International
Comparative
Legal Guides

Practical cross-border insights into digital health law

Digital Health

2023

Fourth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

ICLG.com

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Emerging Trends in the Global Regulation of Digital Health: Fragmented Frameworks Aiming to Catch up with Technological Advancement


Eveline Van Keymeulen


Elizabeth Richards


Nicole Liffrig Molife


Oliver Mobasser

Latham & Watkins

Introduction/Overview

Technological advancements in the healthcare industry create an enormous opportunity to improve and transform healthcare delivery and access, reduce healthcare costs and advance public health as a whole. Digital health technologies have become more common, and are increasingly being used in new ways that are accessible to patients and providers alike. For example, these technologies have been used to impact how, where and when care is delivered to patients, such as through telehealth. They have also been used to expand patient access to clinical research opportunities through "decentralisation" of clinical trials, with remote monitoring of patients to capture health-related data at home. Advancements in digital health have also established new ways or mechanisms to document and transfer electronic health records and enable correspondence between providers. These technologies have improved the ability to predict or characterise sub-clinical signs of disease to assist providers in determining that their patients would benefit from earlier preventive care. Digital health technologies have also been used to promote general health and wellness, such as through mobile applications and wearables intended for everyday use. Consequently, digital health's applications are boundless and full of promise.

The explosion of these technologies, however, is tempered somewhat by the laws and regulations that were not developed with the advancements in digital health in mind. Governmental and regulatory authorities have thus had to grapple with balancing the strict application of their existing legal frameworks in a new world of digital health, while enabling continued advancement in the field. In this chapter, we discuss certain key legal constructs that digital health companies and investors must consider, and the emerging legal trends impacting applications of digital health in the United States ("US"), European Union ("EU") and United Kingdom ("UK").

Key Legal Constructs for Digital Health Companies

Medical device considerations

One of the key legal constructs that companies and investors in the digital health industry must consider is the framework applicable to medical devices across jurisdictions.

US

In the US, the Food and Drug Administration ("FDA") is the primary authority to regulate medical devices. The law defines a device to mean "an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or similar or related article, including any component, part, or accessory, which is" among other things, either "intended for use in the diagnosis of disease or other conditions or in the cure, mitigation, treatment, or prevention of disease" or "intended to affect the structure or any function of the body" and "does not achieve its primary intended purpose through chemical action" and is "not dependent on being metabolised to achieve that purpose".[1] Certain software functions that might otherwise fall within the scope of this broad definition are excluded by law from being regulated as a device. For example, in general, a software function intended for "maintaining or encouraging a healthy lifestyle and [that] is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition" will not be regulated as a device.[2]

With the exception of those software functions deemed to be shielded from the FDA's medical device oversight by statute as a matter of law, the law paints a broad brush; it sweeps many digital health technologies, including certain software – which may not traditionally be viewed as a "device" or "product" – within the FDA's reach. Because the medical device framework was established prior to the relatively recent advent of digital health technologies, it is not tailored to their intricacies and is often a poor fit. Indeed, the FDA and industry alike have recognised that the existing regulatory framework for medical devices can present a barrier to innovation and stifle or slow the potential for digital health technologies' use in improving public health.

To address this conundrum, the FDA has issued a variety of guidance documents and exercised flexibility in applying its regulatory scheme to this new class of technologies. For example, the FDA has issued guidance on software functions and mobile medical applications,[3] general wellness products[4] and clinical decision support software[5] in an effort to establish a clearer line between certain digital health technologies that are subject to FDA oversight and those that are not. In some cases, the FDA has applied a policy of enforcement discretion, noting that although the technology may technically constitute a medical device subject to FDA oversight, the FDA has declined to assert its medical device authority and requirements over such technologies. Consistent with its increased focus on digital health and the regulatory flexibilities these technologies require, in September 2020 the FDA announced the launch of its Digital Health Center of Excellence to "establish a comprehensive approach" to digital health technology to "set[] the stage for advancing and realizing the potential of digital health".[6]

The FDA has also engaged in a number of actions in recent years to address certain novel digital health technologies, including artificial intelligence and machine learning ("AI/ML")

in medical applications.[7] Specifically, the FDA has proposed the establishment of a new regulatory framework to enable a more flexible approach to regulating these technologies, which are designed to make real-time improvements after distribution and use. The FDA recognises that the existing regulatory framework, which was not constructed to account for the ever-changing nature of products using AI/ML technology, must be reworked to enable the technology's built-in ability to evolve, adapt and improve healthcare in the real world.

