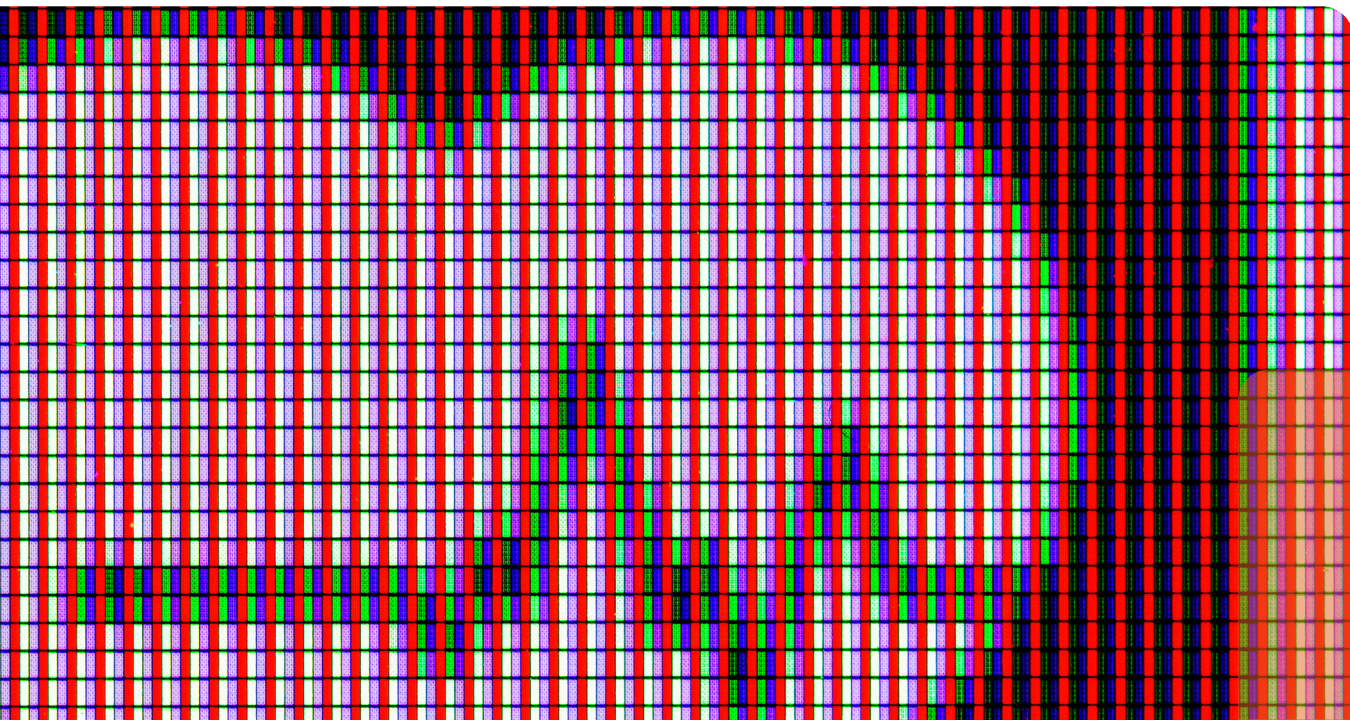


**International
Comparative
Legal Guides**



Digital Health

2024

Fifth Edition

Contributing Editor:

Roger Kuan
Norton Rose Fulbright

glg Global Legal Group

Introductory Chapter

1

Introduction

Roger Kuan, Norton Rose Fulbright
David Wallace, Johnson & Johnson

Expert Analysis Chapters

7

A New Era of Investing and Diligence in Healthcare Solutions

Jason Novak, Dr. Milad Alucozai & Nathanael Green, Norton Rose Fulbright

11

Recent Updates on Emerging Trends in the Global Regulation of Digital Health: Fragmented Frameworks Continue Striving to Catch Up With Technological Advancement

Eveline Van Keymeulen, Elizabeth Richards, Nicole Liffbrig Molife & Oliver Mobasser, Latham & Watkins

Q&A Chapters

20

Australia

Norton Rose Fulbright: Bernard O'Shea & Rohan Sridhar

33

Austria

Herbst Kinsky Rechtsanwälte GmbH:
Dr. Sonja Hebenstreit

43

Belgium

Quinz: Olivier Van Obberghen, Pieter Wyckmans,
Amber Cockx & Chaline Sempels

55

Canada

Norton Rose Fulbright: Vanessa Grant,
Véronique Barry, Brian Chau & Sarah Pennington

