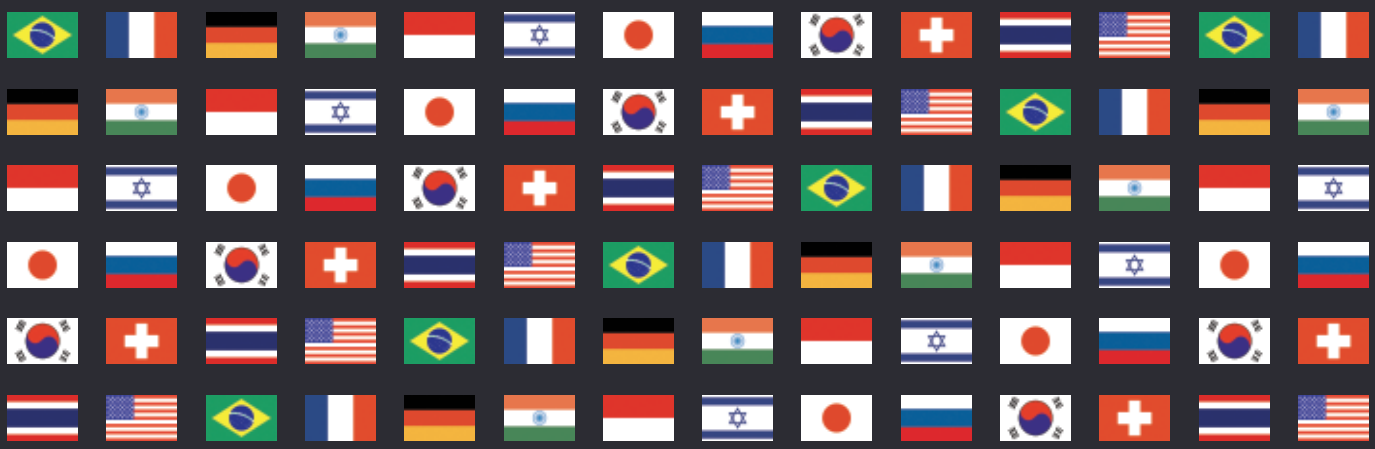
Digital Health
2021



LEXOLOGY®
Getting The Deal Through

© Law Business Research 2021

United Kingdom

Robbie McLaren, Frances Stocks Allen, Oliver Mobasser, Sara Patel and Mihail Krepchev

Latham & Watkins LLP

MARKET OVERVIEW AND TRANSACTIONAL ISSUES

Key market players and innovations

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

The UK has an active digital health market comprising both the private and public sectors, as well as investors. The National Health Service (NHS) is the dominant buyer in the UK's £5 billion healthcare IT and digital market, with the private sector only accounting for spend of approximately £250 million annually. NHS trusts can also currently apply for a share of £50 million in grant funding to scale up digital pathology, radiology and AI capabilities in England.

The digital health market in the UK focuses predominantly on:

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

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

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

- Babylon;
- Benevolent AI;
- Congenica;
- Vernalis;
- DoctorLink;
- Cera;
- Huma; and
- LumiraDx.

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

Investment climate

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

The covid-19 pandemic has further heightened the positive and dynamic investment climate for digital health technologies in the UK. In particular, the pandemic has highlighted the need for resilience in healthcare systems, including through digital health solutions. As a result, the pandemic has significantly accelerated uptake of digital health solutions in the United Kingdom and related investment opportunities. According to the Healthcare Investments and Exits Annual Report 2020 conducted by Silicon Valley Bank, investment in digital health technologies skyrocketed in 2020. The UK was at the centre of this momentum, accounting for 30 per cent of deals in Europe by volume and value as of Q3 2020.

As a result of the pandemic, virtual health has become a new frontier in care delivery. The pandemic is challenging structural barriers that had previously slowed investment in digital health innovations. AI applications can help to meet the challenge of scaling up labour requirements to meet new demands on resources.

Health agencies and tech companies are also striking partnerships at increasing speed. For example, the NHS is reportedly working with companies such as Amazon, Microsoft and Palantir to create data models to optimise the allocation of ventilators, hospital beds and staff.

