iclg

# Digital Health 2025

Sixth Edition

Contributing Editor:

**Roger Kuan**

Norton Rose Fulbright

glg Global Legal Group

# Introductory Chapter



# Expert Analysis Chapters



# Q&A Chapters

# United Kingdom



Pieter Erasmus


Emma Drake


Tristan Sherliker


Mario Subramaniam

Bird & Bird


## 1 Digital Health

### 1.1 What is the general definition of "digital health" in your jurisdiction?

There is no specific definition of "digital health" in the United Kingdom (**UK**). The term generally refers to the use of technology (such as apps, programmes, software, etc.) in healthcare – either standalone or combined with other products such as therapeutics, diagnostics or medical devices.

### 1.2 What are the key emerging digital health subsectors in your jurisdiction?

The key emerging digital health technologies in the UK include the following:

- Digitised health systems – in particular, the wholesale digitisation of patient data and prescription delivery in the UK National Health Service (**NHS**).
- mHealth – apps on mobile and connected wearable devices to monitor and improve health and wellbeing.
- Telemedicine – delivery of health data from mHealth apps to the patient's clinician, and the provision of remote support and care to patients, either through healthcare practitioners, allied service providers or AI. There is a trend towards the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis) of patient health data.
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.
- Artificial intelligence (**AI**) and machine learning (**ML**) – these technologies are being used to enhance digital health more broadly and improve operational efficiencies.

### 1.3 What is the digital health market size for your jurisdiction?

Given the breadth of the market and underlying technology, there is not a specific estimate of the digital health market in the UK; however, certain sources suggest that the UK digital health market will reach approximately £15 billion by 2025, although this is likely to be an underestimation.

### 1.4 What are the five largest (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of the more prominent digital health companies operating in the UK include:

- Cerner Corp.
- Teladoc Health.
- Cera.
- CMR Surgical.
- Veradigm (formerly Allscripts).
- Thriva.

### 1.5 What are the five fastest growing (by revenue) digital health companies in your jurisdiction?

Based on certain sources, examples of growing digital health companies operating in the UK include:

- Doccla.
- Huma.
- Snap40.
- Oviva.
- AccuRx.
- Medbelle.

## 2 Regulatory

### 2.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to digital health in your jurisdiction? What is each authority's scope of enforcement?

The Medicines and Healthcare products Regulatory Agency (**MHRA**) regulates medical devices, including digital health technologies, ensuring they meet safety, quality and performance standards. NHS Digital is responsible for the national digital infrastructure and services, ensuring the secure and efficient use of data and technology in the NHS.

The National Institute for Health and Care Excellence (**NICE**) provides guidance and sets standards for health and social care practices, including the evaluation of digital health technologies.

With respect to the use of such digital health technologies in healthcare settings, the healthcare regulatory regimes in the four nations of the UK are regulated by the following regulatory authorities:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.

- Wales – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

The Information Commissioner's Office (**ICO**) regulates the use of personal data in accordance with the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA**).

**2.2 For these authorities, what are the core healthcare regulatory schemes related to digital health in your jurisdiction (e.g., medical devices/AI/generative AI/SaaS/SaMD/combination product regulatory approval, data privacy, data compliance, anti-kickback, national security, etc.)?**

In an increasingly multi-disciplinary area, the core healthcare regulatory schemes related to digital health in the UK are numerous. In addition to software as a medical device (**SaMD**) and AI as a medical device (**AIaMD**) regulation, these include data protection and privacy; the use of personal data in digital health is regulated primarily by the UK GDPR, the DPA and laws on confidentiality that vary between the different parts of the UK (England, Northern Ireland, Scotland and Wales). Further examples include cybersecurity, data compliance and governance.

**2.3 What are the (i) key, and (ii) emerging areas of enforcement when it comes to digital health?**

Key areas of enforcement include:

- **Data protection and privacy**: Ensuring compliance with the UK GDPR and the DPA. This includes safeguarding patient data and ensuring proper data handling practices.
- **Medical device regulation**: The MHRA oversees the safety, quality and performance of digital health technologies (including software) classified as medical devices.
- **Telemedicine and remote care**: Ensuring that telehealth services meet the required standards for safety and quality, including proper registration and compliance with healthcare regulations.
- **Clinical safety and effectiveness**: Ensuring that digital health solutions provide clinically safe and effective care, adhering to standards set by bodies such as NICE.

Emerging areas of enforcement include:

- **AI and ML**: As AI becomes more integrated into healthcare, there is increasing focus on ensuring these technologies are safe, effective and ethically used.
- **Cybersecurity**: With the rise of digital health technologies, protecting against cyber threats and ensuring the security of health data is becoming a critical area of enforcement.
- **Interoperability standards**: Ensuring that digital health systems can effectively communicate and share data across different platforms and healthcare providers (**HCPs**).
- **Digital therapeutics**: As digital therapeutics become more prevalent, there is a growing need to regulate these solutions to ensure they meet clinical standards and provide real therapeutic benefits.

**2.4 What regulations (and corresponding authority(ies)) apply to software as a medical device and its approval for clinical use?**

SaMD is primarily governed by the UK Medical Devices Regulations 2002, as amended (**MDR 2002**). The MHRA has issued guidance specifically dealing with SaMD, which assists with determining whether software is regulated under the MDR 2002. The MHRA has been working towards the reform of the general medical device regulatory framework in Great Britain (being England, Scotland and Wales). Post-market surveillance draft regulations were laid before Parliament on 21 October 2024 and are expected to come into force mid-2025. A consultation was further launched on 14 November 2024 regarding "Pre-market" regulations with the view that new draft regulations will be put before Parliament during 2025. This area of regulation remains in flux, so it should be monitored closely.

From a SaMD perspective, in 2022, the MHRA published a "roadmap" for its *Software and AI as a Medical Device Change Programme* published the previous year. The programme consists of work packages with problem statements, objectives and deliverables, one of which is "The Transparency for machine learning-enabled medical devices: guiding principles" (published in October 2021), which sets out guiding principles for good ML practice that were jointly established by the US Food and Drug Administration, Health Canada, and the MHRA.

**2.5 What regulations (and corresponding authority(ies)) apply to AI/ML-powered digital health devices or software solutions and their approval for clinical use?**

See response to question 2.4 above.

**2.6 How, if at all, are these authorities evolving, or plan to evolve, their static approval scheme to handle the dynamic nature of AI/ML-based digital health solutions?**

See response to question 2.4 above.