67

China

East & Concord Partners: Cindy Hu, Jason Gong & Jiaxin Yang

78

Denmark

Kennedys Copenhagen: Heidi Bloch,
Julia Tomaszewska & Janus Krarup

89

France

Armengaud Guerlain: Catherine Mateu & Pierre Camadini

97

Germany

McDermott Will & Emery Rechtsanwälte
Steuerberater LLP: Jana Grieb, Dr. Deniz Tschammler,
Dr. Claus Färber & Steffen Woitz

108

Greece

Zepos & Yannopoulos: Nefelie Charalabopoulou,
Natalia Kapsi, Yolanda Antoniou-Rapti & Celia Karvouni

116

India

LexOrbis: Manisha Singh & Pankaj Musyuni

124

Israel

Gilat, Bareket & Co., Reinhold Cohn Group:
Eran Bareket & Alexandra Cohen

134

Italy

Astolfi e Associati, Studio Legale: Sonia Selletti,
Giulia Gregori & Claudia Pasturenzi

147

Japan

Nagashima Ohno & Tsunematsu: Masanori Tosu & Kenji Tosaki

155

Korea

Lee & Ko: Jin Hwan Chung, Eileen Jaiyoung Shin & Sungil Bang

163

Mexico

Baker McKenzie: Christian López Silva,
Carla Calderón, Marina Hurtado Cruz & Daniel Villanueva Plasencia

175

Pakistan

Majeed & Partners, Advocates & Counsellors at Law:
Saqib Majeed

185

Portugal

PLMJ: Eduardo Nogueira Pinto,
Hugo Monteiro de Queirós, Tiago Linhares Carneiro & Bartolomeu Soares de Oliveira

194

Spain

Baker McKenzie: Montserrat Llopart Vidal & David Molina Moya

205

Switzerland

Wenger Plattner: Tobias Meili, Carlo Conti,
Martina Braun & André S. Berne

214

Taiwan

Lee and Li, Attorneys-at-Law: Hsiu-Ru Chien,
Eddie Hsiung & Shih-I Wu

223

United Kingdom

Bird & Bird LLP: Sally Shorthose, Toby Bond,
Emma Drake & Pieter Erasmus

233

USA

Norton Rose Fulbright: Roger Kuan, Jason Novak & Apurv Gaurav

United Kingdom



Sally Shorthose



Toby Bond



Emma Drake



Pieter Erasmus

Bird & Bird LLP

1 Digital Health

1.1 What is the general definition of “digital health” in your jurisdiction?

Apps, programmes and software used in the health and care system – either standalone or combined with other products such as medical devices or diagnostic tests.

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

The key emerging digital health technologies in the United Kingdom (**UK**) are as follows:

- 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 distance support to patients either through healthcare practitioners or AI; the integration of telemedicine services with digitised health systems.
- Health data analytics – the digital collation, analysis and distribution (including on a commercial basis).
- Personalised medicine – using genomics to get a faster diagnosis of a condition and being given personalised treatments based on that diagnosis.

1.3 What are the core legal issues in digital health for your jurisdiction?

The two core legal issues are:

- compliance, in the digital collation and handling of patient data, with the requirements of the UK’s General Data Protection Regulation (**UK GDPR**) and the UK Data Protection Act 2018 (**DPA**); and
- compliance, in delivering digital health services, with the relevant UK healthcare regulatory regime. For example, in the case of telemedicine services, the regulatory regime is not yet fully updated to deal with the issues arising from the delivery of telemedicine services.

1.4 What is the digital health market size for your jurisdiction?

Certain sources estimate that the UK healthcare IT and digital market is currently valued at around £5 billion, although this is likely to grow significantly.

1.5 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 in the UK include:

- Babylon Health;
- Teladoc;
- Cera;
- Huma;
- DnaNudge; and
- Lumeon.

2 Regulatory

2.1 What are the core healthcare regulatory schemes related to digital health in your jurisdiction?

England, Scotland, Wales and Northern Ireland each have their own regulatory regime and competent authority. In England (approximately 85% of the UK population), the relevant legislation is the UK Health and Social Care Act 2008. Broadly equivalent legislation and regulators are in place in the other UK nations. All national regimes require all providers of regulated healthcare services (including e.g. telemedicine) to meet the requirements of the applicable legislation and to register with the relevant national regulatory body in order to be able to legally undertake those services.