Recent deals

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

The most notable recent deals in the UK include:

- In March 2020, Novartis Pharmaceuticals UK Limited and Cievert Limited, a UK provider of innovative digital healthcare solutions, announced a digital innovation partnership to support patient care in rheumatology and dermatology.
- In December 2020, London-based virtual care company HealthHero acquired digital triage platform Doctorlink.
- In November 2020, Congenica, a digital health company enabling rapid and accurate analysis of complex genomic data, received £39 million in Series C funding from various investors, including Cambridge Innovation Capital, Downing Ventures, IDO Investments, Legal & General, Parkwalk Advisors, Puhua Capital, Tencent Holdings and Xeraya Capital.
- In November 2020, Medica, a UK tele-radiology company, announced the acquisition of Global Diagnostics Ireland, the market leader for tele-radiology services in Ireland, for an initial cash consideration of €16 million from private Irish healthcare group, Centric Health.
- In June 2020, online consultation provider Livi announced three NHS partnerships to expand its patient reach in the Midlands and North of England to 1 million.
- In January 2020, Babylon Health, the company behind the GP at Hand phone app, announced a partnership with a UK hospital in a bid to create the world's first integrated digital health system serving an entire city.

© Law Business Research 2021

Due diligence

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

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

- Intellectual property rights: a significant proportion of the value in digital health businesses can be attributed to the intellectual property rights owned or licensed by the company. Accordingly, it is critical to understand whether any such intellectual property rights have been infringed and to assess the validity and strength of any material registered intellectual property rights, such as patents and trademarks. If employees and consultants have developed material intellectual property rights, diligence should be undertaken to ensure that the ownership of those intellectual property rights has vested in or been assigned to the company. If critical intellectual property rights have been in-licensed from a third party, it is also important to ascertain that the terms of that licence are sufficiently flexible to permit the activities planned by the company in its business plan.
- Data: it is highly likely that the ability to use, analyse and process data will be a key part of any digital health company's business plan. Thus, diligence should focus on ensuring that the company processes data in a manner that complies with applicable data protection regimes while also facilitating future growth. The consequences of non-compliance can be business threatening, given the scale of potential enforcement activities.
- Commercial agreements: it is important to confirm the existence and terms of formal written agreements with key customers and suppliers. Such a review can help ensure confidence in future revenue, especially by clarifying whether any such agreements would be impacted by the investment (eg, change of control triggers).
- Regulatory authorisations: it is important to verify that the business holds all necessary regulatory authorisations relevant to the products and services offered.
- Leadership team: many digital health ventures are founder-led businesses, which heavily rely on their leadership teams. Accordingly, it is important to review the terms of key leadership employment and bonus arrangements to ensure they are appropriately incentivised for the long term.

Financing and government support

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

Venture capital funding in the digital health sector has increased significantly in recent years, with the majority of investment appearing to come from private investment firms. However, public financing through IPOs is also on the rise; in fact, the digital health space saw a number of significant IPOs in 2020. Digital health companies seeking private investment in the UK will likely undergo a number of funding rounds from seed and start-up capital through to targeted private investment from venture capital firms as they scale up, if they have not done so already. This investment may be structured through different classes of shares with different voting and economic rights or convertible instruments, or both, potentially alongside additional bank debt.

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

- In September 2020, the government unveiled a £32 million fund for various health technology research projects (including certain AI and robotics-based initiatives).
- In April 2020, the government announced the creation of the Future Fund, which invests up to £5 million into smaller private UK companies. A number of digital and other healthcare companies have taken advantage of the scheme.
- In 2019, the government announced the creation of the £250 million National AI lab – which provides a platform for NHS to partner with academics and technology companies to use AI to improve diagnostics and screening. The government has also pledged financial support for a variety of other digital health initiatives in conjunction with the NHS and other research bodies.

