipline rather than a box ticking exercise with suppliers. Culture, simulations and insurance arrangements should all be regularly tested and refreshed.

You can download a copy of our full report here - The Cyber Continuum: Ready, Resilient, Recovered

If you would like assistance in developing your cyber security strategy or handling a data breach, please let us know. CMS also runs a dedicated 24/7/365 emergency response facility that can be accessed in the event of a cyber attack. CMS Emergency Response Support Line | International law firm CMS UK.

---

[1] News Details
[2] Written statements - Written questions, answers and statements - UK Parliament
[3] NHS ransomware attack contributed to patient's death - BBC News
[4] Network and information systems (NIS) regulations 2018: health sector guide - GOV.UK
[5] Cyber Security and Resilience (Network and Information Systems) Bill - Parliamentary Bills - UK Parliament

Pulling No Punches: High Court Orders ISPs to Block Websites Selling Fake GLP-1 Jabs

In what is understood to be the first website blocking injunction aimed at counterfeit and unlicensed prescription-only medicines, the High Court ordered major UK internet service providers ("**ISPs**") to block access to websites selling fake versions of Novo Nordisk's semaglutide products, including Ozempic and Wegovy. The decision extends a powerful enforcement tool, previously reserved for copyright piracy and counterfeit luxury goods, squarely into the field of public health. A follow-up ruling has since granted a dynamic blocking order, allowing new infringing websites to be blocked without returning to court.

What happened?

Novo Nordisk manufactures semaglutide-based medicines marketed under the brands Ozempic, Wegovy and Rybelsus, used to treat type 2 diabetes and obesity. The global market for GLP-1 receptor agonists hit US$79 billion in 2025, making these products a lucrative target for counterfeiters.

Four target websites – Viogen Pharma, Pharma-Labs, Leo Labs and The Steroid Supplier (together, the "**Target Websites**") – were selling counterfeit and unlicensed versions of Novo Nordisk's products to UK consumers. The products ranged from outright counterfeits bearing Novo Nordisk branding, to unlicensed third-party versions of semaglutide, to products containing entirely different substances such as insulin. Many of the Target Websites' activities amounted to criminal offences under the Human Medicines Regulations 2012 (the "**Regulations**").

The evidence of public health harm was stark: falsified products containing impurities; US data linking over 300 serious health incidents, 100 hospitalisations, and 10 deaths to fake semaglutide products; and UK media reporting seizures of fake pens containing rat poison, cement, mercury, and arsenic. The Medicines and Healthcare products Regulatory Agency ("**MHRA**") had tried and failed to have the websites taken down, and ultimately asked Novo Nordisk for help.

Why does this matter?

The decision in *Novo Nordisk A/S & Anor v British Telecommunications & Ors* [2026] EWHC 1094 (Ch) is significant because it confirms that website blocking injunctions – a remedy well established in cases of online copyright piracy and trade mark infringement – can be obtained on the basis of criminal wrongdoing under medicines regulations alone, without any need to prove intellectual property ("**IP**") infringement.

Mr Justice Mellor held that the court's jurisdiction to grant such orders is not limited to IP infringement. Drawing on the Supreme Court's reasoning in *Cartier International AG v British Sky Broadcasting Ltd* [2018] UKSC 28, he confirmed that the jurisdiction derives from ordinary principles of equity, under which the court may order a party innocently mixed up in wrongdoing to take steps to prevent it. There is no principled distinction between civil and criminal wrongs for these purposes.

What did the court decide?

The court addressed two key issues. First, whether it had jurisdiction to grant a website blocking injunction grounded in criminal offences under the Regulations (rather than IP infringement). Second, whether Novo Nordisk had standing to enforce breaches of those Regulations.

On jurisdiction, the judge found that the target websites were committing multiple criminal offences, including selling unauthorised medicinal products, supplying prescription-only medicines without valid prescriptions, and advertising medicines without marketing authorisation. Criminal wrongdoing was sufficient to engage the court's equitable jurisdiction.

On standing, Mr Justice Mellor concluded that Novo Nordisk had standing to bring the application, noting in particular the MHRA's support and encouragement after its own enforcement efforts had failed. He declined to lay down fixed criteria for standing in future cases.

On proportionality, the order was justified because website blocking can reduce UK visitor access by up to 98%; there was negligible risk of blocking legitimate content; standard safeguards were included (for example, sunset clauses and notification provisions); and the ISPs did not oppose the application. The public health benefit and IP protection clearly outweighed any possible interest of the target website operators.

Dynamic blocking: what comes next?

