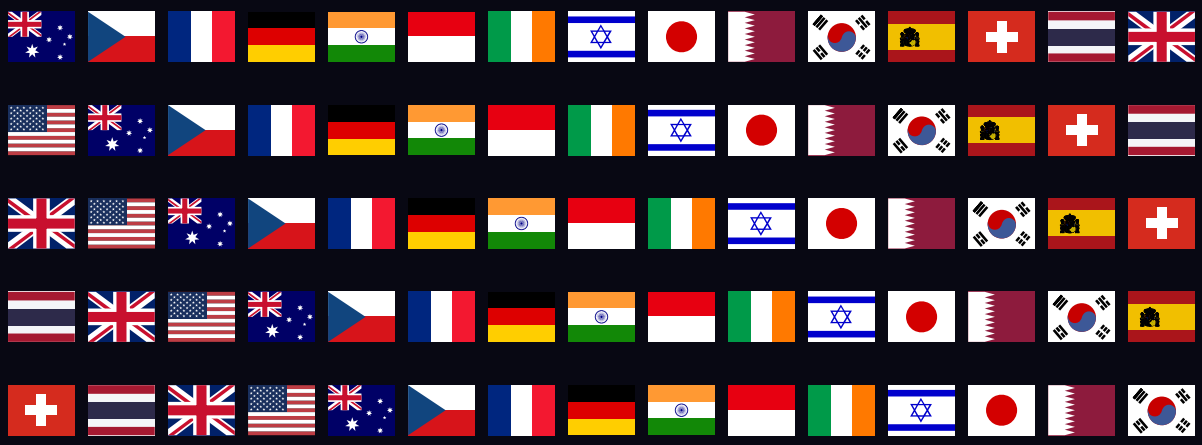
# DIGITAL HEALTH

## United Kingdom



LEXOLOGY
Getting The Deal Through

Consulting editor
*Latham & Watkins LLP*

# Digital Health

Consulting editors

**Eveline Van Keymeulen, Oliver Mobasser, Samantha Peacock, Sara Patel, Brett Shandler**

*Latham & Watkins LLP*

Quick reference guide enabling side-by-side comparison of local insights, including market overview; legal and regulatory framework; data protection and management; intellectual property rights, licensing and enforcement; advertising, marketing and e-commerce; payment and reimbursement; and recent trends.

Generated 30 January 2023

# Table of contents

## UPDATES AND TRENDS

### Recent developments

# Contributors

## United Kingdom


**Eveline Van Keymeulen**
eveline.vankeymeulen@lw.com
*Latham & Watkins LLP*

**Oliver Mobasser**
oliver.mobasser@lw.com
*Latham & Watkins LLP*

**Samantha Peacock**
samantha.peacock@lw.com
*Latham & Watkins LLP*

**Sara Patel**
sara.patel@lw.com
*Latham & Watkins LLP*

**Brett Shandler**
brett.shandler@lw.com
*Latham & Watkins LLP*

## MARKET OVERVIEW AND TRANSACTIONAL ISSUES

### Key market players and innovations

Who are the key players active in your local digital health market and what are the most prominent areas of innovation?

The United Kingdom has an active digital health market comprising both the private and public sectors, as well as investors. While the National Health Service (NHS) remains the dominant buyer in the UK's £5 billion healthcare IT and digital market, private sector spending has increased rapidly over recent years. Valuations and investment in the sector have been driven by venture capital funds and other investors who have identified opportunities in UK digital health startups against a backdrop of the global trend towards the digitisation of healthcare.

The United Kingdom has the highest number of digital health startups in Europe and has attracted the most investment in the region over recent years according to data compiled by Speedinvest . These companies, and their investors, seek to capitalise on increased domestic political support for the digital transformation of health and social care and to compete with international providers to export their products and services to a global market.

The digital health market in the United Kingdom focuses predominantly on:

- telehealth;
- mobile health (mHealth);
- analytics, diagnostics and big data;
- digitised health systems; and
- R&D and genomics.

Each of these sectors has seen vast growth since March 2020 due to the covid-19 pandemic.

Examples of the key participants in the UK digital health market include:

- Babylon;
- BenevolentAI;
- Cera;
- CMR Surgical;
- Congenica;
- Doctorlink;
- Hinge Health;
- Huma;
- Lumeon;
- LumiraDx;
- Medopad;
- Push Doctor;
- Skin Analytics;
- Vernalis; and
- Vira Health.

In addition, it is becoming increasingly common for venture capital funds to adopt sector focuses, with several key venture capital funds having a specific digital health focus, with significant activity in the United Kingdom, including:

- Amadeus Capital;
- Crista Galli Ventures;

- Octopus Ventures;
- Oxford Science Enterprises; and
- Novo Holdings.

Academic institutions, such as the University of Oxford, the University of Cambridge, the University of Edinburgh and Imperial College London, are also very active in the digital health research space. Such institutions frequently receive government sponsorship and grants.

*Law stated - 26 November 2022*

## Investment climate

How would you describe the investment climate for digital health technologies in your jurisdiction, including any noteworthy challenges?

The covid -19 pandemic further heightened the positive and dynamic investment climate for digital health technologies in the United Kingdom. In particular, the pandemic highlighted the need for resilience in healthcare systems, including through digital health solutions. As a result, the pandemic significantly accelerated the uptake of digital health solutions in the United Kingdom and related investment opportunities. Although initial public offering (IPO) and mergers and acquisitions (M&A) activity has reduced from its 2021 peak, according to the Healthcare Investments and Exits Mid-Year Report 2022 conducted by Silicon Valley Bank, investment in digital health technologies remains historically high. Their data indicates that early-stage fundraising looked to be particularly resilient, with first-half 2022 investment keeping pace with the previous year. The United Kingdom is an established player in digital health, accounting for approximately 35 per cent of the European market in 2020 and has, over recent years, accounted for a similar proportion of deals in Europe by volume and value.

The UK's sophistication in health tech research and development is a key component of this and centres around academic institutions in key cities such as London, Oxford and Cambridge. Research by London & Partners showed that in 2021, these three cities accounted for more than 65 per cent of the UK healthcare technology market and over 25 per cent of the European market. According to data from Tech Nation's Data Commons , health tech is now the second biggest component of the UK's tech sector, after fintech.

As a result of the covid-19 pandemic, virtual health has become a new frontier in care delivery. At its height, the pandemic challenged structural barriers that had previously slowed investment in digital health innovations. The pandemic, and the NHS's response to it, highlighted a number of areas where digital health solutions could improve service provision. These include artificial intelligence (AI) applications that have been shown to help to meet the challenge of scaling up labour requirements to meet new demands on resources. Further, the introduction of the covid-19 vaccination status service on the NHS app prompted millions of new users to join. At the end of 2021, the NHS app had over 22 million users, which made it the UK's most popular app. Uptake has further increased in 2022 with now in excess of 30 million users. The NHS has noted that this increase in app downloads has potentially life-saving benefits. In the 12 months preceding May 2022, NHS Digital figures record that the NHS app was used to order over 16 million repeat prescriptions, book 1.3 million general practitioner (GP) appointments, register 377,000 organ donation decisions and view users' GP records more than 90 million times.

The covid-19 pandemic also increased public awareness and interest in health technology. An Organisation for the Review of Health and Care Applications (ORCHA) study published in the British Medical Journal found that online searches for digital health products in the United Kingdom increased 343 per cent during the first pandemic lockdown. Patients have correspondingly adopted telehealth services at pace, motivated by convenience and accessibility.

In 2022, the government released a policy paper titled ' Data saves lives: reshaping health and social care with data ', which acknowledges a number of lessons learned by the NHS throughout the pandemic and sets out plans to apply

data-driven solutions to long-term issues facing the NHS. In ' A plan for digital health and social care ', published by the government in June 2022, the government committed £2 billion for the digitisation of the NHS and at least £150 million to support digital transformation in social care.