The MHRA launched the *AI Airlock* in May 2024 (in collaboration with the Department of Health and Social Care, the NHS AI Lab and Team AB), which is the first regulatory sandbox for AIaMD. The pilot project will run until April 2025. The objective of this project is to identify regulatory challenges associated with AIaMD, to help manufacturers explore how to best collect evidence as support for the approval of their product, and to understand and mitigate any risks that are uncovered through the project. Additionally, and by way of further example, in January 2025 the MHRA launched a pilot real-world evidence Scientific Dialogue Programme, which is designed to help innovators refine their evidence-generation strategies while providing clear guidance on regulatory expectations. This programme aims to facilitate robust decision-making across the entire lifecycle of products, benefitting both regulatory and health technology assessment evaluations relevant to the UK.

**2.7 How, if at all, does clinical validation data play a part in regulatory considerations for AI/ML-based digital health solutions?**

Clinical validation data plays a key role in the regulatory considerations for AI/ML-based digital health solutions. The MHRA requires robust clinical validation data to approve AI/ML-based medical devices. This data helps regulators assess the accuracy, reliability and clinical relevance of the AI/ML algorithms. Clinical validation data also supports ethical

and transparent use of AI/ML in healthcare. It helps in understanding the decision-making process of AI algorithms, and ensuring they are fair and unbiased.

**2.8 How, if at all, are digital health products and solutions being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?**

Regulation in this area remains broadly aligned at the UK national level, subject to the nuance brought about by the Northern Ireland Protocol whereby the regulatory regimes differ between Great Britain and Northern Ireland. Therefore, while the primary regulatory framework is set at the national level, regional health authorities and NHS Trusts may have additional requirements or guidelines for the implementation and use of digital health technologies. These can include specific data-sharing agreements, local clinical governance standards and region-specific pilot programmes.

**2.9 How, if at all, are regulatory enforcement actions being tailored to regulate digital health products and solutions in your jurisdiction?**

As mentioned in the response to question 2.6, examples include the MHRA introducing the *AI Airlock* pilot scheme to test and refine the regulatory framework for AI-powered medical devices. This initiative allows for real-time performance monitoring and continuous validation of AI technologies. In addition, regulatory bodies such as the MHRA and NICE are developing dynamic guidance that can be updated as new evidence and technologies emerge. This ensures that regulations remain relevant and effective.

## 3 Digital Health Technologies

**3.1 What are the core legal and regulatory issues that apply to the following digital health technologies?**

- **Telemedicine/Virtual Care**
  - Determining whether any of the devices used qualify as medical devices.
  - Determining whether such activity requires registration as a regulated activity.
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Contractual issues between the various suppliers of services and devices.
  - If telemedicine is included, compliance with the local pharmacy and prescribing rules and regulations will be necessary.
  - Cybersecurity.
- **Robotics**
  - Liability allocation for poor outcomes – designer, manufacturer, HCP or even power supplier.
  - Compliance with Regulations: e.g. for waste electrical and electronic equipment (**WEEE**).
  - Compliance with MDR 2002.
- **Wearables**
  - Determining whether any of the devices used qualify as medical devices.
  - Data protection compliance – assessing whether health data is collected by publishers or whether this is strictly limited to the local device, ensuring a lawful basis for processing (likely to be consent), ensuring privacy by design, explaining data processing to individuals, implementation of necessary security measures and retention of necessary information.
  - Contractual issues between the various suppliers of services and devices.
- **Virtual Assistants (e.g. Alexa)**
  Similar issues as for Telehealth.
- **Mobile Apps**
  Similar issues as for Telehealth.
- **Software as a Medical Device**
  - Compliance with MDR 2002.
  - Data Protection compliance. Similar issues as for Telehealth.
- **Clinical Decision Support Software**
  Similar issues as for Telehealth.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  Similar issues as for Telehealth.
- **IoT (Internet of Things) and Connected Devices**
  Similar issues as for Telehealth.
- **3D Printing/Bioprinting**
  - Liability allocation for poor outcomes – designer, manufacturer and/or HCP.
  - Contractual issues between the various suppliers and customers of services/products.
  - IP ownership issues.
- **Digital Therapeutics**
  Similar issues as for Telehealth.
- **Digital Diagnostics**
  Similar issues as for Telehealth.
- **Electronic Medical Record Management Solutions**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring compliance with data retention rules.
  - Cybersecurity.
  - Contractual issues between the various suppliers of services.
- **Big Data Analytics**
  - Data protection and patient confidentiality compliance – determining the roles of the parties involved, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; implementation of necessary security measures; and ensuring that algorithms are robust and unbiased.
  - Liability allocation for poor outcomes – algorithm designer and/or HCP.
  - Contractual issues between the various suppliers of services.
- **Blockchain-based Healthcare Data Sharing Solutions**
  Data protection and patient confidentiality compliance – determining the roles of the parties involved, difficulties with amending records, issues with "right to be

forgotten" and erasure of data, appropriate notice and consent practices; determining an appropriate method of handling patient records and sharing with primary care trusts; and implementation of necessary security measures.

- **Natural Language Processing**
  To the extent applicable, similar issues as for Telehealth and Big Data Analytics.

**3.2 What are the key legal and regulatory issues for digital platform providers in the digital health space?**

Data protection and especially the lawful transmission, storing, processing and use of data – and ensuring adequate consent to such use has been obtained. International data transfers remain a compliance hot topic.

The digital platform provider must ensure, to the extent it is responsible: (i) that advice and services provided on the platform are fit for purpose as failure to process information resulting in personal injury may result in liability; and (ii) where the activity requires registration as a regulated activity, such activity is registered and complies with relevant regulations.

## 4 Data Use

**4.1 What are the key legal or regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction for use of personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?**

- The UK GDPR and DPA are the primary laws to consider in relation to data use in the UK. Patient confidentiality is separately regulated as a matter of common law, and is also relevant to the legality of processing personal data.
- Key issues include determining whether relevant data is personal data or has been sufficiently anonymised. Anonymisation is recognised as difficult to achieve in practice, and may reduce the utility of the relevant dataset. Simply removing identifiers may result in pseudonymous data, which is still caught by the UK GDPR.
- Also important is confirming the roles of the parties involved in the processing – which parties are controllers or processors – and putting appropriate contracts in place.
- Identifying whether data is *concerning health* (and therefore subject to more stringent rules, as are other categories of "special-category" data such as personal data on sex life or religion), *versus* less sensitive data that might, for instance, be collected for wellness purposes is usually a key consideration for technologies (e.g. step counts, sporting performance, etc.).
- An important requirement is identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Health data uses almost always require the carrying out of a Data Protection Impact Assessment (**DPIA**), and ensuring that appropriate risk mitigations are put in place, including measures to ensure data minimisation, privacy by design, data retention limits and appropriate information security measures.
- As mentioned above, ensuring that any overlapping requirements related to rules on patient confidentiality are met is also vital.