The original blocking order proved effective, with traffic from UK consumers to all but one of the four initial target websites massively declining. However, attempts to circumvent the block via mirror domain names quickly followed, and Novo Nordisk identified over 130 further websites promoting counterfeit and unlicensed semaglutide and cagrilintide products to UK consumers.

In *Novo Nordisk A/S & Anor v British Telecommunications Plc & Ors* [2026] EWHC 1535 (Ch), Novo Nordisk applied to vary and extend the website blocking injunction to add further target websites to the scope of the order, as well as a "dynamic blocking" mechanism concerning potential further websites. Mr Justice Adam Johnson granted the order which allowed Novo Nordisk to self-certify against designated criteria to add further infringing websites to the block without returning to court. Once the criteria (set out in a confidential schedule to the order) are met, Novo Nordisk would notify the ISPs, and the ISPs would be required to implement the block.

The judge found that the order sought was appropriate given: (1) the MHRA's own enforcement had met limited success; (2) Novo Nordisk had the resources and expertise for the relevant and ongoing monitoring; and (3) the MHRA actively supported the structure, confirming "significant alignment" with its own Criminal Enforcement Unit criteria. The order includes standard safeguards including a sunset clause, notification to target website operators where practicable, and liberty to apply to vary or revoke.

While dynamic blocking mechanisms have precedent in broadcasting and football piracy cases, their extension to pharmaceutical counterfeiting marks a significant development in the sector.

Practical takeaways for the life sciences sector

These decisions open up a powerful new enforcement channel for pharmaceutical companies facing online counterfeiting threats. Practical takeaways include:

— **Monitor online threats:** Companies should invest in systematic online monitoring to identify websites selling fake or unlicensed versions of their products. Such monitoring is also an effective tool in gathering evidence against would-be wrongdoers.

— **Build a comprehensive evidence base:** The court placed considerable weight on the detailed evidence of wrongdoing, public health harm, and failed enforcement attempts. A thorough evidential record will be essential for any future applicant.

— **Engage with regulators early:** The MHRA's active support was clearly influential in this case, both in demonstrating the seriousness of the problem and in bolstering Novo Nordisk's standing. Companies should engage with the MHRA or other relevant regulators at an early stage and document their attempts to have infringing websites removed.

— **Consider the full range of wrongdoing:** Applicants need not rely solely on trade mark infringement, passing off or other IP-related ground. Where target websites are committing regulatory offences, these should be pleaded as additional grounds for relief. As this case proves, they may well be sufficient on their own to obtain a website blocking injunction.

— **Think ahead to dynamic blocking:** Where the threat landscape is fast-moving, consider whether a dynamic blocking mechanism, incorporating appropriate safeguards and regulatory support, could provide more effective ongoing protection than a static order.

For further information please contact the authors or your usual CMS contact. CMS has obtained a number of blocking orders for clients to help tackle anti-piracy related matters.

Poland Allows QR Codes in HCP Advertising: A Small Regulatory Change with Significant Practical Impact

For years, one of the most common frustrations for pharmaceutical companies preparing promotional materials for healthcare professionals ("**HCPs**") in Poland has been the requirement to include extensive mandatory information directly within the advertising material itself. In practice, this often means that a substantial part of a brochure, advertisement or digital material is occupied by legally required information rather than the key promotional message.

A recent amendment to the Polish regulation governing medicinal product advertising may finally offer a practical solution to this long-standing challenge.

The previous position

Until now, promotional materials for medicinal products directed at HCPs in Poland had to include the so-called mandatory information (often referred to as abbreviated prescribing information) directly within the advertising material itself.

This mandatory information can be extensive, as it typically includes key information on the medicinal product, such as its indications, dosage, contraindications and adverse reactions. Particularly for products with lengthy safety profiles, it could run to several pages, significantly limiting the space available for promotional content itself.

Even as promotional activities increasingly shifted towards digital channels, the prevailing approach of the Polish regulatory authorities remained that the promotional content and mandatory information should form a single, integrated communication. As a result, companies could not simply replace mandatory information with a hyperlink or QR code leading to a separate website, as the required information was expected to be provided together with the advertising message itself.

What has changed?