EU

Similarly, in the EU, regulatory authorities may consider digital health technologies to be regulated as devices, pursuant to Regulation (EU) 2017/745 on medical devices ("MDR") or Regulation (EU) 2017/746 on *in vitro* diagnostic medical devices ("IVDR"). The MDR and IVDR clarify that software that is intended by the manufacturer to be used for one of the medical purposes listed in these regulations will be classified as a medical device or *in vitro* diagnostic medical device, respectively. These regulations could therefore capture many digital health solutions, including software incorporating AI when intended for use for medical purposes. As such, to be placed on the EU market, these solutions must be compliant with general safety and performance requirements as a prerequisite for European conformity, or "CE" marking, without which medical devices, including *in vitro* diagnostic medical devices, cannot be marketed or sold in the EU. To guide manufacturers, the Medical Device Coordination Group has issued guidance on the qualification and classification of software under the MDR and IVDR,[8] and the Manual on borderline and classification in the EU regulatory framework for medical devices contains many examples related to qualification of software and mobile applications.[9]

Today, more than 25% of medicines assessed by the European Medicines Agency ("EMA") incorporate a medical device component, which increasingly include digital technologies (such as "digital pills"). In a recent guideline, the EMA addressed the challenges related to the development of these combination products that use emerging technologies by recommending that developers engage with the relevant medicines authorities and notified bodies in a timely manner, e.g., by requesting formal scientific advice, or through an Innovation Office.[10]

As related to AI, on April 21, 2021, the European Commission published a proposal for what may become the world's first regulatory framework on AI ("AI Act"). The proposed AI Act would apply to AI in all sectors, including the health sector. Under the proposed AI Act, most AI systems that are part of medical devices and *in vitro* diagnostic medical devices, or are themselves such products, would be classified as high risk and require a conformity assessment by a notified body (e.g., a device, such as a pacemaker, that uses an AI system to identify the user's normal cardiological parameters and thus monitor the proper functioning of the patient's heart). As most software-based medical devices and *in vitro* diagnostic medical devices are already subject to conformity assessment by MDR- or IVDR-notified bodies, there is a possibility they would have to undergo a second conformity assessment procedure under the proposed AI Act, which could lead to increased cost, resources, documentation and regulatory scrutiny. In addition, such a requirement could create additional constraints for those notified bodies designated under the MDR and IVDR, which are already experiencing enormous backlogs. Given the overlap between the medical device and AI frameworks, further clarification is necessary to ensure that the proposed AI Act advances innovation in the digital health space, rather than stifles it.

UK

As a result of Brexit, the MDR and IVDR do not apply in Great Britain, though they are applicable in Northern Ireland pursuant to the Northern Ireland Protocol. On June 26, 2022, the UK Medicines and Healthcare products Regulatory Agency ("MHRA") published its response to a 10-week consultation[11] on the future regulation of medical devices in the UK. The aims of the consultation included exploring amendments to the current Medical Devices Regulations 2002 with a view to creating an innovative framework for regulating software and AI as medical devices. The new regime was originally scheduled to come into force in July 2023, but has recently been postponed to July 2024. For the most part, the proposed changes in many of these areas align with the new EU regime under the MDR and IVDR.

On October 17, 2022, the MHRA published guidance on "Software and AI as a Medical Device Change Programme – Roadmap",[12] a programme aiming to reform the regulation of these technologies and ensure that the regulatory requirements for software and AI are clear and that patients are protected. The programme consists of proposals to make key reforms across the lifecycle of these products, including qualification, classification, pre- and post-market requirements and cybersecurity.

As regulators in the US, EU and UK continue to refine their approaches to digital health technologies, including when and how such technologies should be regulated as medical devices, the legal and regulatory frameworks are likely to shift. This changing landscape can present difficulties for companies in the digital health industry when assessing the regulatory burdens that may apply across the lifecycle of their products and services. Furthermore, despite regulators' attempts to adapt to technological innovation in a flexible manner, future advancements in digital health may continue to outpace the legal frameworks, with regulators seemingly playing a constant game of catch-up.

Telehealth considerations

Digital health technologies that pertain to the delivery and use of telehealth to deliver care require a thorough evaluation of another set of healthcare regulatory laws outside of the FDA and comparable medical device regulations globally.