**4.2 How, if at all, is personal health data use being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?**

This is not applicable, except as relates to the NHS – see question 4.3 below.

**4.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., personal health data), involved?**

There is a significant distinction between the use of data within *versus* outside the NHS; the impact of "soft law", such as restrictions deriving from NHS policy and "Directions" issued by the UK Secretary of State, will be more acutely felt when working with NHS-originating data, compared to data in (or sourced from) private or consumer settings.

Even in public sector contexts, the rules differ between different parts of the UK. An important example is the "National Data Opt-out", a scheme allowing NHS patients to easily opt out from certain secondary uses of their personal data in England. This does not apply to patient data from Northern Ireland, Scotland or Wales.

**4.4 How do the regulations define the scope of personal health data use?**

The GDPR/DPA generally prohibit the use of health-related personal data without prior, explicit consent, but list exemptions from that restriction – e.g. use of personal data to provide healthcare (by or under the responsibility of a person bound by a duty of confidentiality) is permitted. Similarly, they allow non-consensual scientific research in the public interest (provided that such research does not entail the taking of decisions affecting the relevant individual(s), unless the project has ethical committee approval).

However, as noted in the response to question 4.7 below, there are overlapping restrictions under contract, soft law and confidentiality/misuse of private information (**MoPI**) rules, which may affect the need to obtain consent.

Although this consent does not have to meet the same standard as explicit consent under the UK GDPR, care should be taken (and specialist advice obtained) to ensure that, where relying on UK GDPR/DPA grounds for processing personal data, these restrictions do not apply to the use of personal data.

**4.5 To help ensure comprehensive rights for personal health data use and data collection, what are the key contractual terms to consider in abiding by your jurisdiction's laws and regulations related to personal health data use and data collection?**

Digital health companies will often find themselves subject to heavy requirements imposed by NHS customers. Organisations not dealing with the NHS will often have greater freedom to operate.

More generally, a key consideration for the design and negotiation of contracts is whether, for UK GDPR purposes, the different parties are "processors" or "controllers" of the data – and in the latter case, whether two or more parties are "joint" or "independent" controllers. That classification will dictate the UK GDPR-imposed terms that must be included in the contract, and also inform each party's compliance strategy

and required risk protections (indemnities, warranties, due diligence and insurance).

If personal data is travelling internationally, then the UK GDPR will often require that additional contractual terms (typically based on a pre-approved set of "standard"/"model" contractual clauses) must be put in place between the data's exporter(s) and importer(s), and onward transferees.

By contrast, UK data protection laws generally have little impact on contracts with individuals; data protection-related matters should be dealt with outside of those contracts (e.g. through dedicated privacy notices, and stand-alone consent requests).

The legality of planned and future uses of personal data will be conditional on ensuring that notices, consents, contracts and/or lawful exemptions cover all anticipated uses – or expose an organisation to significant investigations and civil and/or criminal liability. In parallel, failure to secure appropriate IP rights from rights holders can expose the organisation to a risk of being sued by that organisation, and/or additional criminal liability under the DPA (if the data is personal data).

### 4.6 How are issues with personal health data inaccuracy, bias and/or discrimination addressed by the regulatory authorities in your jurisdiction?

The UK GDPR requires controllers to ensure that data is accurate, up to date and processed fairly. It also requires controllers to notify individuals about how their data may be processed, including the logic used in automated decisions made about them. It further requires controllers to ensure that any individuals are not subject to substantial and entirely automated decision-making without explicit consent, contractual necessity or legal obligation.

The ICO has released detailed guidance on the use of AI, including guidance on addressing risks associated with automation such as bias, automated decision-making and risks of discrimination. The ICO is also carrying out active investigations into the use of AI tools in certain sectors, such as recruitment, and the potential for bias in the use of these tools.

The NHS in England has an active AI Ethics Initiative, run by the NHS AI Lab, which has various projects considering bias and risk in AI datasets.

### 4.7 What laws or initiatives exist regarding standards for using and collecting personal health data in your jurisdiction?

The use of personal data in digital health is regulated primarily by the UK GDPR, the DPA and laws on confidentiality that vary between the different parts of the UK.

In addition, a substantial body of "soft law" tends to be imposed by other stakeholders' policies and contracts.

Additional legislation can apply for specific data uses, e.g. the Privacy and Electronic Communication Regulations restricts non-consensual access to and storage of data on Internet-connected devices. Medical device or clinical trial laws further limit the use of personal data.

- The UK GDPR imposes significant restrictions on the use of health data without providing notice of that use and demonstrating an appropriate legal basis for processing the special-category data. Often, explicit consents from individuals will be necessary. This must be specific, informed and freely given.
- Operators in England and Wales (in particular) must also deal with more restrictive requirements of "common law", particularly surrounding patient confidentiality and MoPI. Without consent (which for confidentiality/MoPI purposes could be implied or explicit), or a clear statutory permission, only uses of patient personal data that are necessary for patient care or in the public interest, are permitted under English and Welsh law on confidentiality and MoPI.
- The UK GDPR also imposes additional requirements, including to keep data secure, maintain its availability and accuracy, report data incidents, appoint a Data Protection Officer and/or a "Representative", conduct DPIAs, and generally ensure that usage of personal data is fair, lawful and does not involve excessive amounts of data.
- The UK GDPR grants individuals substantial personal data rights, e.g. to access or delete their data. The DPA adds certain additional rules, including criminal offences for re-identifying personal data, or selling it after it has been improperly obtained.
- Data protection law also includes laws that regulate the use of automated means to take significant decisions that have legal or "substantially similar" effects on an individual. This will need to be borne in mind as software (e.g. AI) becomes increasingly capable of replacing (rather than merely supporting) human decision-making in healthcare settings.
- Organisations should be aware that the UK Government has recently laid draft legislation to review UK data protection law, including provisions that will alter requirements on accountability, further processing and definitions of consent. A stated aim of the Government is the lessening of the burden on organisations carrying out research. A close eye should be kept on these developments throughout 2025.