Medicines and healthcare products (including software as a medical device (**SaMD**)) are governed across the UK by the UK Human Medicines Regulations 2012 and the UK Medical Device Regulations 2002 (**MDR 2002**), as amended.

General legislation such as the Electronic Commerce Regulations 2002, the Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008 may also be relevant to digital health.

2.2 What other core regulatory schemes (e.g., data privacy, anti-kickback, national security, etc.) apply to digital health 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 (England, Northern Ireland, Scotland and Wales).

2.3 What regulatory schemes apply to consumer healthcare devices or software in particular?

Consumer health devices are, to the extent they are “medical devices”, covered by the MDR 2002, as amended. All medical devices need to meet the applicable UK Conformity Assessed (UKCA) marking requirements in these regulations and must be registered. However, as part of the guidance regarding transitional arrangements published by the Medicines and Healthcare products Regulatory Agency (MHRA) in October 2022, manufacturers will be able to continue to place CE marked medical devices on the Great Britain market until the end of June 2024. There will be separate requirements for certain medical devices placed on the Northern Ireland market, which is currently aligned with the EU regime.

All consumer devices that are not regulated as medical devices under the MDR 2002 are regulated by the UK General Product Safety Regulations 2005 and those other CE/UKCA marking regulations which apply to the specific product, e.g. UK Electrical Equipment (Safety) Regulations 2016, etc. Evidence of compliance with applicable CE/UKCA marking laws and regulations must be compiled and maintained by a nominated responsible person in the UK where the manufacturer is based outside the UK. Based on recent guidance, manufacturers of the aforesaid consumer devices that are not regulated as medical devices may continue to use the CE marking on the Great Britain market until 31 December 2024.

2.4 What are the principal regulatory authorities charged with enforcing the regulatory schemes? What is the scope of their respective jurisdictions?

For the healthcare regulatory regimes in the four nations, the relevant regulatory authorities are:

- England – Care Quality Commission.
- Scotland – Healthcare Improvement Scotland.
- Wales – Care Inspectorate Wales.
- Northern Ireland – The Regulation and Quality Improvement Authority.

The MHRA is the competent regulatory authority for medical devices and maintains the register of such devices. Various regulatory bodies have responsibility for particular UKCA marking regulations.

2.5 What are the key areas of enforcement when it comes to digital health?

Primary areas of concern:

- Telemedicine service providers: Loss of registration (and thus loss of ability to legally provide healthcare services) for failing to comply with the relevant standards. Serious criminal conduct may result in prosecution and significant fines.
- Medical devices (including software): Failure to comply with the relevant regulations can result in the product being

recalled and withdrawn from market by the MHRA, and, if there is serious failure to comply with the regulations, an unlimited fine and/or six months imprisonment on conviction.

- In general: Privacy and data security.

2.6 What regulations apply to software as a medical device and its approval for clinical use?

SaMD is governed by the MDR 2002, as amended. In 2022, the MHRA published a “roadmap” for its *Software and AI as a Medical Device Change Programme* published the previous year. Though, the roadmap provides that the changes will primarily come in the form of guidance, some secondary legislation is expected. For example, the MHRA intends to develop secondary legislation to account for cybersecurity and IT risks relating to the large amount of personal data generated in the field of SaMD. The MHRA have further indicated that their aim is to bring new regulations into force by July 2024. The exact outcome of the programme and roadmap on the regulatory landscape in the UK is not yet clear but should become so in the coming years. It will also be interesting to see if any aspects of the EU Medical Devices Regulation are reflected in the new UK legislation.

2.7 What regulations apply to artificial intelligence/machine learning powered digital health devices or software solutions and their approval for clinical use?

See question 2.6 above.

3 Digital Health Technologies

3.1 What are the core legal or 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, healthcare provider (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**
 - No particular issues.

3.2 What are the key issues for digital platform providers?

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, 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.

4 Data Use

4.1 What are the key legal or regulatory issues to consider for use of personal data?

- 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.
- 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 (e.g. step counts, sporting performance, etc.).
- Identifying the appropriate legal basis for processing data and obtaining any necessary consent.
- Carrying out a Data Protection Impact Assessment (DPIA), if required (as is likely) 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.
- Ensuring that any overlapping requirements related to rules on patient confidentiality are met.