Against this backdrop, health agencies and tech companies are striking partnerships at increasing speed. For example, the NHS is reportedly working with companies such as Amazon, Microsoft and Palantir to create data models to optimise the allocation of hospital beds and staff. The NHS is also encouraging development at a more local level with its Digital Health Partnership Awards programme that provides funding with the aim of accelerating the adoption of digital health technologies.

Although global deal-making across industries has slowed throughout 2022 in response to macroeconomic factors and changes to investor mindsights from a record-breaking 2021, the strong potential for growth in the digital health sector remains an attractive prospect for investors. This is reinforced by the UK's strong position within the European market and domestic political focus on the adoption and application of technology in healthcare.

*Law stated - 26 November 2022*

## Recent deals

### What are the most notable recent deals in the digital health sector in your jurisdiction?

The most notable recent deals in the United Kingdom include:

- in August 2022, Cera, a London-based digital home healthcare company, raised US$320 million to expand its patient base to 100,000 per day, up from its current total of 15,000. The company also plans to expand its patient base into the United States and other countries in Europe. The round included support from 8090 Partners, Guinness Ventures, Jane Street, Kairos HQ, Oltre Impact, Schroders, Squarepoint Capital, Robin Klein and Vanderbilt University endowment;
- in June 2022, a group of investors led by venture capital firm Advent Life Sciences LLP acquired an undisclosed stake in Proximie Ltd, the provider of a health technology platform, through a US$80 million series C funding round;
- in May 2022, Physitrack plc, the London-headquartered provider of virtual care technology for rehabilitation acquired Champion Health Ltd in a deal in excess of £10 million;
- in April 2022, a group of investors led by GV Management Co LLC, Northpond Ventures LLC and Sanofi Ventures acquired an undisclosed stake in OMass Therapeutics Ltd, a biotechnology company based out of Oxford, for US $100 million;
- in April 2022, Canadian Dialogue Health Technologies acquired Tictrac, the London-based provider of a digital health platform, for £35 million, aiming to introduce wellness offerings to its integrated health platform;
- in March 2022, AstraZeneca acquired an undisclosed stake in Huma Therapeutics, a London-founded global healthcare company focused on the development of a health-management app for mobile devices;
- in March 2022, a consortium of investors led by Octopus Ventures Ltd acquired an undisclosed stake in Vira Health, a UK software company engaged in providing digital therapeutics to women;
- in January 2022, UK-based Huma Therapeutics acquired iPLATO Healthcare Ltd, the US-based developer of myGP – a patient engagement platform that simplifies access to healthcare, covering a network of 26.6 million patients across nearly 3,000 NHS primary care organisations and one of the most downloaded medical apps in the United Kingdom;
- in January 2022, Lyra Health Inc, a US-based software company engaged with building a data-driven platform to identify people at risk of behavioural and mental health conditions, acquired ICAS World, a UK-based employee support services provider;
- in January 2022, Square Health, a private medical services company providing digital and medical services for

insurance companies, acquired Push Doctor, a provider of online doctor consultation services based in Manchester; and

- in November 2021, UK private equity firm LDC acquired a minority stake in IEG4 Ltd, a Cheshire-based provider of cloud-based digital solutions for local authority and health markets.

*Law stated - 26 November 2022*

## Due diligence

### What due diligence issues should investors address before acquiring a stake in digital health ventures?

Potential investors in digital health should, in addition to the usual considerations that apply to a venture-stage investment, do due diligence on the following:

- intellectual property rights: a significant proportion of the value in digital health businesses can be attributed to the intellectual property rights owned or licensed by the company. Accordingly, it is critical to understand whether any such intellectual property rights have been infringed and to assess the ownership, validity and strength of any material registered intellectual property rights, such as patents and trademarks. If employees and consultants have developed material intellectual property rights, diligence should be undertaken to ensure that the ownership of those intellectual property rights has vested in, or been assigned to, the company. If critical intellectual property rights have been in-licensed from a third party, it is also important to ascertain that the terms of that licence are sufficiently flexible to permit the activities planned by the company in its business plan;
- data privacy and cyber security: it is highly likely that the ability to use, analyse and process data will be a key part of any digital health company's business plan. Given the sensitivity of health data, due diligence should focus on ensuring that the company understands the data protection regimes to which it is subject and processes and protects data in a manner that complies with applicable and upcoming data protection and cyber security regimes while also facilitating future growth. The consequences of cyber incidents, data breaches and non-compliance can be business-threatening, given the scale of potential enforcement activities and reputational harm;
- commercial agreements: it is important to confirm the existence and terms of formal written agreements with key customers, distributors, manufacturers and suppliers. Such a review can help ensure confidence in future revenue, especially by clarifying whether any such agreements would be impacted by the investment (eg, change-of-control triggers);
- regulatory landscape: it is important to verify that the business holds all necessary regulatory authorisations and licences relevant to the products and services offered. Further, the regulatory landscape is rapidly evolving, including in relation to digital health and medical devices. It is important to ensure the company understands the regulatory landscape to which it is subject, both now and in the future, being mindful of the different regimes that apply to the European Union, the United Kingdom and the United States, and also where the service offering is business-to-consumer as opposed to business-to-business. The extent to which services are offered online is also becoming the subject of increased regulation, particularly in the European Union; and
- leadership team: many digital health ventures are founder-led businesses, which heavily rely on their leadership teams. Accordingly, it is important to review the employment terms of key leadership; in particular, in relation to remuneration and bonus arrangements, notice periods, restrictive covenants, assignment of intellectual property and confidentiality to ensure key leadership is appropriately incentivised for the long-term and key provisions are adequate and enforceable.

*Law stated - 26 November 2022*

### Financing and government support

What financing structures are commonly used by digital health ventures in your jurisdiction? Are there any notable government financing or other support initiatives to promote development of the digital health space?

Venture capital funding in the digital health sector has increased significantly in recent years, with the majority of investment appearing to come from private investment firms. The digital health space saw a number of significant IPOs in 2020 and 2021, although public financing through IPOs has decreased in 2022 in line with many other sectors. Digital health companies seeking private investment in the United Kingdom will likely undergo a number of funding rounds from seed and startup capital through to targeted private investment from venture capital firms as they scale up if they have not done so already. With IPO and M&A activity at reduced levels, mature digital health companies may also continue to seek additional fundraising (including through convertible loan notes and similar instruments) in anticipation of a listing or sale once market conditions improve. Investments may be structured through different classes of shares with different voting and economic rights or convertible instruments, or both, potentially alongside additional bank debt.

The government has recently announced a number of initiatives in the digital health sector, including:

- in October 2022, the National Institute for Health and Care Research was allocated over £800 million in additional funding to boost innovation, including the adoption of medical technology;
- in June 2022, in the policy paper 'A plan for digital health and social care', the government committed £2 billion for the digitisation of the NHS and at least £150 million to support digital transformation in social care;
- in September 2020, the government unveiled a £32 million fund for various health technology research projects (including certain AI and robotics-based initiatives);
- in April 2020, the government announced the creation of the Future Fund, which invests up to £5 million into smaller private UK companies. A number of digital and other healthcare companies participated in this scheme. While this closed to new applications in January 2021, due to its success the government announced in April 2021 a successor scheme, Future Fund: Breakthrough, a £375 million UK-wide scheme to encourage private investors to co-invest with the government in high-growth and innovative UK companies. The scheme is focused on UK-based R&D-intensive companies with significant UK operations. The minimum total investment round size is £30 million and the company must have raised at least £5 million in previous funding rounds;
- since its launch in 2019 with initial funding of £250 million, the NHS AI Lab has awarded 79 innovations with more than £100 million of AI award funding and delivered five proofs-of-concept AI tools to NHS trusts. The platform continues to roll out new programmes and seeks to aid the development of AI technologies that may be applied to health and care services and to build the frameworks under which they operate; and
- the government has also pledged financial support for a variety of other digital health initiatives in conjunction with the NHS and other research bodies.