LEGAL AND REGULATORY FRAMEWORK

Legislation

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

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

- Digital health products (including software, apps, wearables, AI and algorithms) that are classified as medical devices are regulated under the Medical Devices Regulations 2002 (the MDRs), as amended (implementing EU Council Directive 93/42/EEC on medical devices,EU Council Directive 90/385/EEC on active implantable medical devices and EU Directive 98/79/EC on ***in vitro*** diagnostic medical devices). Broadly, a product falls within the remit of the MDRs if: (1) its intended purpose is to fulfil a medical function, including diagnosis, prevention, monitoring or treatment of disease; and (2) it does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means.
- The provision of health or social care (including by remote means) in England is primarily governed by the Health and Social Care Act 2008. Similar legislation covers Wales, Scotland and Northern Ireland. There is currently no specific legislation governing the provision of telemedicine services. The Electronic Commerce (EC Directive) Regulations 2002 (the eCommerce Regulations) may also apply to the provision of telemedicine services.
- The processing of personal data in relation to digital health offerings is governed by (1) the Data Protection Act 2018, which has been amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 to make certain changes necessary as a result of Brexit; and (2) the UK General Data Protection Regulation, as defined in the Data Protection Act 2018 (the UK GDPR), which effectively mirrors the provisions of the EU General Data Protection Regulation in UK law. Both the European and the UK data protection regimes have extra-territorial aspects. This means that organisations in the UK may be subject to the GDPR, as well as UK data protection laws, if they offer goods or services to, or monitor the behaviour of, individuals in the EEA.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 may also apply to digital health companies that market to their users by electronic means, or use cookies or similar technologies that track information about people accessing a website or other electronic service such as a digital health mobile application.
- General consumer legislation may also apply to digital health products and services, and particularly to apps and digital content. Such legislation includes the Consumer Protection Act 1987, the General Product Safety Regulations 2005, the Consumer Protection from Unfair Trading Regulations 2008, the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 and the Consumer Rights Act 2015.

© Law Business Research 2021

Regulatory and enforcement bodies

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

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

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

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

- England: the Care Quality Commission (CQC);
- Scotland: Health Improvement Scotland (HIS);
- Wales: Health Inspectorate Wales (HIW); and
- Northern Ireland: the Regulation and Quality Improvement Authority (RQIA).

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

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

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

Licensing and authorisation

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

New rules following the end of the Brexit transitional period mean that all medical devices must be registered with the MHRA before being placed on the market in Great Britain. A grace period ranging from four to 12 months may apply, depending on the risk classification of the device. Separate timelines and rules apply to Northern Ireland, which falls under the EU regulatory regime.

In general, a medical device must undergo a conformity assessment that results in it being affixed with a 'CE' mark before it can be placed on the UK market. For Class I devices, this assessment can generally be conducted through a self-assessment procedure. However, for higher-risk devices, in Class IIa, IIb or III, the conformity assessment must involve a notified body. Under the current classification rules, many software devices are classified as Class I. However, the upcoming EU regulations will have the effect of 'up-classifying' most software medical devices, meaning that self-assessment will no longer be an option for manufacturers. It remains to be seen whether the UK will implement similar changes to the classification rules. As a result of the UK's departure from the EU, the CE mark will be replaced by a new 'UKCA' mark, subject to an 18-month grace period. Manufacturers can use the UKCA mark on a voluntary basis until 30 June 2023. However, from 1 July 2023, a UKCA mark will be required to place a medical device on the Great Britain market.

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

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

Soft law and guidance

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

The MHRA has published detailed guidance on standalone software, including apps. This guidance provides helpful clarity on when software will be regulated as a medical device.

The NHS has published 'A guide to good practice for digital and data-driven health technologies', which aims to help innovators understand what NHS considers when purchasing digital and data-driven technology. This way, principles of good practice can be built into the strategy and product development 'by design'.

The National Institute for Health and Care Excellence has published Evidence Standards Framework For Digital Health Technologies, which describes the standards for digital health technologies to demonstrate their value in the UK healthcare system.

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

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

The ICO has also published various guidances on the processing of personal data in the context of healthcare and social care.

Liability regimes

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

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

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

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

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

The retained Rome I Regulation (Regulation (EC) No 593/2008) and Rome II Regulation (Regulation (EC) No 864/2007), as amended, apply to: (1) contracts that conclude after the end of the Brexit transition period; and (2) events giving rise to damage that occur after the end of the Brexit transition period. In such instances, these regulations determine applicable law in relation to contractual or non-contractual obligations. Generally, this means that contractual disputes will be governed by the law chosen by the parties or, in the absence of choice, as determined in the principles in the Rome I Regulation. Non-contractual disputes will generally be governed by the law of the country in which the damage occurs.