## 5 Data Sharing

### 5.1 What are the key legal and regulatory issues, and corresponding laws/regulations, to consider in your jurisdiction when sharing personal health data, including laws/regulations that are agnostic and not necessarily specific to healthcare technologies?

As with general use of such data, the key laws are the UK GDPR, the DPA and patient confidentiality derived from common law. The sharing of personal data means that confidentiality and privacy concerns will often be more acute than simply using data within a single organisation. For example, in England and Wales, even greater attention needs to be paid to the existence of a care need, consent, statutory permission and/or a public interest justification for the proposed data sharing if it involves patient data processed for the purposes of providing care. To complicate matters, that legal basis might be different for the different parties, and thus subject to differing restrictions and conditions.

Sharing personal data also introduces potentially significant counterparty risk: both parties to a data-sharing arrangement might face legal risk even if just one of the parties misuses the data. Due diligence, contracting and clear compliance arrangements are therefore important.

Key aspects of the data sharing may need to be explained to individuals, in accordance with the GDPR's transparency obligations. Finally, sharing personal data across borders – even just by providing remote access to it – raises GDPR data transfer compliance issues.

**5.2 How, if at all, is personal health data sharing being differentially regulated by the State/Regional and Federal/Country level regulatory authorities in your jurisdiction?**

This is not applicable.

**5.3 How do such considerations change depending on the nature of the entities, or nature of the data (e.g., patient data), involved?**

As with data use, key legal variations tend to be driven by differences in the purpose of data sharing, not the nature of the entities involved. That said, certain public sector entities (particularly, those within the NHS) might have specific legal powers – or restrictions – regarding data sharing and the performance of their public duties. This could also vary depending on their location within the UK.

**5.4 What laws or initiatives exist regarding standards for sharing healthcare data in your jurisdiction?**

There are numerous NHS initiatives for the sharing of healthcare data. For example:

- NHS England has a role as statutory custodian for health and social care data for England, taking a role in creating data collections, data sets and allowing specific authorised access to third parties.
- The Health Research Authority's (**HRA**) Confidentiality Advisory Group provides independent expert advice to the MHRA and the Secretary of State for Health on whether applications to access confidential patient or service user information without consent should or should not be approved.
- The Clinical Practice Research Datalink, a real-world research service supporting retrospective and prospective public health and clinical studies collecting data from a network of services.
- The NHS Federated Data Platform.
- The NHS Data Security and Protection Toolkit, for those who have access to NHS data.
- NHS pilot programmes, including Improving Elective Care Coordination for Patients and Dynamic Discharges.

**5.5 What are the key issues, laws and regulations to consider with respect to federated models of healthcare data sharing?**

Where a choice has been taken to consider federated learning data sharing for the purposes of protecting patient confidentiality and personal data, it is key to ensure that appropriate protections are offered by the tools, software and contracts establishing this framework to ensure these purposes are fulfilled – there must be appropriate security, use of sufficient anonymisation tools and restrictions on sharing to ensure the intended benefits are achieved.

The preceding responses, in particular to questions 4.1, 4.5, 5.1 and 5.3, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

## 6 Intellectual Property

**6.1 How do patent laws in your jurisdiction impact the scope of patent protection for digital health technologies?**

Patent protection is still available for digital health technologies that satisfy the requirements for the grant of a patent in accordance with the UK Patents Act 1977 (**PA**).

**6.2 How do copyright laws in your jurisdiction impact the scope of copyright protection for digital health technologies?**

Copyright protection is still available for digital health technologies that satisfy the requirements of the UK Copyright, Designs and Patents Act 1988 (**CDPA**); see also response to question 6.5 with respect to protection of software.

**6.3 How do trade secret laws in your jurisdiction impact the scope of trade secret protection for digital health technologies?**

Digital health technologies that satisfy the requirements of a trade secret and/or confidential information will continue to be protected as a trade secret (protection under statute) and by the common law of confidence, which protects information that:

- has a quality of confidence;
- is disclosed under an express or implied obligation of confidence; and
- is used or further disclosed in an unauthorised manner.

The UK Trade Secrets (Enforcement, etc.) Regulations 2018 also prevent acquisition, use or disclosure of trade secrets where this would constitute a breach of confidence in confidential information.

**6.4 What are the rules or laws that apply to, or regulate, academic technology transfers in your jurisdiction?**

IP rights in technology developed in academic institutions usually vests in the academic institution, as a result of employment or other contractual arrangements. Absent contractual arrangements, the ownership of IP rights can be more complicated. Academic institutions typically seek to commercialise technologies by way of licensing arrangements (for example, to existing businesses, commercial research partners, or via the creation of a spin-out company dedicated to commercialising the technology).

There are no specific laws governing academic technology transfer. In very rare cases, under the PA, the publication of a patent or disclosure of related information may be restricted if it might be prejudicial to national security or public safety, with resulting effects on technology transfer.

**6.5 How do intellectual property laws in your jurisdiction impact the scope of intellectual property protection for software as a medical device?**

A software-implemented invention is only patentable in the UK to the extent that it meets the requirements in the PA. While

inventions implemented in software are patentable, software *per se* is not. The requirements are stringent and difficult to meet. Generally, software *per se* will be protected as a literary work under the CDPA (although the protection applies to the particular expression of ideas and principles that underly an algorithm and not to the ideas and principles themselves) (see response to question 6.2).

**6.6 Can an artificial intelligence device be named as an inventor of a patent in your jurisdiction? Why or why not?**

No. Following the decision of the UK Supreme Court in *Stephen L Thaler v The Comptroller- General of Patents, Designs And Trade Marks* [2023] UKSC 49, an AI device cannot be named as an inventor of a patent in the UK under current legislation. In October 2021, the UK Intellectual Property Office (**UKIPO**) (the executive Government Department) issued a public consultation on whether the PA should be amended to permit an AI system to be named as an inventor or whether the definition of inventor should be expanded to include humans responsible for an AI system that devises inventions. The outcome of the consultation was that AI was not considered advanced enough to invent without human intervention and that there was therefore no planned change to UK patent law for AI-devised inventions.

**6.7 What scope of intellectual property rights are provided to the government by rules/laws related to government-funded inventions?**

Government funding for innovation is available in the UK. This funding is classed as a subsidy and therefore must be consistent with the UK subsidy control regime, WTO rules, the EU–UK Trade and Cooperation agreement and other bilateral UK Free Trade agreements.