*Law stated - 26 November 2022*

## LEGAL AND REGULATORY FRAMEWORK

### Legislation

What principal legislation governs the digital health sector in your jurisdiction?

Digital health in the United Kingdom is currently governed by a patchwork of different legal regimes, rather than bespoke legislation. The relevant regime depends on the nature of the product or service, for example:

- digital health products (including software, apps, wearables, artificial intelligence (AI) and algorithms) that are classified as medical devices are regulated under the Medical Devices Regulations 2002 (the MDRs), as amended (implementing EU Council Directive 93/42/EEC on medical devices, EU Council Directive 90/385/EEC on active implantable medical devices and EU Directive 98/79/EC on in vitro diagnostic medical devices). Broadly, a product falls within the remit of the MDRs if:
  - its intended purpose is to fulfil a medical function, including diagnosis, prevention, monitoring or treatment of disease; and
  - it does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means;
- the provision of health or social care (including by remote means) in England is primarily governed by the Health and Social Care Act 2008 and the Health and Care Act 2022. Similar legislation covers Wales, Scotland and Northern Ireland. There is currently no specific legislation governing the provision of telemedicine services. The Electronic Commerce (EC Directive) Regulations 2002 (the eCommerce Regulations) may also apply to the provision of telemedicine services;
- the processing of personal data in relation to digital health offerings is governed by:
  - the Data Protection Act 2018, which has been amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 to make certain changes necessary as a result of Brexit; and
  - United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR), as defined in the Data Protection Act 2018, which effectively mirrors the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) in UK law. Both the EU and the UK data protection regimes have extra-territorial aspects. This means that organisations in the United Kingdom may be subject to the GDPR, as well as UK data protection laws, if they offer goods or services to, or monitor the behaviour of, individuals in the European Economic Area;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 may also apply to digital health companies that market to their users by electronic means, or use cookies or similar technologies that track information about people accessing a website or other electronic service such as a digital health mobile application; and
- general consumer legislation may also apply to digital health products and services, and particularly to apps and digital content. Such legislation includes the Consumer Protection Act 1987, the General Product Safety Regulations 2005, the Consumer Protection from Unfair Trading Regulations 2008, the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 and the Consumer Rights Act 2015.

*Law stated - 26 November 2022*

## Regulatory and enforcement bodies

### Which notable regulatory and enforcement bodies have jurisdiction over the digital health sector?

In the United Kingdom, various regulatory and enforcement bodies have jurisdiction over the digital health sector.

Medical devices are regulated in the UK by the Medicines and Healthcare products Regulatory Agency (MHRA).

The provision of health and social care is regulated by the following agencies, based on the jurisdiction:

- England: the Care Quality Commission (CQC);
- Scotland: Healthcare Improvement Scotland (HIS);
- Wales: Healthcare Inspectorate Wales (HIW); and

- Northern Ireland: the Regulation and Quality Improvement Authority (RQIA).

Specifically, the CQC regulates telehealth providers under the regulated activity of 'transport services, triage and medical advice provided remotely'. Other national regulators have not published specific telemedicine policies for healthcare providers. While these bodies regulate healthcare 'providers', individual practitioners are subject to licensing and enforcement by their professional bodies; in particular, the General Medical Council (GMC), in respect of doctors, and the General Pharmaceutical Council, in respect of pharmacists.

Information rights, including data protection, are regulated across the United Kingdom by the Information Commissioner's Office (ICO).

Consumer legislation is primarily enforced in the United Kingdom by the Competition and Markets Authority.

*Law stated - 26 November 2022*

## Licensing and authorisation

### What licensing and authorisation requirements and procedures apply to the provision of digital health products and services in your jurisdiction?

All medical devices must be registered with the MHRA before being placed on the market in Great Britain. Separate rules apply to Northern Ireland, which falls under the EU regulatory regime.

In general, a medical device must undergo a conformity assessment that results in it being affixed with a UKCA mark before it can be placed on the UK market. For class I devices, this assessment can generally be conducted through a self-assessment procedure. However, for higher-risk devices, in class IIa, IIb or III, the conformity assessment must involve a notified body. Under the current classification rules, many software devices are classified as class I. However, the recent proposals from the MHRA in response to its consultation on the future regulation of medical devices will, if implemented, have the effect of 'up-classifying' many software medical devices from July 2023, meaning that self-assessment will no longer be an option for manufacturers. As a result of the UK's departure from the European Union, the CE mark, which was previously used under the MDRs (and will continue to be used in the European Union under EU MDR Regulation (EU) 2017/745 (the EU Medical Devices Regulations) and Regulation (EU) 2017/746 (the EU In Vitro Diagnostic Medical Devices Regulations), has been replaced by a new UKCA mark. Devices certified under the EU MDR or EU IVDR may be placed on the market under the CE mark until either the certificate expires or for five years after the EU MDR or EU IVDR take effect, whichever is sooner. However, devices certified under the previous directives ( EU Council Directive 93/42/EEC on medical devices, EU Council Directive 90/385/EEC on active implantable medical devices and EU Directive 98/79/EC on in vitro diagnostic medical devices ) may be placed on the market until either the certificate expires or for three years (for general medical devices) and five years (for in vitro diagnostics) after the EU MDR and EU IVDR take effect, whichever is sooner.

Telemedicine service providers are required to register with the CQC in England, HIS in Scotland, HIW in Wales or the RQIA in Northern Ireland. A provider's registration may be subject to certain conditions imposed by the relevant regulator, and registered providers will be subject to inspection and enforcement by the regulator.

Healthcare professionals must be appropriately qualified and registered with their professional governing body to provide the relevant healthcare service. This obligation applies regardless of whether the service is provided remotely or in person. As a result of the UK's departure from the European Union, the 'country-of-origin' principle under the eCommerce Regulations and the rules on cross-border care from Directive 2011/24/EU no longer apply, meaning professionals providing telemedicine services from the United Kingdom to patients in the European Economic Area may also need to be licensed in the country in which the patient is located.

*Law stated - 26 November 2022*

## Soft law and guidance

### Is there any notable 'soft' law or guidance governing digital health?

The MHRA has published detailed guidance on standalone softwar e, including apps. This guidance provides helpful clarity on when the software will be regulated as a medical device. On 17 October 2022, the MHRA also published guidance ' Software and AI as a Medical Device Change Programme – Roadmap ', which consists of 11 work packages detailing the UK's proposals to provide a regulatory framework for software and artificial intelligence medical devices that provides a high degree of protection for patients and the public and also makes sure that the United Kingdom is the home of responsible innovation for medical device software setting out its objectives. The MHRA has stated that the Change Programme will be implemented primarily through guidance that will build on legislation.

The NHS has published ' A guide to good practice for digital and data-driven health technologies ', which aims to help innovators understand what NHS considers when purchasing digital and data-driven technology. This way, principles of good practice can be built into the strategy and product development 'by design'. NHS Digital also publishes standards and guidance, including in relation to 'Clinical Risk Management: its Application in the Manufacture of Health IT Systems'.

The National Institute for Health and Care Excellence has published ' Evidence standards framework (ESF) for digital health technologies ', which describes the standards for digital health technologies to demonstrate their value in the UK healthcare system.

The GMC has published guidance on remote consultations , which enable healthcare professionals to manage patient safety risks and decide when they can safely treat patients remotely. In addition, the GMC, along with a number of other UK healthcare regulators, has published guidance on remote prescribing .

The CQC has published guidance on its regulatory methodology for digital healthcare providers .

The ICO has also published various guidance on special categories of personal data (including health data) and on data subject access requests with respect to health data .

*Law stated - 26 November 2022*

## Liability regimes

### What are the key liability regimes applicable to digital health products and services in your jurisdiction? How do these apply to the cross-border provision of digital health products and services?

Digital health products and services are subject to the general rules on liability in the United Kingdom.