© Law Business Research 2021

On an EU level, the European Parliament has passed a resolution on the civil liability regime for artificial intelligence. This resolution recommended that existing liability regimes be adjusted to accommodate specific new and future-oriented ideas. Under the proposed regulation, AI systems that present a high risk to the general public would be subject to a strict liability regime, whereas those deemed to present a lower risk would have fault-based liability. The extent to which the UK will align with this proposed approach is not yet clear.

DATA PROTECTION AND MANAGEMENT

Definition of `health data'

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

Health data

Under the UK General Date Protection Rules (GDPR), 'data concerning health' means personal data related to the physical or mental health of a natural person. This definition includes the provision of healthcare services, which reveal information about a person's health status. The Information Commissioner's Office (ICO) has confirmed that 'data concerning health' can also relate to healthy individuals, and includes data from medical devices and fitness trackers (eg, the number of steps taken by the user or athletic performance). Data such as appointment details, reminders and invoices may also constitute health data if it reveals or could in combination with other data reveal information about a person's health through 'reasonable inference'.

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

Anonymous data

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

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

Data protection law

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

Data concerning health, genetic data and biometric data is among a list of 'special categories of personal data' under the UK GDPR. Such data can only be processed if one of a limited number of conditions are met, which are exhaustively set out in law. Those conditions most likely to be applicable to a digital health company may include one or more of the following:

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

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

The ICO recognises health data as 'some of the most sensitive personal data'. This assessment is likely to play a part in the regulator's analysis of a company's obligations, such as whether: (1) security measures applied to the data are appropriate in light of the potential risk to the rights and freedoms of natural persons; and (2) security incidents with respect to personal data are notifiable to the ICO and to data subjects.

Anonymised health data

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

Anonymised data falls outside of the UK data protection regime's scope, as it no longer constitutes 'personal data'. However, controllers of anonymised data should keep in mind that the act of anonymising could in itself constitute data processing within the meaning of the UK GDPR.

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

© Law Business Research 2021

Enforcement

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

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

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

The ICO's Assurance team carries out audits across a broad range of health organisations. Breaches found during the audit can lead to ICO investigations, which in turn may lead to the ICO mandating remedial actions by the breaching party. One notable ICO enforcement against digital healthcare technologies concerned TPP's SystmOne, the second-most widely used GP electronic patient record system in England. In 2017, the ICO raised concerns around the software's 'enhanced sharing' function. This function allowed authorised users at hospitals and other care organisations to access, and add to, a patient records. Following the ICO investigation, new controls were implemented in 2018 giving GP data controllers more control in how they share patient records for the purposes of patient care.

The ICO relaxed advice and enforcement during the covid-19 pandemic in the public interest. For example, the ICO began allowing clinicians to use consumer video conferencing solutions at the same time that NHSX, a government unit responsible for leading IT policy across NHS, began allowing healthcare professionals to use messaging tools such as Skype, WhatsApp and FaceTime in the course of executing their duties.

Cybersecurity

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

The EU Directive on security of network and information systems (the NIS Directive), which aims to ensure the security of critical IT systems in central sectors of the economy, was implemented in the UK by the NIS Regulations 2018 (the NIS Regulations). The NIS Regulations' requirements for relevant entities include to:

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

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

- providers of non-primary NHS healthcare in England;
- local health boards and NHS trusts in Wales;
- the 14 territorial health boards and four special NHS boards in Scotland; and
- health and social care trusts in Northern Ireland (paragraph 8, Schedule 2, NIS Regulations 2018).

However, this scope is set to widen with the entry into force of the revised NIS Directive (the NIS 2). In its draft proposal released on 16 December 2020, the European Commission recommended expanding the scope of NIS 2 to include entities that manufacture pharmaceutical products (including vaccines) or critical medical devices. The UK is not required to implement NIS 2 post-Brexit, and it is unclear if steps will be taken to maintain harmonisation. However, if the UK were to enact legislation to align with NIS 2, more manufacturers and companies operating in the life sciences space in the UK would become subject to the regime's requirements.