**6.8 What are the key precedential legal cases or decisions affecting intellectual property rights protection of digital health innovation in your jurisdiction?**

The following guidelines and IP decisions are particularly relevant with regard to the AI and software aspects of digital health innovations. The UKIPO and the European Patent Office (**EPO**) have established guidelines on the patentability of AI-related innovations. The various responses to the UK Government's 2024 consultation into the general regulatory landscape regarding AI and ML also provide useful guidance on the rationales that may inform future decisions from regulators.

Patent case law emphasise the importance of demonstrating that the software component of the digital health product has a technical effect, beyond the mere implementation of a mathematical method on a computer. For instance, the EPO's decision in G 1/19 (Simulations) and the UK court's decision in *Aerotel v Telco and Macrossan's Application* [2006] EWCA Civ 1371 clarified the approach to computer-implemented inventions, which can be relevant to AI in digital health.

Copyright case law in relation to software programming highlight that ideas and principles (such as operational methods, mathematical concepts and procedures) in software are not protected by copyright (*SAS Institute v World Programming*, Case C-406/10; *Nova Productions Ltd v Mazooma Games Ltd* [2007] EWCA Civ 219). Therefore, a competitor can develop a competing software product that does effectively the same thing or operates according to the same principles, as long as the competitor did not copy the code or other pivotal structural design aspects of the original product.

## 7 Commercial Agreements

**7.1 What contractual and strategic considerations should parties consider when dealing with collaborative improvements?**

It is often suggested that joint ownership of IP/improvements is the fairest way of approaching collaborations. The downside of this blanket approach is that treatment of jointly owned IP varies from jurisdiction to jurisdiction and also by IP right. The consequence is that the joint owner might be unclear as to their rights to exploit such IP if not expressly set out in the collaboration agreements.

Alternative ways of approaching collaborative improvements would be for ownership to follow the ownership of background on which the improvement is made or to assign such collaborative improvements in accordance with predetermined fields of use. In all instances, it would be prudent to include relevant licences to background and royalty provisions, as applicable.

More broadly, parties should consider including robust provisions relating to confidentiality to protect sensitive information shared during the collaboration, as well as clearly defining performance obligations and milestones to track progress and ensure accountability. The parties should be prepared to adapt to changing circumstances and new information and rightsholders, as flexibility is crucial for navigating the dynamic nature of collaborative projects in digital health technologies.

**7.2 What contractual and strategic considerations should parties consider when dealing with agreements between healthcare and non-healthcare companies?**

As with any agreement, the allocation of rights and obligations should be set out clearly, especially in relation to liability. It is likely that the parties will have responsibilities related to their respective expertise, and these should be specified, as well as responsibility for data protection compliance.

Public sector HCPs often have very strict rules (even to the extent of bureaucracy) which can mean that negotiation of IP rights, for example, can be difficult to deviate from standard form agreements. The parties should therefore ensure that the agreement includes provisions for compliance with relevant healthcare regulations and standards.

**7.3 What contractual and strategic considerations should parties consider when dealing with federated learning healthcare data sharing agreements between companies?**

Agreements should carefully outline the terms of the data sharing, specifying who has control over the data and how decisions regarding data usage will be made. Issues related to data access, modification and deletion should also be addressed. Rules around ownership of the model itself should also be established.

As the raw data is not shared, parties should agree on common data formats and standards to ensure interoperability. Ideally, the data sharing agreement should facilitate

seamless integration of data from different sources, potentially by using established healthcare interoperability standards such as Fast Healthcare Interoperability Resources.

Agreements should also comply with data protection laws, for example, setting out rules around data minimisation and purpose limitation.

**7.4 What contractual and strategic considerations should parties consider when dealing with the use of generative AI in the provisioning of digital health solutions?**

Parties should ensure clear data ownership agreements that respect the interests and expectations of both parties, as well as data subjects and stakeholders involved.

The quality and availability of data is another consideration. It may be difficult to obtain large amounts of high-quality data to train the AI model due to the sensitive and confidential nature of most healthcare data. Biased, inaccurate or unrepresentative data in datasets could lead to bias or inaccuracies in the results.

Navigating rules around patient privacy and data protection will also be an issue, along with rules and regulations governing generative AI itself, which are rapidly evolving from country to country.

## 8 Artificial Intelligence and Machine Learning

**8.1 What are the principal regulatory authorities charged with enforcing regulatory schemes related to AI/ML in your jurisdiction? What is each authority's scope of enforcement?**

There is currently no AI-dedicated regulator in the UK. Regulators have been encouraged by the Government to develop approaches specific to their own domains, and the wider approach to legislation and development is under development. See response to question 8.2 below for information about important programmes of relevance to AI/ML in healthcare.

**8.2 For these authorities, what are the core regulatory schemes related to AI/ML in your jurisdiction? Please also describe any regulatory schemes specific to AI/ML in healthcare.**

For now, unlike the EU, there is currently no specific regulatory regime in relation to AI/ML in the UK, although the Government is developing an AI Opportunities Action Plan over the course of 2025. At the moment, there are cross-sector guiding principles published by the UK Government that are implemented by various regulatory authorities using their existing powers and under existing regimes. However, the landscape is developing. In particular:

- The Government Department for Science, Innovation and Technology has a special division, the AI Safety Institute – a state-backed organisation to conduct research and safety assessments for AI in the UK.
- In early 2024, a Government consultation concluded into the general regulatory landscape under AI and ML topics was conducted. The consultation involved communication with, and consultation responses from, many interested regulators including the MHRA, ICO and Office for Statistics Regulation (the body governing official statistics in the UK). The regulator responses to the Government consultation, and the consultation itself, are useful resources for understanding the direction of movement, albeit that the incumbent Government has changed in the UK since that consultation took place and, to the extent that regulation is enacted pursuant to Government policy, the policy objectives may differ (as to which, see below).
- The MHRA in particular has been active in developing its regulatory posture and has conducted consultation and development activities since at least 2021.
- In December 2024, a Government consultation and call for views began in the field of copyright and AI. The consultation will run until at least February 2025.
- The Government has stated its policy goals in relation to AI generally, and the overlap between AI and IP specifically, to be broadly in favour of promoting the development and adoption of AI technologies in the UK.
- It is therefore likely that the regulatory response to AI will develop significantly throughout the course of 2025.