US

No uniform federal law governs the delivery of telehealth services. Instead, telehealth is regulated at state level, and digital health companies need to evaluate a patchwork of state laws to understand the restrictions that impact how healthcare providers and healthcare entities use technology, and how each step in the care delivery model can be structured to comply with varying state laws. Because state standards were developed when care was predominantly provided through in-person encounters, state laws lag behind innovation and do not fully contemplate the range of available technology that is changing the healthcare delivery model.

Each state has developed its own licensing requirements and standards governing: (i) the general practice of telehealth and the ability for remote delegation, supervision and prescribing; (ii) whether the delivery of care can be synchronous or asynchronous; and (iii) the scope of clinical care, coordination and management that can be delivered digitally. Specialty societies are stepping in to shape the standards of practice and spur policy discussion. For example, the American Medical Association ("AMA") has developed a Digital Health Implementation

Playbook[13] and has defined the concept of "augmented intelligence", focusing on AI's assistive functions.[14] The AMA has also proposed a policy on augmented intelligence, with the goal of advancing high-quality, clinically validated augmented intelligence in patient care.[15]

In addition, state licensing laws limit the geographic reach of licensed healthcare professionals ("HCPs") by requiring them to be licensed where the patient resides, unless the care was provided directly to another HCP (rather than to the patient) or in an emergency situation. The onset of the COVID-19 pandemic prompted states to temporarily loosen licensure restrictions on the practice of telehealth and apply waivers from these requirements, accelerating the use and acceptance of telehealth services and allowing HCPs to provide services to patients across state lines. However, many of the state waivers that were implemented during the pandemic have not been extended, resulting in a setback in the advancements in telehealth that were gained over the past few years. Efforts to reduce these licensure barriers continue, including state licensure compacts, such as the Interstate Medical Licensure[16] and Psychology Interjurisdictional Compact,[17] which are designed to streamline the licensing process for HCPs who wish to be licensed in multiple jurisdictions.

Lastly, leveraging technology to deliver remote care or augment an HCP's ability to diagnose and treat patients through AI implicates another set of laws, called state corporate practice laws. These laws generally prohibit lay, unlicensed entities from delivering healthcare or exercising undue influence or control over the delivery of healthcare services. These laws may require companies to implement certain corporate structures or safeguards to ensure that HCPs maintain unfettered control over clinical decision-making.

EU

The European Commission defines telehealth as "the provision of healthcare services, through the use of [information and communications technology], in situations where the health professional and the patient (or two health professionals) are not in the same location" and involves "secure transmission of medical data and information, through text, sound, images or other forms needed for the prevention, diagnosis, treatment and follow-up of patients".[18] As in the US, the regulation of telehealth services in the EU remains fragmented, as such services are essentially regulated at a national level. The most relevant effort to regulate health services across the EU is Directive 2011/24/EU on patients' rights in cross-border healthcare (the "Cross Border Healthcare Directive"), which ensures continuity of care for European citizens across borders (e.g., e-prescribing) and dates back many years.

A 2018 European Commission market study on telemedicine concluded that "most telemedicine solutions are deployed at the national or regional level" and that "this is due to the significant differences in national regulations and social security schemes".[19] The study recommended that "EU countries… harmonize their legal frameworks in order to make solutions compatible and to enable cross-border telemedicine practices".[20] The recent European Commission proposal for a Regulation on the European Health Data Space included provisions seeking to harmonise and encourage cross-border telemedicine,[21] but these provisions appear to have been removed by the European Council during the ongoing legislative process. While recent developments at the EU level in this space remain limited, it is worth noting that in November 2022, the World Health Organization ("WHO") issued a consolidated telemedicine implementation guide, which provides an overview of the key considerations for implementing telemedicine globally.[22]

UK

No specific laws govern telehealth in the UK. However, the provision of health or social care (including by remote means) in England is primarily governed by the Health and Social Care Act 2008 and the Health and Care Act 2022. Similar legislation covers Wales, Scotland and Northern Ireland. The Electronic Commerce (EC Directive) Regulations 2002 (the "eCommerce Regulations"), which impose certain requirements for the provision of online services, may also apply to the provision of telemedicine services.

The provision of health and social care is regulated on a regional basis by different agencies. For example, in England, the Care Quality Commission ("CQC") regulates telehealth providers under the regulated activity of "transport services, triage and medical advice provided remotely". Telemedicine service providers (including individuals or corporate entities) are required to register with CQC or the equivalent body in Scotland, Wales or Northern Ireland.