Providers or manufacturers of digital health products or services could face potential liability under the law of contract. Such liability depends on the relationship with the recipient. Providers could also face potential liability under the general law of negligence, including the principles of professional negligence that apply to the doctor-patient relationship.

Strict liability could apply to defective products under the Consumer Protection Act 1987.

Section 168 of the Data Protection Act 2018 provides a right for data subjects to bring claims, including through representative class actions, for compensation for material or non-material damage due to infringement of the UK GDPR.

The retained Rome I Regulation (Regulation (EC) No. 593/2008) and Rome II Regulation (Regulation (EC) No. 864/2007) , as amended, apply to:

- contracts that conclude after the end of the Brexit transition period; and
- events giving rise to damage that occurs after the end of the Brexit transition period.

In such instances, these regulations determine the applicable law in relation to contractual or non-contractual obligations. Generally, this means that contractual disputes will be governed by the law chosen by the parties or, in the absence of choice, as determined in the principles in the Rome I Regulation. Non-contractual disputes will generally be governed by the law of the country in which the damage occurs.

On an EU level, the European Commission has published a proposal for a new directive on the civil liability regime for artificial intelligence . This proposed directive introduces a rebuttable presumption of causality between a defendant's fault and the output of an AI system in cases where the defendant has breached a duty of care, where it is reasonably likely that the defendant's fault has influenced the output of the AI system or where the output of the AI system gave rise to the harm suffered. For high-risk AI systems, the presumption of causality does not apply where the defendant demonstrates that sufficient evidence and expertise are reasonably accessible for the claimant to prove the causal link. The extent to which the United Kingdom will align with this proposed approach is not yet clear, but on 18 July 2022, the government published the policy paper ' Establishing a pro-innovation approach to regulating AI ' on AI regulation, which signals a pro-innovation and flexible approach to AI regulation that envisages no need for new legislation at this stage.

*Law stated - 26 November 2022*

## DATA PROTECTION AND MANAGEMENT

### Definition of 'health data'

What constitutes 'health data'? Is there a definition of 'anonymised' health data?

### Health data

United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR), 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status. The Information Commissioner's Office (ICO) has confirmed that 'data concerning health' includes any data related to a person's past, current or future health status and includes data from medical devices and fitness trackers (eg, the number of steps taken by the user or athletic performance). Data such as appointment details, reminders and invoices may also constitute health data if it reveals, or could in combination with other data reveal, information about a person's health through 'reasonable inference'.

Additionally, the UK GDPR uses the concepts of 'genetic data' and 'biometric data'. 'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question. 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person. Biometric data is an open category and can include a broad set of identifiers such as DNA matching, iris and retina recognition, facial recognition, and fingerprint and voice recognition.

### Anonymous data

The preambles to the UK GDPR describe 'anonymous information' as 'information which does not relate to an identified or identifiable natural person' or personal data that has been 'rendered anonymous in such a manner that the data subject is not or no longer identifiable'. Therefore, genuinely anonymised information does not constitute personal data for the purposes of and is not regulated by the UK's data protection regime.

Companies should bear in mind that identifiability is a spectrum and is evaluated by taking into account the full commercial context of the processing. Fully identifiable data (eg, data including a person's name) sits on one end of the spectrum, whereas fully anonymised data (namely, data from which it would be impossible to identify an individual) sits on the other. Key-coded (or, in the terminology of the UK GDPR, 'pseudonymised') data, as is commonly used in many healthcare and research contexts, sits in between fully identifiable data and fully anonymised data. Pseudonymisation is considered an important security measure but, unlike anonymised data, pseudonymised data is considered personal data for data protection law purposes. The same data set may be anonymised in the hands of one party, but identifiable in the hands of another party. For example, a key-coded result of a patient's test may be anonymous in the hands of a data analytics company that has no access to the 'key', but may be identifiable in the hands of that patient's treating physician who does have access to the 'key'.

On 28 May 2021, the ICO began a consultation on its updated draft guidance on anonymisation, pseudonymisation and privacy-enhancing technologies. The first five draft chapters of this updated guidance, covering topics including ensuring effective anonymisation; pseudonymisation; accountability and governance; and privacy-enhancing technologies, were published throughout 2021 and 2022. The consultation closes on 31 December 2022. In the draft guidance published to date, the ICO emphasises that data protection law does not require anonymisation techniques to be completely risk-free, but rather envisages mitigating the risk of re-identification until it is sufficiently remote that the information is 'effectively anonymised'.

*Law stated - 26 November 2022*

## Data protection law

What legal protection is afforded to health data in your jurisdiction? Is the level of protection greater than that afforded to other personal data?

Data concerning health, genetic data and biometric data are included in a list of 'special categories of personal data' under the UK GDPR. Such special category data is afforded a greater level of protection than other personal data. Such data can only be processed if one of a limited number of conditions is met (in addition to the legal bases that must be met for processing personal data more generally), which are exhaustively set out in law. Those conditions most likely to be applicable to a digital health company may include one or more of the following:

- the data subject has given their explicit consent;
- the processing is necessary for the purposes of preventive or occupational medicine, the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment, or the management of health and social care systems and services;
- the processing is necessary for reasons of public interest in the area of public health; and
- the processing is necessary for scientific research purposes in the public interest.

A number of the conditions listed above trigger the application of further requirements under the Data Protection Act 2018, and in many circumstances, an 'appropriate policy document' will also be required.

The ICO recognises health data as 'particularly sensitive'. This view is likely to play a part in the regulator's analysis of a

company's obligations, such as whether:

- security measures applied to the data are appropriate in light of the potential risk to the rights and freedoms of natural persons; and
- security incidents with respect to personal data are notifiable to the ICO and data subjects.

*Law stated - 26 November 2022*

## Anonymised health data

### Is anonymised health data subject to specific regulations or guidelines?

Anonymised data falls outside of the scope of the UK data protection regime, as it no longer constitutes 'personal data'. However, controllers of anonymised data should keep in mind that the act of anonymising could in itself constitute data processing within the meaning of the UK GDPR and, as such, this act will be subject to compliance requirements under UK data protection laws including transparency and legal basis.

It should be borne in mind that anonymisation is typically considered together with subsequent processing purposes, such as machine learning or other forms of data analytics. If the use of patients' data post-anonymisation is contemplated, patients may be entitled to understand what further uses will be made of their data, whether such data will be commercialised and in what ways. While such post-anonymisation activities are not within the scope of the UK data protection regime (assuming the data remains anonymised and is not subsequently re-identified), patients or users may legitimately expect to receive at least a high-level information notice explaining what will happen to the data post-anonymisation. Failure to adequately do so may reduce take-up if the organisation in question is seeking the consent of such persons, or may lead to reputational harm if it becomes known that health data was inappropriately or unexpectedly used after being anonymised.

*Law stated - 26 November 2022*

## Enforcement

### How are the data protection laws in your jurisdiction enforced in relation to health data? Have there been any notable regulatory or private enforcement actions in relation to digital healthcare technologies?

The ICO has broad investigative powers and can issue sanctions, including administrative fines up to the higher of £17.5 million or 4 per cent of the company's total worldwide annual turnover under the UK GDPR. To date, ICO enforcement activities have mainly been triggered by data breaches, and there have not been any notable enforcement actions against digital healthcare technologies.

Additionally, any person who has suffered 'material' or 'non-material' (eg, emotional) damage as a result of a data protection violation has the right to compensation.

The ICO's Assurance team carries out audits across a broad range of health organisations. Breaches found during the audit can lead to ICO investigations, which in turn may lead to the ICO mandating remedial actions by the breaching party. In June 2022, the ICO issued a penalty notice to The Tavistock and Portman NHS Foundation Trust for security failures that affected 1,781 patients of the trust's Gender Identity Clinic. Although not specifically related to digital health, the notice is a useful insight into the ICO's approach to the security of data, in particular, to data from which health information could be inferred. The ICO's action against Easylife Limited, in October 2022, suggests that the ICO takes a relatively expansive view of the scope of health data protected as special category data, including within that category health information inferred from consumer transaction data and potentially even that transaction data itself

(although, as above, this decision was not made in the context of digital health).