4.2 How do such considerations change depending on the nature of the entities 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.

4.3 Which key regulatory requirements apply?

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 (**PECR**) 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 misuse of private information (**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 2024.

4.4 Do the regulations define the scope of 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 question 4.3 above, there are overlapping restrictions under contract, soft law and confidentiality/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 What are the key contractual considerations?

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 preapproved 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).

4.6 What are the key legal issues in your jurisdiction with securing comprehensive rights to data that is used or collected?

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).

4.7 How are issues with 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 UK’s data protection regulator, 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.

4.8 What are data-usage legal or regulatory issues that are unique to generative AI companies and how are those issues being addressed in your jurisdiction?

There are no data protection issues that are strictly unique to generative AI companies. The key issues with generative AI in the health sector are:

- ensuring that the use of generative AI to prepare any documentation for use with a patient does not lead to inaccurate processing – there must not be use that could lead to inaccuracies that would lead to any risk to a patient; and
- there must not be any breach of patient confidentiality in using generative AI – this means that a generative AI provider must not be given the ability to access personal data of third parties.

5 Data Sharing

5.1 What are the key issues to consider when sharing personal data?

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 do such considerations change depending on the nature of the entities 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.

5.3 Which key regulatory requirements apply when it comes to sharing data?

The preceding answers, in particular for questions 4.1, 4.3, 4.5, 5.1 and 5.2, have covered the key regulatory requirements applicable to the sharing of personal data in a digital health context.

5.4 Are there any governmental initiatives to establish standards for creating, maintaining and sharing healthcare data in your jurisdiction?

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

- NHS Digital, which currently has the 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. This is a role being subsumed by NHS England in early 2024.
- The Health Research Authority's Confidentiality Advisory Group (CAG) 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 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.

6 Intellectual Property

6.1 What is the scope of patent protection for digital health technologies?

Monopoly patent protection is available for novel, non-obvious products or processes which have industrial application. Fees are payable on application and renewal. Protection lasts 20 years from the date of application once the patent is granted (see UK Patents Act 1977).

6.2 What is the scope of copyright protection for digital health technologies?

The right to prevent copying, dealing in copies, issuance of copies to the public, performance, broadcast or adaptation for (relevant works only):

- Literary, musical, artistic works (including software) – life of author plus 70 years.
- Published sound recordings – 70 years from date of publishing.
- Broadcasts – 50 years from date of broadcast.

Copyright (generally) arises on creation and fixation of the work, with no requirement for registration. (See UK Copyright, Designs and Patents Act 1988 (CDPA).)

6.3 What is the scope of trade secret protection for digital health technologies?

Common law of confidence protects trade secrets. It 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. However, the common law of confidence provides stronger and more comprehensive protection.

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. The institution will typically seek to license the technology either to existing businesses or via the creation of a spin-out company to commercialise the technology.

There are no specific laws governing academic technology transfer.

6.5 What is the scope of intellectual property protection for software as a medical device?

Software is only patentable in the UK to the extent that it meets the requirements in the UK Patents Act 1977. These requirements are stringent and difficult to meet for software. Generally, however, software will be protected as a literary work under the CDPA (see 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?

Following the decision in *Stephen L. Thaler v The Comptroller-General of Patents, Designs And Trade Marks* [2021] EWCA 1374, an AI device cannot be named as an inventor of a patent in the UK. In October 2021, the UKIPO issued a public consultation on whether the Patents Act 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 which 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 are the core rules or laws related to government-funded inventions in your jurisdiction?

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

7 Commercial Agreements

7.1 What 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, so the joint owner might find themselves in an invidious situation if complete clarity is set out regarding the permitted uses a joint owner may have over the IP.

There may be better ways of approaching this – have ownership following the ownership of background on which the improvement is made or assign it in accordance with predetermined fields of use. Royalty payments and licences to background technology should also be provided for.

7.2 What 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 the norm.

7.3 What 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 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 may be an issue, along with rules and regulations governing generative AI itself, which are rapidly evolving and very region-dependent.