UK entities may also be subject to the NIS Directive extraterritorially. After Brexit, if a digital service provider is no longer established in the EU but offers digital services into the EU, it will be subject to the obligation to designate a representative in an EU member state in accordance with article 18(2) of the NIS Directive.

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

Best practices and practical tips

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

Companies engaged in the digital health space should bear in mind the concepts of 'privacy by design' and 'privacy by default', which are built into the UK data protection regime and also the ICO's stated priority on records management in the healthcare space.

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

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

In 2020, we saw a continuation of the trend of ransomware attacks increasingly targeting companies with large amounts of electronic health records or profiles. Defending against and responding to a ransomware incident, particularly one with multi-jurisdictional impact, is complex and requires consideration of a number of regulatory areas, including data protection, cybersecurity, law enforcement, industry-specific regulation

© Law Business Research 2021

and sanctions (in relation to ransom payments). The UK National Cyber Security Centre (NCSC) has prepared a guidance note on mitigating such attacks. The NCSC recommends using layers of defence across an organisation in what is known as a 'defence-in-depth' approach, which includes:

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

INTELLECTUAL PROPERTY

Patentability and inventorship

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

Digital health products that comprise mechanical, chemical or electrical components may, if novel and inventive, be patentable in the UK. The processes associated with using a device, and any inventions generated by the device, may also be patentable. However, section 1(2) of the Patents Act 1977 (Patents Act) expressly excludes 'a program for a computer' (ie, software, from patentable inventions). However, software that makes a 'technical contribution' to the state of the art is an exception (*Symbian Ltd v Comptroller General of Patents* (2008) EWCA Civ 1066). For example, if an AI programme learns to identify and classify tumours from diagnostic imagery, this has a technical effect on a process carried on outside the computer (ie, diagnosis of a pathology) and therefore may be patentable (*Re AT&T Knowledge Ventures* (2009) EWHC 343 (Pat)). No official guidance or case law directly relating to the patentability of AI in the UK currently exists, and the UK Intellectual Property Office (IPO) continues to examine patent applications on a case-by-case basis.

When an invention is generated by an algorithm or other machine, inventorship should be carefully considered before applying for a patent. In *Stephen L Thaler v Comptroller-General of Patents, Designs and Trade Marks* (2020) EWHC 2412 (Pat), the court held that an inventor must be a natural person, and to be entitled to a patent, the owner of an inventing machine must be able to demonstrate on the basis of the Patents Act that they are entitled to the property rights in the invention, either as first creator of the property right (ie, an inventor or joint inventor) or by subsequent transfer of the property right (eg, by an enforceable term of any agreement entered into with the inventor before the making of the invention (including employee inventions) or as a successor in title to any of the above.

An invention will belong to the employer if it is made by an employee in the UK in the course of their employment duties (section 39(1)(a) and (b), Patents Act). The nature of an employee's 'duties' can evolve over time and is not limited to their job description. The definition can extend, for example, to a manager of business development charged with the task of identifying new products or to an employee that is otherwise employed to innovate on behalf of the employer (*LIFFE Administration & Management v Pinkava* (2007) RPC 30). Otherwise, the employee is the owner of an invention.

Patent prosecution

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

Patent prosecution in the UK commences with the filing of a national application directly with the IPO. Alternatively, if a European patent has already been granted for the technology, patent owners may seek a validation of the granted patent in the UK (article 2(2), European Patent Convention) or the UK national phase can be entered from a Patent Cooperation Treaty application, which is administered by the World Intellectual Property Organisation.

There are no special rules for digital health technologies.

Other IP rights

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

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

Copyright is the main source of protection for software under the Copyright, Designs and Patents Act 1988 (CRDPA). There is no register for copyright in the UK, so (to the extent that it is challenged) ownership must be proved by way of documentation. Retaining correspondence, agreements and any other records pertaining to the creation of copyright-protected works is important for this reason.

Know-how and trade secrets must be protected through adoption of robust confidentiality practices, to avoid the disclosure of the relevant information or data to a third party.