One notable ICO investigation into digital healthcare technologies concerned TPP's SystmOne, the second most widely used general practitioner (GP) electronic patient record system in England. In 2017, the ICO raised concerns about the software's 'enhanced sharing' function. This function allowed authorised users at hospitals and other care organisations to access, and add to, patient records. Following the ICO investigation, new controls were implemented in 2018 giving GP data controllers more control over how they share patient records for the purposes of patient care.

*Law stated - 26 November 2022*

## Cybersecurity

### What cybersecurity laws and best practices are relevant for digital health offerings?

The UK Network and Information Systems Regulations 2018 (the NIS Regulations) aim to ensure the security of critical IT systems in central sectors of the economy. The NIS Regulations require relevant entities to:

- take appropriate and proportionate technical and organisational measures to manage risks to the security of their network and information systems;
- consider the latest developments and potential risks facing their systems;
- take appropriate and proportionate measures to prevent or minimise the impact of security incidents; and
- notify the relevant supervisory authority without undue delay if any security incident occurs that has a significant impact on service continuity.

Within the healthcare sector, the scope of the NIS Regulations is limited to:

- providers of non-primary NHS healthcare in England;
- local health boards and NHS trusts in Wales;
- health boards and special health boards in Scotland; and
- health and social care trusts in Northern Ireland (paragraph 8, Schedule 2 of the NIS Regulations 2018).

The government's second post-implementation review of the NIS Regulations highlighted a number of areas for proposed improvement, including reassessing the scope of the NIS Regulations, additional obligations to secure supply chains, enhanced incident reporting and increased cross-sector coordination. The proposed development of the NIS Regulations complements the government's consultation on broader legislative reform to improve the UK's cyber resilience, conducted in early 2022.

The government has proposed specific legislation in relation to digital and connected consumer product security, in the Product Security and Telecommunications Infrastructure Bill (PSTI Bill). The PSTI Bill proposes to, among other things, require manufacturers of 'connectable products' (devices that can access the internet or that can connect to multiple other devices) to inform customers about the minimum amount of time for which a product will receive security updates and patches, or disclose that a product does not come with security updates. The current draft of the PSTI Bill includes fines for non-compliance of up to £10 million or 4 per cent of global annual turnover.

There is no legal requirement in the United Kingdom for companies to obtain cybersecurity insurance.

*Law stated - 26 November 2022*

## Best practices and practical tips

What best practices and practical tips would you recommend to effectively manage the ownership, use and sharing of users' raw and anonymised data, as well as the output of digital health solutions?

Companies engaged in the digital health space should bear in mind the concepts of 'privacy by design' and 'privacy by default', which are built into the UK data protection regime.

In practical terms, this means implementing technical and organisational measures that secure the data and ensure it is processed in a manner commensurate to the purposes for its processing. For example, companies should:

- collect as little personal data as is necessary for their purpose. For example, if the user's age suffices, the user's full date of birth should not be collected;
- anonymise and aggregate personal data when possible. For example, if a company is trying to build an analytics model of how many steps users in a particular city take on average, it can aggregate that information and not hold the exact number for each user;
- when possible, only obtain access to pseudonymised data and when accessing data from a third-party source, a digital health company should build organisational and contractual safeguards that ensure that it has no ability to re-identify the pseudonymised data to which it has access;
- make sure that any consents obtained from data subjects are freely given, specific, informed and unambiguous. Where possible, separate consents should be obtained for separate processing purposes. While the UK regime allows some level of generality when obtaining consent for future research, companies should explain to data subjects what the company proposes to do with the data in as much detail as possible at the outset;
- maintain visibility over the personal data they process across the organisation. One of the easiest ways to achieve this is to maintain a fulsome 'record of processing', as is required in accordance with article 30 of the UK GDPR (sometimes also referred to as a data inventory or asset register); and
- implement effective cybersecurity measures to protect the personal data, as well as information security training and awareness campaigns for personnel, to reduce the risk of data breaches caused by human error and to support data compliance more generally. Companies should also maintain robust and effective incident response processes, and should engage in regular cyber incident simulation exercises to stress-test and refine their response.

In 2022, we saw a continuation of the trend of ransomware and other cybersecurity attacks increasingly targeting companies with large amounts of electronic health records or profiles. Defending against and responding to a cybersecurity incident, particularly one with multi-jurisdictional impact, is complex and requires consideration of a number of regulatory areas, including data protection, cybersecurity, law enforcement, industry-specific regulations and sanctions (in relation to ransom payments). The UK National Cyber Security Centre (NCSC) has prepared a guidance note on mitigating such attacks . The NCSC recommends using layers of defence across an organisation in what is known as a 'defence-in-depth' approach, which includes:

- making backup copies of information;
- implementing technical measures that prevent malware from being delivered to devices in the first place;
- implementing technical measures that only permit trusted applications to run on devices; and
- preparing an organisation for an eventual attack by having a response plan in place.

*Law stated - 26 November 2022*

## INTELLECTUAL PROPERTY

### Patentability and inventorship

What are the most noteworthy rules and considerations relating to the patentability and inventorship of digital health-related inventions?

Digital health products vary in nature and may incorporate inventions across a range of technical fields. Digital health products or aspects of digital health products may be eligible for patent protection in the United Kingdom, subject to being novel, displaying an inventive step, and being capable of industrial application (among other requirements). Aspects of a digital health-related product in respect of which a patent may be sought may include hardware elements, as well as processes and methods associated with using the product.

In considering the patent eligibility of inventions underlying digital health products, it is necessary to consider various exclusions and exceptions under UK and EU law that may be engaged, particularly with respect to software and medical exclusions. In this regard, it should also be noted that the respective tests and approaches adopted by the Intellectual Property Office of the United Kingdom (UKIPO) and the European Patent Office (EPO) regarding patent eligibility may differ.

#### Software exclusions

Section 1(2) of the Patents Act 1977 inter alia excludes from patentability programs for computers (namely, software), mathematical methods and business methods as such. Article 52 of the European Patent Convention (EPC) includes similar exclusions.

Notwithstanding this, under UK law, when the task or process performed by the relevant computer program reveals a 'technical contribution' to the known art (as a matter of substance), then the invention is not excluded and may be patentable. A computer program is likely to make such a contribution if, when it runs on a computer, its instructions:

- embody a technical process that exists outside the computer;
- contribute to the solution of a technical problem lying outside the computer;
- solve a technical problem lying within the computer itself; or
- define a new way of operating the computer in a technical sense.

See, in this regard, the four-step test set out in Aerotel Ltd v Telco Holdings Ltd & Macrossan's Application [2007] RPC 7. Similarly, under EPO practice, a computer program must have a 'technical character' to avoid exclusion from patentability. This means that the computer program must produce a 'further technical effect' when run on a computer, being one that goes beyond the 'normal' physical interactions between the program (software) and the computer (hardware) on which it is run.

#### Medical exclusions

In addition, the Patents Act 1977 and EPC exclude from patentability methods of treatment of the human or animal body by surgery or therapy, and methods of diagnosis practised on the human or animal body. However, these exceptions do not apply with respect to substances or compositions for use in any such methods.

It should also be emphasised that the diagnostic method exclusion is in practice construed quite narrowly. Among other points, to fall within the exclusion all steps leading to a diagnosis would generally need to be claimed, and the

method be performed on the human body. As such, digital health inventions that relate to the diagnosis and treatment of a disease may, depending on their nature and how they are characterised and claimed, nevertheless be patentable.

### Artificial intelligence

In September 2022, the UKIPO released guidelines for the examination of patent applications for inventions relating to artificial intelligence (AI). These guidelines essentially cover the circumstances in which AI inventions will be eligible for patent protection, including what will constitute a 'technical contribution' in the context of AI. In addition, they address the sufficiency of the disclosure of an invention necessary to satisfy UK patent law requirements.