8 Artificial Intelligence and Machine Learning

8.1 What is the role of machine learning in digital health?

The statistical and pattern recognition capabilities of machine learning have a wide range of possible applications in the digital health context. These encompass activities which are trivial for any human to complete, but challenging for traditional computer systems (e.g. converting handwritten medical records into text) and those which require many years of human expertise (e.g. detecting breast cancer in mammograms). Their use also covers the full range of potential medical purposes from diagnosis, prevention, monitoring, prediction and prognosis of disease to its treatment and alleviation. Applications currently receiving particular attention are the use of pattern recognition techniques to detect abnormalities in medical imaging data. Olfactory AI is also emerging as a new potential diagnostic technique for certain diseases.

However, any digital health problem which involves the identification of signals in a noisy environment is potentially susceptible to the use of machine learning.

Machine learning can also be applied to the manner in which digital health services are delivered. Natural language processing can, for example, be used to facilitate human interaction with systems which are themselves based on machine learning techniques. Potential applications include “chat bots” combined with expert diagnostic systems to replicate a doctor’s consultation. Current systems are limited to diagnosing specific conditions in tightly controlled situations. Future systems will generalise this approach to broader diagnostic platforms with general application. Recent advances in language models and generative AI will open new possibilities for synthesising and communicating information in a healthcare setting.

8.2 How is training data licensed?

Under English law there is no single property right which applies to data *per se* and there is a general reluctance to treat information as a form of property. There may, however, be legal rights which may, depending on the nature/source of the data, be used to control access to, use and disclosure of training data. These include rights in confidential information along with IP rights in the data elements (e.g. copyright, where applicable) or in an aggregation of data (e.g. copyright in original databases or EU database rights).

Where these rights exist, they can form the subject matter for a contractual licence to training data, e.g. an IP licence and/or knowhow licence. The English courts have also recognised that it is possible to impose contractual restrictions on access to, use and disclosure of data even where that data is not protected by other rights. Training data can therefore also be licensed on a purely contractual basis under English law. The possibility of granting a purely contractual licence does not, however, give rise to some general right of “ownership” in the data being licensed.

Unless they refer to intellectual property rights in the data, reference to “ownership” of data in licences may give rise to confusion as this term has no clear legal meaning under English law.

Well-drafted data licences will commonly focus on the rights and restrictions regarding access, use and disclosure of the data and will only refer to ownership in the context of intellectual property rights in the data. They will also address (often complex) issues relating to access, use and disclosure of derived data which is created by the licensee using the licensed data. Data provisions in AI service agreements should also consider the status of meta-data which may be generated through customer interactions with the system.

8.3 Who owns the intellectual property rights to algorithms that are improved by machine learning 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 which 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 machine learning 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 machine learning 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 machine learning 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.

8.4 What commercial considerations apply to licensing data for use in machine learning?

Many machine learning projects often involve collaboration between a party with expertise in deploying machine learning and another party with access to the data required to train a machine learning system to solve a particular problem. Common commercial issues which 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 which 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 which 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 intellectual property 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 which is used to provide the service, or potentially to develop new AI models for use in a different context.

Customers may resist contractual terms which 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.

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 GDPR might create joint and several liability between partnering organisations if GDPR noncompliance 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, Scottish 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 post-Brexit, at least in the short term.

9.3 What are best practices to minimise liability risks posed by the use of 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 expert clinicians who can overrule them if they propose a potentially harmful path, thereby shifting all responsibility to the clinician or their place of work.

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 machine learning practice for medical device development.

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 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, and these regulations can vary from jurisdiction to jurisdiction – no broad-brush approach will be applicable. It is also a fast-moving market and keeping up with the changes in regulation is 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, MDR and WEEE.
- Consider competition – are they first, second or third to market?
- Consider patent protection – has this been secured where applicable and have they taken steps to protect and exploit unregistrable IP, such as trade secrets?
- Do they own all necessary IP?
- Do they have good supply and service contracts in place, and secure sources of hardware?

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 aforementioned reform plans in the field of medical device regulation indicate that the regulatory environment is undergoing significant change to "catch up".

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* (**ABHI**) plays a key

role in representing the industry to stakeholders, such as the Government, NHS and regulators.

Lobbying in the UK is less formalised, although ensuring that the particular digital health solutions meet certain criteria such as the NICE Evidence standards framework for digital health technologies would improve the likelihood of widespread adoption.

10.6 Are patients who utilise digital health solutions reimbursed by the government or private insurers in your jurisdiction? If so, does a digital health solution provider need to comply with any formal certification, registration or other requirements in order to be reimbursed?