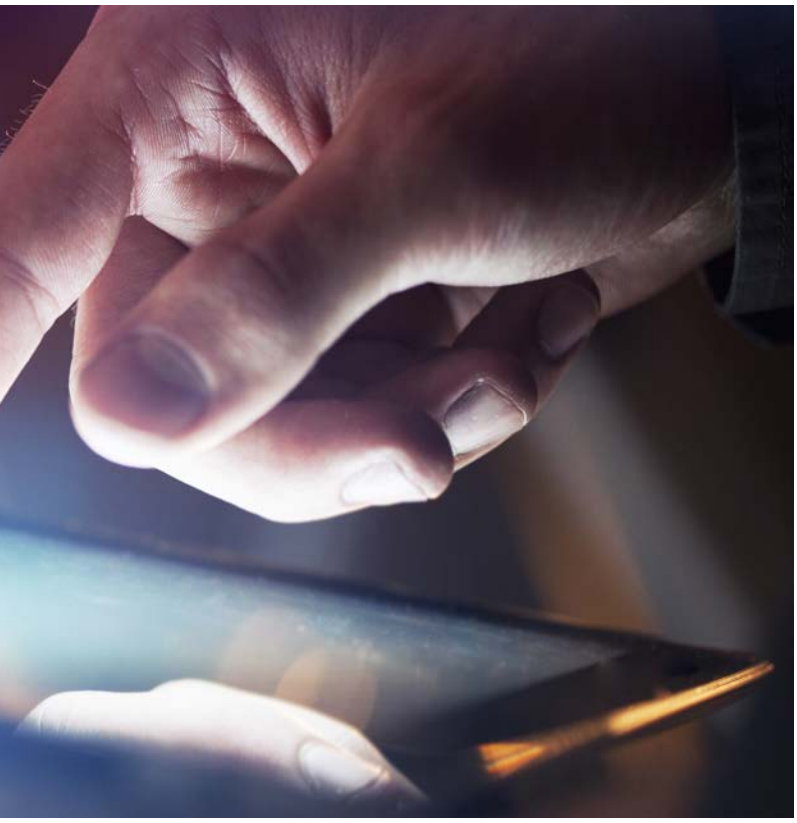
A recent amendment to the Polish regulation on medicinal product advertising, published on 7 July 2026, introduces a practical simplification for advertisements directed at HCPs. The new rules apply to both human and veterinary medicinal products.

Under the new rules, the mandatory information accompanying promotional materials may now be provided electronically, including by means of a QR code or a hyperlink directing the recipient to a website or electronic platform containing the required information.

More fundamentally, the amendment appears to move away from the long-standing assumption that advertising content and mandatory information should form a single integrated communication. This may provide greater flexibility when designing both printed and digital promotional materials.

Why does this matter?

Although the amendment is relatively narrow in scope, it may have a noticeable impact on the way pharmaceutical companies design and use promotional materials in practice. The requirement to include extensive mandatory information directly within promotional materials has long presented a practical challenge.



The amendment is particularly relevant for digital formats, including banners, email campaigns, conference presentations and other promotional content where the inclusion of extensive mandatory information has often been technically challenging or detrimental to user experience.

The new rules should allow companies to:

— improve the readability of promotional materials;

— dedicate more space to substantive promotional content;

— simplify graphic design and layout;

— reduce the need for repeated updates of printed materials when mandatory information changes; and

— better align promotional activities with modern digital communication channels.

For marketing, medical and regulatory affairs teams, the amendment is likely to facilitate the preparation and approval of promotional materials while maintaining access to the information required by law.

What has not changed?

Importantly, the amendment does not alter the scope of the information that must be made available to HCPs. The change concerns only the manner in which that information may be provided. Companies therefore remain responsible for ensuring that the mandatory information is complete, accurate, up to date and easily accessible to the recipient.

The rules governing advertisements addressed to the general public remain unchanged. In particular, there is still no possibility to replace mandatory information required in public advertising with a QR code or a link to digital content.

Practical considerations

Although the new rules are welcome, companies operating in Poland should carefully consider how they intend to implement them in practice.

Several questions will likely arise, including:

— how to ensure that the linked website remains continuously available;

— how to manage updates to mandatory information made available online;

— how to document the content accessible through the QR code at a particular point in time for compliance and inspection purposes; and

— how to adapt internal review and approval procedures to the new model.

Businesses may therefore wish to review their existing promotional material templates and internal SOPs to ensure that they reflect the new possibilities introduced by the amendment.

What is next?

The new rules entered into force on 22 July 2026.

For the pharmaceutical and veterinary sectors, the amendment represents one of the most practical advertising-related changes introduced in Poland in recent years. Similar approaches have already been adopted in a number of European jurisdictions, where QR codes and digital access to prescribing information are commonly used in promotional materials.

For companies operating in Poland, the possibility of replacing pages of mandatory information with a simple QR code may significantly improve the design, usability and efficiency of HCP-facing promotional materials. Overall, the amendment is a welcome and pragmatic development that brings the Polish regulatory framework closer to the realities of modern healthcare communication.

Key Life Sciences and Healthcare Developments in 2026: CEE and Adria Region

The life sciences and healthcare sector in Central and Eastern Europe and the Adria region is facing a year of significant regulatory change. In 2026, businesses will need to navigate a broad set of new and developing requirements — from cybersecurity and AI to product liability, market access and anti-corruption compliance.