In relation to inventions generated by an AI system, the English Court of Appeal in 2021, by a majority, held that a UK patent cannot be granted if an AI system is named as the inventor thereof, as under the Patents Act 1977, an inventor must be a person ( Thaler v The Comptroller-General of Patents, Designs and Trade Marks [2021] EWCA Civ 1374). In August 2022, the UK Supreme Court agreed to grant special leave to the appellant, Dr Stephen Thaler, to appeal this decision, with the appeal likely to be heard in 2023.

In June 2022, the government announced the outcome of its consultation titled 'Artificial Intelligence and Intellectual Property: copyright and patents'. Among other points, the government indicated that no changes to UK patent law are currently planned in relation to AI-devised inventions, on the basis that most consultation respondents felt that AI is not yet advanced enough to invent without human intervention. However, the government noted that it will keep this area of law under review.

### Employee inventions

An invention will belong automatically to an employer if it is invented by its employee in the United Kingdom in the course of their normal employment duties, or duties specifically assigned to the employee that might reasonably be expected to result in an invention or other duties, the nature of which gives rise to a special obligation to further the interests of the employer (section 39(1)(a) and (b) of the Patents Act 1977). The nature of an employee's 'duties' can evolve over time and is not limited to their job description. The definition can extend, for example, to a manager of business development charged with the task of identifying new products or to an employee who is employed to innovate on behalf of the employer ( LIFFE Administration & Management v Pinkava [2007] RPC 30). Otherwise, the employee is the owner of an invention. By contrast, inventions by contractors will not automatically belong to the party engaging such contractor and therefore robust assignment provisions are required in agreements with such contractors. It is often good practice to also obtain confirmatory assignments from employee inventors as they may need to be filed in some jurisdictions as part of the patent application process.

*Law stated - 26 November 2022*

## Patent prosecution

### What is the patent application and registration procedure for digital health technologies in your jurisdiction?

There are no specific rules for patent application and registration for digital health technologies in the United Kingdom.

There are a number of different routes for obtaining a UK patent, including:

- filing a national application directly with the UKIPO;
- filing a European patent application that designates the United Kingdom, such that the patent can be validated in the United Kingdom once granted under the EPO's central examination procedure; and

- by way of an often-called ‘international’ patent application filed with the World Intellectual Property Organisation pursuant to the Patent Cooperation Treaty, which can then enter the regional phase in Europe or the national phase in the United Kingdom.

Each of these routes will involve different procedural requirements and timelines and will have various advantages and disadvantages that will need to be considered in light of the relevant circumstances and portfolio.

*Law stated - 26 November 2022*

## Other IP rights

### Are any other IP rights relevant in the context of digital health offerings? How are these rights secured?

Other intellectual property rights and related rights relevant to digital health offerings include: copyright, know-how, trade secrets, design rights, database rights and trademarks.

### Copyright

Copyright is, in practice, the main source of protection for software under the Copyright, Designs and Patents Act 1988 (CDPA 1988). Data sets may, depending on their nature and the circumstances of their creation, attract copyright protection. In addition, the selection or arrangement of the contents of a database may be protected under copyright as a literary work. Visual elements of a graphical user interface may also attract copyright protection as artistic works. Literary, dramatic, musical or artistic works that are computer-generated can obtain copyright protection under CDPA 1988, the author of which shall be taken to be the person by whom the arrangements necessary for the creation of the work were undertaken (section 9(3) of CDPA 1988). In June 2022, the government indicated that it is not planning any changes to the current scheme granting copyright protection to computer-generated works.

There is no official register for copyright in the United Kingdom, so (to the extent that it is challenged) ownership must be proved by way of documentation. Retaining correspondence, agreements and any other records pertaining to the creation of copyright-protected works is important for this reason.

### Trade secrets and know-how

Companies may seek to protect certain IP underlying digital health technologies such as data, algorithms and processes through trade secret protection. In addition, know-how may play an important role in implementing or giving effect to a digital health-related technology.

While the protection of trade secrets and know-how does not require registration and is potentially indefinite in term, it requires the adoption of robust confidentiality practices and measures to avoid the disclosure of the relevant information or data to third parties or the public.

### Design rights

Registered designs are governed by the Registered Designs Act 1949 , and protect the overall appearance of the product (including lines, contours, colours, materials, texture and shape) that meets certain criteria, but do not protect features that are dictated by technical function. Registered design protection can last for up to 25 years, and does not require proof of copying to establish infringement.

The UK unregistered design right under CDPA 1988 provides protection for the shape and configuration of three-dimensional (3D) articles for up to 15 years from the end of the year in which the design was first recorded, or a corresponding article was first made. It is an automatic form of IP protection that, subject to meeting certain criteria, protects the design from being copied.

Designs protected in the United Kingdom as EU Unregistered Community Designs (UCD) before January 2021 are now protected as UK continuing unregistered designs, and will continue to be protected in the United Kingdom for the remainder of the three-year term attached to them. UCD protection covers the two-dimensional (2D) and 3D appearance of the whole or part of a product. In addition, the United Kingdom has created a UK unregistered design right called the supplementary unregistered design, which mirrors the UCD, and protects the 2D and 3D appearance of the whole or part of a product for a period of three years (see Designs and International Trade Marks (Amendment etc) (EU Exit) Regulations 2019 ).

### Database rights

In addition to protection under the CDPA as a copyrighted work, there exists under UK law an automatic, unregistered sui generis database right under the Copyright and Rights in Databases Regulations 1997 . In essence, if there has been a substantial investment in obtaining, verifying or presenting the contents of the database (among other qualifying requirements), then this right provides protection against the extraction or re-utilisation of all or a substantial part of the contents of the database. The first owner of the right will be the maker of the database. The term of this right is 15 years from the end of the calendar year in which the making of the database was completed, or 15 years from the end of the calendar year in which the database was first made available to the public in circumstances where a database is made available to the public during that period.

### Trademarks

Trademarks are protected under the Trade Marks Act 1994 and should be registered with the initial public offering. They are subject to registration fees and, every 10 years, renewal fees.

Many digital health products will be protected by a combination of the above rights, so it is good practice to consider each of these at the outset. It is often the case that a barrier to third parties entering the market is a web or layering of IP rights and part of companies' IP strategies is often deploying varying forms of protection, which can also help to mitigate the impact of patent expiry.

*Law stated - 26 November 2022*

## Licensing

### What practical considerations are relevant when licensing IP rights in digital health technologies?

The practical considerations for licensing intellectual property rights in digital health technologies are similar to those in any other technical field. Clearly defining the scope of the licence granted, any reserved rights, the duration of the licence and any exclusivity is a key step. When know-how is included in the scope of the licence, non-use and disclosure restrictions must be considered and documented. Clearly defining which party will have the first right to prosecute, maintain and enforce intellectual property rights is also important, as is any backup right of the other party. Non-exclusive licensees of IP rights may have either limited or no standing to bring infringement proceedings independent of the relevant licensor unless the agreement provides for this. For example, as a matter of English law, a patent licensee will only have the standing to bring an infringement claim if it is an exclusive licensee within the relevant licensed field.

Licences of patents, trademarks and exclusive licences of copyright must be in writing and signed by or on behalf of all the parties to be effective.

While not compulsory to do so, licences of certain IP rights such as patents and trademarks can be registered with the UKIPO (but not copyright licences). Registering such licences can provide a number of benefits, including by protecting the licensee in the event of a subsequent transaction that is inconsistent with the licensee's rights, and enabling a licensee that has succeeded in infringement proceedings to claim its litigation costs (subject to the licence being registered within six months of the date of the agreement, in most cases) (see sections 33 and 68 of the Patents Act 1977 and section 25 of the Trade Marks Act 1994).

*Law stated - 26 November 2022*

## Enforcement

What procedures govern the enforcement of IP rights in digital health technologies? Have there been any notable enforcement actions involving digital health technologies in your jurisdiction?