This would depend on the product in question. From an England perspective, while there may not yet be specific publicly funded provision of general health apps *per se* direct to patients, the provision of, e.g. telemedicine may, under certain circumstances, be funded via the NHS. This would be an area to keep a close watch on since the recent launch of the NICE Office for Digital Health, which intends to, amongst other things, work with strategic partners to improve digital health approval pathways and reimbursement policy.

10.7 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 trend to watch in 2024 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.

Acknowledgment

The authors would like to thank Max Gross for his invaluable assistance in the updating of this chapter. Max is a trainee solicitor at Bird & Bird LLP, based in London.



Sally Shorthose is a Partner in the Life Sciences and Intellectual Property Group at Bird & Bird LLP, based in London and Dublin, and is the joint head of the International Life Sciences Regulatory Group. Before her return to private practice in 2001, she had spent 11 years working in-house in senior roles in the Life Sciences industry, including several years as Legal Director of the Novartis Group in the UK. She now specialises in transactional IP work and life sciences regulatory and commercial work and regularly undertakes due diligence and freedom-to-operate projects. She is the editor of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023, and is a regular speaker internationally on all types of IP and regulatory issues. She has spent much of the last three years leading the Brexit advisory team at Bird & Bird.

Solicitor – England & Wales, 1988.

Solicitor – Ireland, 2017.

Bird & Bird LLP

12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7982 6540

Email: sally.shorthose@twobirds.com

LinkedIn: www.linkedin.com/in/sally-shorthose-271833



Toby Bond is a Partner in Bird & Bird's Intellectual Property Group, based in London. Much of his work focuses on helping clients navigate issues relating to the protection and commercialisation of data as they take advantage of the power of big data analytics and AI. He has a particular interest in the wider intellectual property issues arising from the development and deployment of AI systems. Toby also advises clients on medical devices legislation and his broader experience covers CE marking, EU batteries legislation, REACH/CLP, RoHS, WEEE and Electromagnetic Compatibility, with a particular focus on emerging technologies including IoT and AI.

Bird & Bird LLP

12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6718

Email: toby.bond@twobirds.com

LinkedIn: www.linkedin.com/in/toby-bond-49a2112b



Emma Drake is a Legal Director in Bird & Bird's Privacy and Data Protection Group. She works with a variety of healthcare and life science clients, from traditional pharmaceutical companies to health informatics providers to new entrants handling personal data in the context of wellness apps or new technology. She has helped clients on diverse topics spanning application of research exemptions, anonymisation, assessing the compliance of new medical technologies, patient support programmes and the processing of data for pharmaceutical regulations such as pharmacovigilance or restrictions under the ABPI code.

Bird & Bird LLP

12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7415 6728

Email: emma.drake@twobirds.com

LinkedIn: www.linkedin.com/in/emma-drake-43a3573b



Pieter Erasmus is a Senior Associate in the Intellectual Property 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 advice in relation to a broad range of matters in these fields, including pharmaceuticals, medical devices, general healthcare, clinical trials, marketing and advertising of health products, etc. Pieter's experience further includes corporate and commercial work, including transactional work and the drafting of a wide range of general and bespoke commercial agreements in the life sciences and healthcare sectors. He is a co-author of the Kluwer Law publication, the *EU and UK Guide to Pharmaceutical Regulatory Law*, the latest edition of which was released at the beginning of 2023. Before joining Bird & Bird in 2019, he spent over six years working at the Johannesburg offices of Africa's largest law firm.

Bird & Bird LLP

12 New Fetter Lane
London, EC4A 1JP
United Kingdom

Tel: +44 20 7905 6217

Email: pieter.erasmus@twobirds.com

LinkedIn: www.linkedin.com/in/pieter-miguel-erasmus

Recognised across the major global directories as a top-tier firm for life sciences and healthcare expertise, Bird & Bird is the go-to international law firm for over 50% of the world's largest pharmaceutical and biotechnology companies. We guide our clients through every aspect of the life cycle of innovative healthcare products and services, including incorporation, development and financing, exploitation of IP and portfolio management, regulatory and contractual issues, clinical trials and securing marketing authorisation.

www.twobirds.com

Bird & Bird

International Comparative Legal Guides

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

Digital Health 2024 features one introductory chapter, two expert analysis chapters and 22 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