In this article, we take a high-level look at the key developments shaping the regulatory landscape across thirteen jurisdictions: Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Hungary, North Macedonia, Poland, Romania, Serbia, Slovakia, Slovenia and Ukraine.

There are four areas that will be particularly important for businesses operating in the region:

NIS2, data privacy, AI

Across the region, countries are transposing the EU NIS2 Directive into national law, significantly broadening cybersecurity obligations for healthcare providers, pharmaceutical manufacturers, medical device companies, CROs, and digital health providers — many of which were previously outside scope. At the same time, the EU AI Act is imposing risk-based requirements on AI systems used in clinical, diagnostic, and medical device contexts, while the European Health Data Space and the EU Data Act are reshaping how health data is accessed, shared and protected.

Market access and reimbursement

The briefing tracks important shifts in how medicines and medical devices reach patients and secure public funding. Poland is progressing with a major amendment to its reimbursement law designed to simplify procedures and shorten timelines. Ukraine has introduced regional budget pooling for managed entry agreements and is expanding its outpatient reimbursement programme, including for innovative therapies with partial public funding for the first time. In Bulgaria, the Supreme Administrative Court has struck down successive NHIF reimbursement mechanisms, and the currently applicable mechanism is again under appeal. Croatia has introduced new supply-monitoring obligations for marketing authorisation holders, distributors, and wholesalers.

Anti-corruption and compliance

Hungary has strengthened its corporate criminal liability framework, extending liability to foreign entities, legal successors, and negligent conduct by executives — with particular attention to corruption offences in the pharmaceutical sector. Poland may see a reorganisation of its anti-corruption enforcement architecture, while at the EU level, a new Anti-Corruption Directive is expected to be formally adopted in 2026. In Ukraine, new binding standards for pharmaceutical promotional practices have been adopted, alongside more active enforcement.

Product liability

The new EU Product Liability Directive (EU) 2024/2853 ("**EU PLD**") must be transposed by 9 December 2026, expanding the definition of "product" to cover software, digital files, SaMD, and AI-enabled technologies, and introducing new factors for assessing defectiveness — including cybersecurity requirements and the capacity of AI systems for continuous learning. Hungary is the only Member State who has fully implemented the EU PLD, while others are in the process of preparing draft laws or have begun the first phase of implementation.

Contacts

We hope you have enjoyed reading this summer briefing, if you would like to discuss any of the subjects in this publication with us, please do reach out to our Life Sciences & Healthcare Sector Co-Heads or the authors of the articles below.

David Bridge
Partner, Co-Head Life Sciences & Healthcare sector
T +44 20 7367 3021
E david.bridge@cms-cmno.com

Candice Blackwood
Partner, Co-Head Life Sciences & Healthcare sector
T +44 20 7524 6726
E candice.blackwood@cms-cmno.com

Cyber Security in Healthcare and Life Sciences: A Leadership Priority

Amit Tyagi
Partner
T +44 20 7367 3578
E amit.tyagi@cms-cmno.com

Anna Walsh
Partner
T +44 20 7067 3420
E anna.walsh@cms-cmno.com

Heather Flaherty
Trainee Solicitor
T +44 161 393 4799
E heather.flaherty@cms-cmno.com

Pulling No punches: High Court Orders ISPs to Block Websites Selling Fake GLP-1 Jabs

David Bridge
Partner, Solicitor Advocate, Co-Head of Life Sciences & Healthcare
T +44 20 7367 3021
E david.bridge@cms-cmno.com

Tom Scourfield
Partner
T +44 20 7367 2707
E tom.scourfield@cms-cmno.com

Daniel Boden
Trainee Solicitor
T +44 20 7367 2215
E daniel.boden@cms-cmno.com

Poland Allows QR Codes in HCP Advertising: A Small Regulatory Change with Significant Practical Impact

Agnieszka Starzynska
Partner
T +48 22 520 84 58
E agnieszka.starzynska@cms-cmno.com

Natalia Matuszewska
Associate
T +48 22 520 84 17
E natalia.matuszewska@cms-cmno.com

Key Life Sciences and Healthcare Developments in 2026: CEE and Adria Region

Borys Danevych
Partner
T +380 44 391 7706
E borys.danevych@cms-cmno.com

Gabriela Staber
Partner
T +43 1 40443 4800
E gabriela.staber@cms-rrh.com

CMS Legal Updates subscription service

Sign up now for the free online email alert service delivering commentary, analyses and insights from CMS experts on the legal issues affecting your business, directly to your inbox.
cms.law/subscription

CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

2607-0210049-2