### IP enforcement

IP actions are typically brought before the Chancery Division of the High Court of England and Wales. This includes the specialist Patents Court subdivision of the High Court, and the Intellectual Property Enterprise Court (IPEC), which is a specialist list of the Chancery Division within the Business and Property Courts of England and Wales that is intended to provide a less costly and complex forum for the resolution of appropriate IP disputes.

The High Court is particularly suited to high-value or complex claims, whereas the IPEC is directed to less complex claims with values not exceeding £500,000, and which can be tried in no more than two days. The total maximum costs that a successful party in an IPEC multi-track claim can recover are capped at £60,000 in respect of the final determination of a liability claim, and £30,000 in respect of an inquiry as to damages or account of profits. This procedure not only caps the overall costs that a losing party will have to pay, but also limits costs payable for each stage of the proceedings.

For completeness, it should also be noted that there exists a scheme within the Business and Property Courts of England and Wales for certain claims that can be tried in four days or less under the Shorter Trials Scheme, which is intended to achieve short and earlier trials for business-related litigation at a reasonable and proportionate cost.

Certain claims can also be brought before the UKIPO, including with respect to revocation, invalidation and entitlement. Importantly, however, infringement proceedings cannot be brought before the UKIPO.

In addition, where a party wishes to revoke a European patent that has been validated in the United Kingdom, then it can file an opposition to the grant of a European Patent by the EPO up to nine months after publication of the mention that a European Patent has been granted. If the EPO makes a final determination to revoke that patent, then the corresponding national parts of that patent will also be revoked, with any such revocation taking precedence over any validity decision of a national court (including the High Court of England and Wales). It should also be noted that the same dynamic does not apply with respect to trademarks.

Last, and as noted, the UPC is not currently expected to have jurisdiction over UK designations of European Patents, and the territorial scope of the new Unitary Patent will not extend to the United Kingdom.

### Recent decisions

A recent enforcement decision involving digital health technologies is Tehrani v Hamilton Bonaduz AG & Ors [2021] EWHC 3457 (IPEC), in which the claimant alleged the infringement of a patent claiming a method and apparatus for

automatically controlling a ventilator based on the processing of certain patient oxygen data. Following a trial, the Court concluded that the patent-in-suit was invalid on the grounds of a lack of novelty and inventive step, but that claim 1 thereof would have been infringed by the Defendants had it been valid.

Another such decision is Software Solutions Limited v 365 Health and Wellbeing Limited [2021] EWHC 237 (IPEC), under which the IPEC upheld a claim for infringement of copyright in an Extensible Markup Language (XML) schema that formed part of a mental health application used for providing interactive clinical sessions. An XML schema is a set of data formats that provides the structure and verification rules for XML files. The defendants' application was developed using the XML format to create, validate and run applications. The defendants were found to have infringed the claimants' copyright as the XML schema that was used in the defendants' application was substantially the same as the XML schema used in the claimants' application.

*Law stated - 26 November 2022*

## ADVERTISING, MARKETING AND E-COMMERCE

### Advertising and marketing

What rules and restrictions govern the advertising and marketing of digital health products and services in your jurisdiction?

The legal framework for advertising digital health products and services is regulated under general consumer law, including the Consumer Protection from Unfair Trading Regulations 2008 and the Business Protection from Misleading Marketing Regulations 2008 .

Digital health products (including software, apps, wearables, artificial intelligence and algorithms) that consist of medical devices must also be marketed and promoted in compliance with the Medical Devices Regulations 2002 , which prohibit the marketing of non-CE or non-UKCA marked medical devices. New UK medical device regulations are expected to be brought into force by July 2024 – a year later than originally anticipated. Such regulations are likely to include provisions governing claims about medical devices similar to those in EU Regulations (EU) 2017/745 (the EU Medical Devices Regulations) and EU Regulations (EU) 2017/746 (the EU In Vitro Diagnostic Medical Devices Regulations) prohibiting misleading claims.

Companies can also voluntarily adhere to a number of industry codes of practice governing advertising and marketing, or become members of trade associations including:

- the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing, enforced by the Advertising Standards Authority (ASA), which applies to all advertisers, agencies and media;
- the UK Code of Broadcast Advertising, enforced by the ASA, which applies to all advertisements on radio and television services licensed by the Office of Communications;
- the Association of British Healthcare Industries (ABHI) Code of Practice, including the ABHI Guidelines on Advertisements & Promotions, addressed solely or primarily to healthcare professionals;
- the PAGB Medical Devices Consumer Code, enforced by the Proprietary Association of Great Britain (PAGB);
- following inter-member complaints regarding breaches of the code; and
- the MedTech Europe Code of Ethical Business Practice.

Companies that process personal data for marketing purposes must also comply with the Data Protection Act 2018 , including the UK General Data Protection Regulation. The Privacy and Electronic Communications (EC Directive) Regulations 2003 also apply to digital marketing, and require marketing consents from recipients in certain circumstances.

The General Medical Council's ' Good medical practice ' guide also contains provisions regarding the advertisement of medical services, which will also apply to telemedicine.

*Law stated - 26 November 2022*

### e-Commerce

What rules governing e-commerce are relevant for digital health offerings in your jurisdictions?

UK e-commerce rules governing digital health offerings (both business-to-business and business-to-customer) are found in a number of different statutes and statutory instruments. The following regulations are of particular significance:

- the Electronic Commerce (EC Directive) Regulations 2002 (the E-Commerce Regulations) impose a range of obligations on the providers of 'information society services', including obligations to provide users with certain information about the operator and its services. As a result of the UK's departure from the European Union, the 'country-of-origin' principle no longer applies for the purpose of the E-Commerce Regulations, meaning parties providing online services, such as telemedicine, from the United Kingdom to customers or patients in the European Economic Area may also need to be licensed in the country in which the customer or patient is located;
- the Consumer Rights Act 2015 provides for statutory rights and remedies for consumers in relation to goods and services, including digital content;
- the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 place additional obligations on website operators who deal with consumers, and introduced cancellation rights for consumers;
- the Consumer Protection from Unfair Trading Regulations 2008 regulate online advertising and govern the content of commercial communications or promotions to consumers, including comparative advertising, while the Business Protection from Misleading Marketing Regulations 2008 also regulate online advertising and govern the content of commercial communications or promotions to businesses; and
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 govern the use of cookies, location data, opt-in rules for marketing calls and email marketing, unsolicited marketing, etc.

*Law stated - 26 November 2022*

## PAYMENT AND REIMBURSEMENT

### Coverage

Are digital health products and services covered or reimbursed by the national healthcare system and private insurers?

The National Health Service (NHS) funds the majority of digital health products and services provided to patients in the United Kingdom. A smaller but growing private healthcare sector where patients fund for themselves or through private insurance also exists. There are a number of routes for products to be made available for reimbursement by the NHS, including selling directly to trusts or primary care organisations or procurement through the NHS supply chain or public tenders through a decentralised process. In addition, products, including digital health products, can undergo a technology appraisal from the National Institute for Health and Care Excellence (NICE). The NHS is legally obliged to fund and resource treatments recommended by NICE's technology appraisals.

NHS Digital (a division of the NHS) is the lead national delivery partner for improving the use of data and digital technologies in the health and care system. The NHS has published ' A guide to good practice for digital and data-driven health technologies' , which is designed to help innovators understand what the NHS is looking for when it buys

digital and data-driven technology, so that principles of good practice can be built into the strategy and product development 'by design'. NICE has also published ' Evidence standards framework for digital health technologies ' (ESF), which describes the standards for digital health technologies to demonstrate their value in the UK health and care system.

ESF is complemented by the Digital Technology Assessment Criteria (DTAC), which was launched in the spring of 2021 by the NHSX (a joint unit of NHS England and the Department of Health and Social Care, supporting local NHS and care organisations to digitise their services). The DTAC is a tool providing baseline criteria for digital health technology assessment. It covers five core areas:

- clinical safety;
- data protection;
- technical security;
- interoperability; and
- separate conformity rating of usability and accessibility.