Design rights may also arise, for example, in the design of a user interface (if any). Design rights in the UK can be protected in the form of unregistered rights, for up to 15 years after creation. Registering design rights under the Registered Designs Act 1949 and obtaining protection for up to 25 years is also possible.

Databases may be protected as works of copyright under the CRDPA and also under the *sui generis* right in the Copyright and Rights in Databases Regulation 1997.

Trademarks should be registered with the IPO. They are subject to registration fees and, every 10 years, renewal fees.

Licensing

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

The practical considerations for licensing intellectual property rights in digital health technologies are similar to those in any other technical field. Clearly defining the scope of the licence granted, any reserved rights, the duration of the licence and any exclusivity is a key step. When know-how is included in the scope of the licence, non-use and disclosure restrictions must be considered and documented. Clearly defining which party will have the first right to prosecute, maintain and enforce is also important, as is any back-up right of the other party. In addition, licences of patents, trademarks and exclusive licences of copyright must be in writing and signed by or on behalf of all the parties to be effective.

Registering patent or trademark licences is not necessary, but is prudent to do because this allows the licensee to confidently assert their rights against subsequent rights holders and users. For example, an exclusive patent licensee may directly sue a third party for infringement of the relevant patent(s) (section 67, Patents Act). A licence must be registered within six months of the date of the agreement to enable the licensee to recover costs from a successful patent or trademark infringement proceeding. Copyright licences cannot be registered.

© Law Business Research 2021

Enforcement

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

Intellectual property rights in the UK, including those in digital health technologies, are generally enforced through civil proceedings. Proceedings may be filed either in the courts or through the IPO, or in some cases both (eg, patent enforcement actions), depending on the type of claim. Specialist IP courts include the Patents Court of England and Wales (a specialist court within the Chancery Division of the High Court), which is suitable for complex, high-value actions. The Intellectual Property Enterprise Court (IPEC), which can hear any type of IP claim, will hear less complex cases with a value under £500,000. Note that UK national patents cannot be enforced in the Unified Patent Court following the UK's withdrawal in July 2020.

A notable recent enforcement case involving digital health technologies is *Technomed Ltd v luecrest Health Screening Ltd* (2017) EWHC 2142 (Ch), under which the High Court upheld a claim for infringement of the *sui generis* database right and copyright in an internet-based electrocardiogram (ECG) analysis and reporting system. This consisted of a platform that enabled a qualified cardiologist to remotely analyse ECG readings and select a classification from a range of options corresponding to each ECG variable in a database. The database outputted an extensible mark-up language file with a standardised format that was then used to generate a report for distribution to the patient or practitioner. The first defendant was found to have infringed the claimants' database right and copyright when it switched services to a competitor (the second defendant) and, for the next two years, copied certain explanatory documents from the claimants' ECG system and provided these to the competitor for use in delivering the competing services.

ADVERTISING, MARKETING AND E-COMMERCE

Advertising and marketing

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

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

Digital health products (including software, apps, wearables, AI and algorithms) that consist of medical devices must also be marketed and promoted in compliance with the Medical Devices Regulations 2002, which prohibit marketing of non-CE marked medical devices.

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

- The UK Code of Non-broadcast Advertising and Direct & Promotional Marketing, enforced by the Advertising Standards Authority (the ASA), which applies to all advertisers, agencies and media;
- The UK Code of Broadcast Advertising, enforced by the ASA, which applies to all advertisements on radio and television services licensed by the Office of Communications;
- The Association of British Healthcare Industries (ABHI) Code of Practice, including the ABHI Guidelines on Advertisements & Promotions addressed solely or primarily to healthcare professionals; and
- The MedTech Europe Code of Ethical Business Practice.

Companies that process personal data for marketing purposes must also comply with the Data Protection Act 2018, including the UK GDPR. The Privacy and Electronic Communication Regulations may also apply to digital marketing.

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

e-Commerce

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

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

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

PAYMENT AND REIMBURSEMENT

Coverage

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

The NHS funds the majority of digital health products and services provided to patients in the UK. A smaller but growing private healthcare sector where patients fund for themselves or through private insurance also exists.