Some regulatory programmes with specific relevance to digital health include:

- **Personal Data**: The ICO lists AI as a "priority area" due to the potential effects on individuals. The ICO operates a regulatory "Sandbox" programme, which is a free service designed to give access to regulators themselves, for businesses in need of specific guidance. The ICO lists digital healthcare companies as examples of beneficiaries of this programme.
- **SaMD**: The MHRA operates a dedicated Software Group for the regulation of SaMD *per se*. In October 2022, the agency published a Roadmap for the regulation of AIaMD. The Roadmap indicated a blend of recommended legislative, regulatory and best-practice guidelines in that context. The recommendations ranged from passing new laws, to changing the use of nomenclature and increased monitoring and surveillance of SaMD in use.
- **Health Data Governance**: NHS Digital and the HRA oversee the use of health data in AI/ML applications. They regulate the use of data in healthcare AI in respect of compliance with data protection laws and ethical standards, particularly in research contexts.
- **AI in Clinical Trials and Research**: For AI/ML technologies used in clinical trials, the HRA and MHRA provide guidance on ethical considerations, data management and regulatory compliance. This includes ensuring that AI systems used in research are transparent, explainable and subject to rigorous evaluation.
- **Ethical Standards and Best Practices**: NICE has, in 2024, published an AI Code of Ethics, covering seven topics (plus sub-topics) for the adoption of AI in clinical and research settings. The principles touch on broad matters including integrity, transparency and accountability, as well as addressing specific concerns such as bias mitigation, and the use of quality checks and regular assessments.

**8.3 Who owns the intellectual property rights to algorithms that are improved by AI/ML without active human involvement in the software development?**

Under English law, algorithms are potentially protectable by copyright as original literary works, although the protection

applies to the particular expression of ideas and principles that underly an algorithm and not to the ideas and principles themselves.

Where an algorithm is written by a human, the author of that work is the person who creates it (Section 9(1) CDPA). This is taken to be the person responsible for the protectable elements of the work, being those elements which make the work "original" (i.e. those parts that are the "author's own intellectual creation").

First ownership of a work and the duration of the protection available are defined with reference to the author. However, where an algorithm is written using ML without active human involvement, it may not be possible to identify a human who can be said to have created the work, i.e. there is no human author such that the work qualifies as "computer generated" under Section 178 CDPA. In these circumstances, Section 9(3) CDPA deems that the author of the work is the "person by whom the arrangements necessary for the creation of the work are undertaken". This can potentially be one or more natural or legal persons. Under Section 12(7), the duration of protection of a computer-generated work is 50 years from the end of the calendar year in which it is created.

While the test set out in Section 9(3) CDPA determines the identity of the author of a computer-generated work, it is not currently clear as a matter of English law whether such work will qualify as copyright work. Under Section 1(1) CDPA, copyright only subsists in original literary works, which requires an intellectual creation by the author which reflects an expression of their personality. It is questionable whether an algorithm developed by ML without human involvement could be said to be an intellectual creation reflecting the personality of the person making the arrangements necessary for its creation.

As a result, such an algorithm may not qualify for copyright protection under English law. An alternative view is that Section 9(3) CDPA in fact creates its own *sui generis* right for computer-generated works which is not subject to the usual requirement for originality. These issues have not thus far been addressed by the English courts and claims to copyright (or an absence of rights) in algorithms developed by ML without human intervention must therefore be treated with caution.

In October 2021, the UKIPO issued a public consultation seeking views on possible reforms to the protection of computer-generated works in the UK. The options under consideration included retaining the existing position under Section 9(3) CDPA, removing protection for computer-generated works or replacing Section 9(3) with a new and narrower form of protection with a limited duration, e.g. five years from creation. The UKIPO published its response to the consultation on 28 June 2022. It concluded that AI was still in its early stages, and it was not possible to undertake a proper evaluation of any changes to the law, which may have unintended consequences. The Government therefore proposed to make no changes to the current law, while keeping a decision of whether to amend, replace or remove protection under Section 9(3) under review.

Note that over the course of 2025, the UK Government is expected to continue to develop and set out its approach on AI regulation and will act to ensure the UK has a competitive copyright regime that supports the UK's AI sector. The Government has cited AI technology as a major part of its policy focus.

### 8.4 What commercial contractual and strategic considerations apply to licensing data for use in AI/ML? How do these considerations change when licensing healthcare data?

Many ML projects often involve collaboration between a party with expertise in deploying ML and another party with access to the data required to train a ML system to solve a particular problem. Common commercial issues that arise in this context include the rights each party obtains in the resulting system, e.g. can the resulting system be resold to others or adapted for purposes that go beyond those originally envisaged?

Similar considerations apply to the future use and disclosure of the training data itself, e.g. is the recipient allowed to retain the data after the project is complete and can it be re-used for other purposes (either in its original form or in some aggregated/derived form) and/or shared with third parties (and if so, under what terms)? Where the data is provided on a long-term basis with a defined scope of use, the licensor may wish to include audit rights to ensure the data continues to be used and disclosed in compliance with the terms of the licence.

Data licences will need to address potential liabilities arising from use of the licensed data. These will include any harm arising from defects in the licensed data, e.g. systematic inaccuracies in training could give rise to models that do not perform as required. A licensor will generally try to disclaim liability for errors or inaccuracies in a dataset. Liabilities could also arise through infringement of third-party rights in the data. These could include infringement of IP rights and other related rights, e.g. infringement of copyright in scientific publications or breach of an obligation of confidence owed by the licensor to a third party with respect to a particular dataset. In addition to conducting pre-contract due diligence on the legal rights affecting datasets, licensees will also often seek warranties and indemnities in the licence agreement to reduce their exposure to these risks.

Issues regarding use of training data commonly arise in the context of AI service agreements. An AI service provider will commonly wish to re-use data received from a customer during the course of providing the service to further improve the AI system that is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms that permit this re-use of their data for these purposes, considering it to be a net value transfer from them to the service provider. Provisions relating to the use of derived data and meta-data, anonymisation and data retention post-termination may all be affected by this issue.

### 8.5 How, if at all, do the regulatory bodies overseeing AI/ML technologies differentiate standard AI vs. generative AI technologies and products?

At present, UK regulatory bodies have not established distinct regulatory frameworks specifically differentiating between standard AI and generative AI technologies. However, they are aware of the unique challenges and considerations that generative AI presents. For instance, the MHRA is working with a developer of a generative AI tool that helps users write documents or analyse data. Additionally, the Digital Regulation Cooperation Forum – formed of the ICO, Ofcom, Competition and Markets Authority (**CMA**) and Financial Conduct Authority – undertook joint consumer research on generative AI; the joint report found that consumers tend to assume regulation is in place if using generative AI in certain settings (financial services in particular) and expect organisations deploying generative AI tools to be accountable if things go wrong; as such, warnings and messaging can increase consumers' sense of personal responsibility.