*Law stated - 26 November 2022*

## UPDATES AND TRENDS

### Recent developments

What have been the most significant recent developments affecting the digital health sector in your jurisdiction, including any notable regulatory actions or legislative changes?

On 17 October 2022, the UK Medicines and Healthcare products Regulatory Agency (MHRA) published guidance ' Software and AI as a Medical Device Change Programme – Roadmap ', which provides an outline of the government's intended future regulation of medical devices that are expected to come into force in 2024. Noting that the roadmap is 'patient centred', the MHRA has set out work packages covering the following:

- the MHRA will address what qualifies as Software as a Medical Device (SaMD) and software in a medical device (eg, medical device software versus in vitro diagnostic (IVD) software), as well as clarify the concept of what entity counts as a 'manufacturer' for SaMD;
- software will be reclassified so the classification rules, which will be reformed, are proportionate to the risk. The 'airlock process' will be explored;
- pre-market requirements for software will be clarified, ensuring the requirements fit the software. The MHRA aims to address essential requirements, 'best practice' for development, deployment, retrospective non-interventional studies, joint guidance with the Health Research Authority on the governance of research;
- post-market surveillance will implement stronger safety signals for SaMD and mitigate the risk of patient safety incidents. Real-world evidence will be used to provide assurance that the surveillance functions as intended, there will be clear change management requirements for SaMD and the surveillance system will be strengthened to support the capture of adverse incidents for SaMD;
- the MHRA will consider cyber security requirements, management of unsupported software devices and reporting of vulnerabilities;
- the MHRA intends to create machine learning guidance to supplement the good machine learning guiding principles published last year. Best practice guidance will be produced, and there will be experimental work to detect, measure and correct for bias;
- noting that the regulatory requirements do not currently adequately consider the interpretability of artificial intelligence (AI) as a medical device (AIaMD), best practice guidance on human-centred SaMD will be developed by the MHRA, as well as standards for developing trustworthy AI; and

- the MHRA will create principles on adaptivity and change management, review the concept of 'drift', significant or substantial change and set out proposals for pre-determined change control plans for SaMD and also AIaMD.

The MHRA plans to publish their deliverables in a step-wise manner, with the first sub-set expected by the end of the year.

On 29 June 2022, the government published a policy paper titled ' A plan for digital health and social care '. This policy paper sets out the government's far-reaching plans for the digital transformation of health and social care in England, noting that digital transformation is a top priority for the Department of Health and Social Care and National Health Service (NHS) England. The plan includes:

- systematic digitisation of health and social care records, with the aim to have core digital capabilities and electronic health records in place by March 2025. £2 billion of funding is committed to supporting this digitisation;
- the creation of a life-long health and social care record, which would be accessible to all clinical teams in an integrated care system and would provide a complete view of a person's health and social care record;
- equipping the NHS with digitally-supported diagnoses, including technology to enable image sharing and clinical decision support based on artificial intelligence;
- supporting individuals in living independently healthy lives by increasing the functionality of the NHS app and website and scaling digital self-help, diagnostics and therapies;
- accelerating the adoption of proven technology by supporting further partnerships between technology innovators and frontline teams;
- using regulatory levels, including oversight by the NHS and the Care Quality Commission and enforcing standards, to help guide digital transformation; and
- enable the availability of research and development through a federated network of trusted research environments.

On 26 June 2022, the MHRA published its response to a 10-week consultation on the future regulation of medical devices in the United Kingdom. The aim of the consultation was to explore amendments to the Medical Devices Regulations 2002 with a view to the United Kingdom creating new access pathways to support innovation, creating an innovative framework for regulating software and artificial intelligence as medical devices, reforming IVD regulation and the United Kingdom becoming a sustainability pioneer through the re-use and re-manufacture of medical devices. The new regime was originally scheduled to come into force in July 2023, but has recently been postponed to July 2024. The consultation covered 15 key areas, including the scope of the regulations, classification of medical devices, economic operators, registration and unique device identifiers, conformity assessment, clinical studies, IVDs, software and routes to market. For the most part, the proposed changes in many of these areas align with the new EU regime under Regulation (EU) 2017/745 (the EU Medical Devices Regulations) and Regulation (EU) 2017/746 (the EU In Vitro Diagnostic Medical Devices Regulations), although there are some notable divergences. In particular, the consultation suggests the following departures from the EU regime:

- new rules around software medical devices, including a definition of 'placing on the market', a provision for temporary classification and additional 'essential requirements';
- new requirements for the environmental and public health impact of medical devices, including impact assessments and supply chain waste management responsibilities;
- new routes to market, including a single regulatory audit of quality management systems to meet requirements of multiple jurisdictions, acceptance of approvals from other international medical device regulators and an alternative pathway for innovative medtech;

- more stringent requirements for the re-manufacture of devices and assemblers of systems, procedure packs and kits and manufacturers of custom-made devices;
- new requirements for economic operators to inform the MHRA if they are aware of any issues that will interrupt supply or cause a shortage on the UK market; and
- additional requirements for in-house manufacture, including a requirement for health institutions to register medical devices manufactured or modified in-house.

On 20 May 2022, National Institute for Health and Care Excellence (NICE) published its first guidance on a digital therapeutic , this is the first time NICE has recommended the use of a digital therapeutic as a first-line treatment in preference to drug therapy. This may also indicate a push towards an increasingly centralised approach to digital healthcare funding.

On 15 June 2022, the government also published a policy paper titled ' Data saves lives: reshaping health and social care with data ' setting out the government's plans to transform the use of data to improve health and social care and empower research.

Medical devices are not provided for in the Trade and Cooperation Agreement between the European Union and the United Kingdom, and there is therefore no mutual recognition of medical device certifications post-Brexit between the United Kingdom and the European Union. Consequently, companies will need to comply with two separate regulatory regimes in the United Kingdom and European Union going forward. The United Kingdom and European Union are still required to cooperate and exchange information on product safety and compliance and therefore product issues arising in the European Union will likely be communicated directly by EU regulators to the MHRA and vice versa.

On 27 October 2021, the MHRA announced a collaboration with US and Canadian regulators to develop guiding principles intended to lay the foundation for developing good machine-learning practices for medical devices using artificial intelligence or machine-learning software.

On 17 September 2021, the NHSX published the Digital Clinical Safety Strategy , which builds on the national NHS Patient Safety Strategy and sets out a clear vision and recommendations to make care safer for patients, use digital to improve safety and expand staff access to digital safety.

The government has proposed wide-ranging reforms to UK data protection laws, set out in the UK Data Protection and Digital Information Bill (the UK Reform Bill), which was introduced to Parliament in July 2022. The UK Reform Bill largely maintains Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR) framework in UK law, albeit with a number of modifications reflecting the government's intention to move away from prescriptive requirements to a more risk-based approach, including the introduction of 'privacy management programmes' to replace certain aspects of the GDPR's accountability framework.

*Law stated - 26 November 2022*

# Jurisdictions

| | |
|---|---|
| **Australia** | Gilbert + Tobin |
| **Czech Republic** | dubanska & co |
| **France** | Intuity |
| **Germany** | Ehlers Ehlers & Partner |
| **India** | Chadha & Chadha Intellectual Property Law Firm |
| **Indonesia** | ABNR |
| **Ireland** | Mason Hayes & Curran LLP |
| **Israel** | Naschitz Brandes Amir |
| **Japan** | Anderson Mōri & Tomotsune |
| **Qatar** | Al Marri & El Hage Law Office |
| **South Korea** | Bae, Kim & Lee LLC |
| **Spain** | Baker McKenzie |
| **Switzerland** | Lenz & Staehelin |
| **Thailand** | Baker McKenzie |
| **United Kingdom** | Latham & Watkins LLP |
| **USA** | Seyfarth Shaw LLP |