There are a number of routes for products to be made available for reimbursement by the NHS, including selling directly to trusts or primary care organisations or procurement through the NHS supply chain or public tenders. In addition, products, including digital health products, can undergo a technology appraisal from the National Institute for Health and Care Excellence (NICE). The NHS is legally obliged to fund and resource treatments recommended by NICE's technology appraisals.

© Law Business Research 2021

NHS Digital (a division of the NHS) is the lead national delivery partner for improving the use of data and digital technologies in the health and care system. The NHS has published 'A guide to good practice for digital and data-driven health technologies', which is designed to help innovators understand what the NHS is looking for when it buys digital and data-driven technology, so that principles of good practice can be built into the strategy and product development 'by design'. NICE has also published Evidence Standards Framework For Digital Health Technologies, which describes the standards for digital health technologies to demonstrate their value in the UK health and care system.

The NHS recently launched HealthTech Connect to assist in identifying and supporting health technologies (including devices, diagnostics and digital) as they move from inception to adoption in the UK health and care system.

UPDATES AND TRENDS

Recent developments

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

The regulatory framework of medical devices in the EU is due to be overhauled with the introduction of two new regulations on 26 May 2021 and 26 May 2022 governing medical devices and in vitro diagnostic medical devices, respectively. These two new regulations had been due to be mirrored in UK law. However, this 'mirroring' legislation was revoked prior to the end of the Brexit transitional period.

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

The Medicines and Medical Devices Act, which received royal assent on 11 February 2021, introduces delegated powers in favour of the Secretary of State or an 'appropriate authority' to amend or supplement regulations in the area of medical devices. The MHRA has noted in its guidance on regulating medical devices that it is 'developing a robust, world-leading regulatory regime for medical devices that prioritises patient safety. We will take into consideration international standards and global harmonisation in the development of our future system', meaning the UK may choose in future to align with the new EU regulations or may choose to retain regulatory flexibility.

In January 2020, NHSX AI Lab convened a roundtable of 12 regulators, including the MHRA, National Institute for Health and Care Excellence (NICE), Health research Authority (HRA) and the Care Quality Commission (CQC), to discuss the roles of the MHRA in regulating AI systems; the HRA in overseeing research to generate evidence; NICE in assessing product value and CQC in ensuring providers are following best practice, and to oversee development of a regulatory sandbox. It was agreed that regulations covering use of AI in digital health technologies will need to be put in place as soon as possible. As such, companies should continue to monitor developments in this rapidly evolving area as further guidance from regulatory authorities is expected.

In October 2020, NHSX, the technology and digital unit of the UK's NHS, published its Digital Technology Assessment Criteria, which sets the baseline criteria for the assessment of digital health and social care technologies for use by the NHS. It contains five core areas that developers should adhere to, being clinical safety, data protection, technical assurance, interoperability and usability and accessibility.

Coronavirus

26 What emergency legislation, relief programmes and other initiatives specific to your practice area has your state implemented to address the pandemic? Have any existing government programs, laws or regulations been amended to address these concerns? What best practices are advisable for clients?

To assist with the rapid adoption of digital health technology and other medical devices during the covid-19 pandemic, the MHRA has clarified the scope of the existing exemptions to certain requirements of medical devices legislation, including CE marking. Manufacturers of medical devices (including apps and other software) can apply directly to the MHRA for fast-track approval for such products, provided they fulfil certain criteria. Specific guidance has been published in relation to software and apps, which clarifies the route and requirements for claiming this exemption for software or apps that have either been specifically developed in response to covid-19 or developed and CE marked for a different purpose, but which have a role in responding to the covid-19 pandemic. Such authorisation or derogation would be granted under Regulations 12(5),26(3) and 39(2) of the Medical Devices Regulations 2002, which already provides for derogations in the interests of public health.

In addition, the Information Commissioner's Office has adopted a pragmatic approach to data protection enforcement during the covid-19 pandemic, noting that it will take into account the compelling public interest in the current health emergency. Specific guidance has also been issued for health and social care organisations. NHSX has also issued guidance relating to the use of video conferencing and consultation tools and the GMC's guidance on remote consultations will continue to apply.

© Law Business Research 2021

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

an LBR business

© Law Business Research 2021