**8.6 What are the legal or regulatory issues that are unique to generative AI technologies and how are those issues being addressed in your jurisdiction? Describe initiatives within your jurisdiction committed to continued development of regulations related to generative AI?**

**IP**: In the field of IP, the dominant conversation concerns the use of copyright-protected works for the training of ML models, and the effect of the use of ML models on IP rights ownership in their outputs. The UK Government's *AI Opportunities Action Plan* (2025) highlights that it will act to ensure there is a competitive copyright regime that supports the UK's AI sector, and states that it may take forward the recommendation of establishing a copyright cleared training data set that can be licensed internationally at scale.

**Misinformation, Deepfakes and Defamation**: The UK Government's ongoing open consultation on copyright and AI includes assessing whether the current legal framework is sufficient to provide individuals with control over use of their likeness and whether further intervention is required. The ICO is also currently reviewing the application of UK data protection rules in this area and will issue guidance in due course.

**Bias and Discrimination**: Fairness is one of the UK Government's guiding AI principles and is therefore a key aspect implemented by regulatory authorities such as the ICO and CMA and NICE (as referred to above). Additionally, in 2023–2024, a UK Government scheme offered £400,000 in investment to fund innovative solutions to tackle bias and discrimination in AI systems. One of the winners of the scheme was King's College London, who will design a solution to address bias and discrimination in healthcare, in particular in early warning systems used to predict cardiac arrest in hospital wards.

**Data Privacy and Confidentiality**: This continues to raise issues with respect to: the use of personal data and training materials; the potential applications of synthetic data; and security issues arising from the risk of AI-powered malware.

**Accountability and Liability**: This will be a significantly developing issue. Questions of responsibility for actions attributable to AI are not clear under the current law. The regulatory response is being developed, and accountability is one of the UK Government's guiding AI principles and is therefore a key consideration for regulatory authorities.

**8.7 How is your jurisdiction addressing trained AI/ML models that may include data for which the developer lacks the appropriate data rights for use in the given AI/ML model? Are there data disgorgement laws and/or initiatives in your jurisdiction? Please describe.**

These are difficult issues under the UK law and are currently before the courts in at least one major dispute. It is likely that the first half of 2025 will begin to bring clarity to the assessment of these questions, at least from a jurisdictional standpoint. It is also highly likely that some legislative or policy developments will emerge from the open consultation on copyright and AI that is currently underway.

## 9 Liability

**9.1 What theories of liability apply to adverse outcomes in digital health solutions?**

Liability for adverse outcomes in digital health is governed both by the law of contract (where services are delivered in accordance with a contract) and by the common law of tort/negligence where, whether or not a contract is in place, a duty of care exists between parties, and a breach of that duty (by falling below the reasonable standard expected in carrying out that duty) causes loss (including personal injury).

Additionally, the UK Consumer Protection Act 1987 sets out a strict liability regime for consumer products, including medical devices. In summary, under such claims a claimant does not need to show any fault on the part of the defendant. Instead, a claimant needs to demonstrate: (i) the presence of a defect in a product according to an objective standard of safety as reasonably expected by the public; and (ii) a causal link between that defect and the loss suffered.

Finally, the UK GDPR might create joint and several liability between partnering organisations if non-compliance led to an adverse outcome – for example, basing clinical decisions on inaccurately-recorded patient data or a biased algorithm.

**9.2 What cross-border considerations are there?**

Previously, under EU law (the Rome Regulations), generally, UK national (English and Welsh, Scots or Northern Irish) laws have applied to non-contractual (e.g. personal injury) and contractual claims based on digital health delivery to consumers/patients in the UK, whatever the country of origin of the provider. In accordance with retained EU law, the situation is not expected to change significantly in the short term.

**9.3 What are best practices to minimise liability risks posed by the use of AI/ML (including standard AI and generative AI) in the provisioning of digital health solutions?**

Developers of generative AI products bear a duty towards the end-users, especially when the AI's decision-making mechanisms are unclear or complex. However, software developers may counter this by stating that generative AI-based healthcare solutions are designed to work in conjunction with HCPs who can overrule them if they propose a potentially harmful path, thereby shifting responsibility to the HCPs.

The British Medical Association's principles for the application of AI in healthcare (2024) provides some best practices to follow, such as ensuring HCP staff and patient involvement throughout the development and implementation process, ensuring HCP staff are initially and continuously trained on new technologies, and allowing HCPs to challenge decisions made by AI.

In the absence of legislation clearly governing liability of parties, it is essential that commercial contracts spell out which party is liable for errors when using generative AI in digital health solutions. Indemnification clauses could limit the liability of HCPs and AI algorithm creators. Alternatively, a special adjudication system could be considered. This would establish a separate legal pathway for addressing claims related to generative AI usage in healthcare, particularly for those claims that are challenging to resolve under current liability structures.

Insurance could serve as a safeguard against the financial risk linked with the application of generative AI by compensating for any potential damages and promoting responsible AI use among HCPs.

When building new generative AI tools, HCPs should insist that developers' models follow the MHRA's 10 guiding principles in relation to good ML practice for medical device development.

**9.4 What theories or liability apply to misuse of healthcare data included in trained AI/ML models used in digital health solutions?**

The general principles briefly set out in the response to question 9.1 above apply. There may also be breach of patient confidentiality if patient data is used without appropriate anonymisation and without consent or other lawful exemption to consent.

## 10 General

**10.1 What are the key issues in Cloud-based services for digital health?**

Key issues include: (i) data security; (ii) commercial re-use of the data by the Cloud-based service provider; and (iii) whether data will leave the UK.

**10.2 What are the key issues that non-healthcare companies should consider before entering today's digital healthcare market?**

It is a complicated and heavily regulated area, with regulations varying, in some instances, within the UK. There is no single, broad-brush approach and given the rapid development of digital health technologies, monitoring regulatory changes will be essential.

**10.3 What are the key issues that venture capital and private equity firms should consider before investing in digital healthcare ventures?**

When considering a target:

- Ensure that procedures are in place for compliance with relevant areas, especially data protection, patient confidentiality, and the variety of medical device regulations and guidance.
- Consider IP ownership and protection – do they own all necessary IP and have steps been taken to secure protection for all material IP, for instance including trade secrets?
- Competitive landscape – what other competing digital health technologies are in the market and what are their competitive advantages, e.g. advanced relationship with NHS, etc.?
- Do they have good supply and service contracts in place, and secure sources of hardware, software and labour?

**10.4 What are the key barrier(s) holding back widespread clinical adoption of digital health solutions in your jurisdiction?**

Generally, the use of digital health solutions in the UK is well established. The COVID-19 pandemic has increased the prevalence of digital health solutions.

However, regarding the delivery of telemedicine services specifically, there remains some legal uncertainty because the UK healthcare regulatory environment is not yet fully updated to deal with the issues arising from the delivery of telemedicine services. However, programmes like the Government's *Life Sciences Vision* and the MHRA's plans for reform to medical device regulation indicate that the regulatory environment is undergoing significant change to address these challenges.

**10.5 What are the key clinician certification bodies (e.g., American College of Radiology, etc.) in your jurisdiction that influence the clinical adoption of digital health solutions?**

While not a clinician certification body *per se*, in the UK, the Association of British HealthTech Industries plays a key role in representing the industry to stakeholders, such as the Government, NHS and regulators.

There is continued need for leadership by the UK Government and its relevant ministries, for instance by ensuring that standardised and easily accessible criteria, such as the NICE Evidence standards framework for digital health technologies, are adopted in a risk-based manner.

**10.6 What reimbursement models have been provided by government and/or private healthcare payors for digital health solutions in your jurisdiction? Describe any formal certification, registration or other requirements in order to be reimbursed?**

This would depend on the digital health solution and in which country in the UK it was deployed. In England, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, for example, telemedicine may, under certain circumstances, be funded via the NHS. The recent launch of the NICE Office for Digital Health, which will work with strategic partners to improve digital health approval pathways and reimbursement policy, may see future development of funding arrangements for digital health solutions.

**10.7 What due diligence gaps exist in the healthcare ecosystem for analysing digital health solutions in general, and particularly those that are data-driven products, including AI/ML-based solutions?**

There may be various gaps depending on the complexity of the digital health solution in question, but potential due diligence gaps may include matters relating to data provenance, quality and integrity, regulatory compliance (from a data protection and medical device perspective, among others), interoperability issues, relationships with the NHS and HCPs, ethical considerations, etc.

**10.8 Describe any other issues not considered above that may be worthy of note, together with any trends or likely future developments that may be of interest.**

A key trend to watch in 2025 is the increased use of genomic data and the resulting growth of precision diagnostics. As part of the Genome UK: 2022 to 2025 implementation plan, the UK Government is investing a total of £178 million for the research and implementation of genomic medicine. While the regulatory and data concerns highlighted above are sure to apply as genomic data is harnessed at scale, other concerns may develop as the regulatory landscape struggles to cope with such rapid developments in genomic technologies.

We can expect to see further disruption to the medical device and life science sectors, as the use of smartphones

and social media continue to transform the way that people manage their health. The practice of medicine has already been transformed by software and we expect this trend to continue, whilst interactions between patients and providers are fundamentally altered and boundaries blurred. Some of the key UK regulatory frameworks applicable to digital health products are also going to be subject to change from 2025.

## Acknowledgments

The authors would like to thank David Pemberton and Quinn Liang for their invaluable contributions in the preparation of this chapter.

**Pieter Erasmus** is a senior associate in the IP Group in London, with a focus on regulatory and commercial matters primarily in the life sciences and healthcare sectors.
Having a keen interest in all things life sciences and healthcare, he specialises primarily in providing regulatory and commercial advice in relation to a broad range of matters in these sectors. His experience includes advising on the regulation of pharmaceuticals, medical devices, general healthcare services, clinical trials, marketing and advertising of health products, borderline products, food and beverages (including food supplements and novel foods), cosmetic products and legislative drafting in the healthcare context. A key focus area is advising on all aspects relating to digital health, including software as medical device, the impact of AI and telemedicine.

**Bird & Bird**
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 905 6217
Email: pieter.erasmus@twobirds.com
LinkedIn: www.linkedin.com/in/pieter-miguel-erasmus

**Emma Drake** is a partner working on data and online safety compliance from the London office. She works with a wide variety of organisations, particularly in the media, sports and life sciences sectors. She also advises extensively on children's and employee privacy matters. Her work covers all aspects of data protection, e-privacy and online safety law, including advice on compliance documentation, policy and procedure, risk and impact assessment and individual rights. She has a particular focus on digital regulation that impacts on the handling of special category data or vulnerable groups, including employees and children. She regularly helps clients with assessment of new products or processes, including across multiple jurisdictions and defence in front of regulators.

**Bird & Bird**
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6728
Email: emma.drake@twobirds.com
LinkedIn: www.linkedin.com/in/emma-drake-43a3573b

**Tristan Sherliker** specialises in resolving IP disputes before the Courts in London, where he is of counsel in the IP practice.
He is a solicitor advocate working in leading IP cases and high-technology disputes. His focus is on litigation in the High Court and Court of Appeal, and advisory work to prevent disputes that could otherwise go there. He builds close working relationships with clients with a deep knowledge of their business, their needs and their technology. In disputes, he acts in the dual role of solicitor and counsel. Before law, his background was in biomedical engineering, combining more traditional engineering disciplines (such as electronics, mechanics, materials science and computing) with medical concepts (including anatomy, drug delivery and biochemistry).

**Bird & Bird**
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6641
Email: tristan.sherliker@twobirds.com
LinkedIn: www.linkedin.com/in/sherliker

**Mario Subramaniam** is a partner in our highly rated (*The Legal 500* and *Chambers*) Life Sciences and IP Team, advising Life Science clients on strategic licensing, collaboration and partnering transactions.
He has over 15 years of experience in advising Life Science clients on the development and exploitation of pharmaceutical, biotech, medtech and digital health technologies, with a particular emphasis on strategic IP licensing, collaboration and partnering transactions, as well as joint ventures, high-value manufacturing, supply and outsourcing arrangements. He also provides strategic support on M&A and asset acquisitions and disposals for Life Science clients.

**Bird & Bird**
12 New Fetter Ln
City of London, London EC4A 1JP
United Kingdom

Tel: +44 207 415 6000
Email: mario.subramaniam@twobirds.com
LinkedIn: www.linkedin.com/in/mariosubramaniam

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

**Digital Health 2025** features one introductory chapter, three expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Digital Health
- Regulatory
- Digital Health Technologies
- Data Use
- Data Sharing
- Intellectual Property
- Commercial Agreements
- Artificial Intelligence and Machine Learning
- Liability

The International Comparative Legal Guides are published by: glg Global Legal Group