While these regulators have authority over healthcare service providers (i.e., the individual or the entity), individual providers are also subject to licensing and enforcement by their professional bodies. In particular, the General Medical Council has licensing and enforcement authority in respect of doctors, and the General Pharmaceutical Council has such authority in respect of pharmacists. The obligation to be appropriately qualified and registered with a professional governing body applies regardless of whether the service is provided remotely or in person. As a result of Brexit, the "country-of-origin" principle under the eCommerce Regulations – which allow European Economic Area ("EEA") online service providers to operate in any EEA country, while only following relevant rules in the country in which they are established – and the rules on cross-border care from the Cross Border Healthcare Directive no longer apply. This means that professionals providing telemedicine services from the UK to patients in the EEA may also need to be licensed in the country where the patient is located.

Coverage and reimbursement considerations

Beyond the legal considerations applicable to compliance of digital health technologies with the medical devices framework and telehealth restrictions and requirements, companies must consider the laws and regulations applicable to coverage and reimbursement for their digital health technologies, or coverage and reimbursement of healthcare services provided using digital health technologies.

US

Coverage and reimbursement for health services that use digital health technologies (like telehealth) are often determined on a payor-by-payor basis, which can make it difficult for companies to navigate the payor landscape and achieve certainty with respect to payor adoption of their technologies. While the US does not have a single payor system that establishes uniform reimbursement and coverage for healthcare services that use digital health technologies, policies established by the Centers for Medicare & Medicaid Services ("CMS") – which administers Medicare, the nation's single largest public insurance programme – are particularly important because they often influence coverage and payment policies adopted by other payors.

In recent years, CMS has expanded coding and payment policies for remote monitoring services, allowing for increased flexibility with respect to the types of patients who are eligible for remote monitoring and the level of physician supervision required in order for clinical and auxiliary personnel to perform

remote monitoring services. However, several Medicare Administrative Contractors ("MACs") recently announced that they are convening a Contractor Advisory Committee ("CAC") in February 2023 to evaluate "the strength of published evidence on remote physiologic monitoring ("RPM") and remote therapeutic monitoring ("RTM") for non-implantable devices, and that they are seeking compelling clinical data to assist in defining meaningful and measurable patient outcomes (e.g., decreases in emergency room visits and hospitalisations)" for Medicare beneficiaries.[23] Although not binding on the MACs, the CAC's assessment could result in the adoption of additional coverage limitations for RPM and RTM services, which could limit the use and adoption of these services for certain segments of the population.

In addition, Congress and various federal and state agencies have continued to provide expanded flexibilities to enable coverage and reimbursement for telehealth services during the declared COVID-19 public health emergency ("PHE"), including policies allowing certain telehealth services to be reimbursed at the same rate as equivalent in-person services. While some of these flexibilities have been extended through the end of 2024,[24] others are expected to terminate when the COVID-19 PHE ends. The explosion of telehealth and digital health offerings in the US healthcare system as a result of these policies has been paralleled by an increasing number of enforcement actions, scrutiny by federal regulators and the issuance of a special fraud alert around the use of telehealth services.[25] It is important that digital health companies stay abreast of this increased regulatory scrutiny, and the evolving regulatory scheme, as they structure their operations.

EU

The reimbursement landscape for digital health tools is fragmented across the EU, given that reimbursement decisions are made at a national or even regional level, and not by EU authorities. This poses particular challenges to both the manufacturers that are developing digital health technologies and the health authorities that are evaluating them. In particular, these authorities' traditional methods to evaluate products for coverage and reimbursement do not focus on aspects that are relevant to digital health technologies (e.g., interoperability, privacy, data security and ethical considerations). Moreover, because these technologies are often updated more quickly than traditional devices (especially when incorporating AI/ML), they require similarly speedy evaluation decisions. As a consequence, national reimbursement schemes for digital health technologies are inconsistent across the EU, including with respect to the type of evidence that is accepted as sufficient, and little guidance is available to assist manufacturers in navigating the requirements. Certain countries have implemented specific frameworks for reimbursement decisions with respect to digital health technologies. Germany, for instance, is the first EU country to have recently implemented a "fast track" reimbursement for certain digital medical products, such as wearable devices or mobile applications.

The EU Health Technology Assessment ("HTA") Regulation (2021/2282), which for the first time introduces a permanent legal framework for joint HTA work (i.e., joint clinical assessments and scientific consultations) by EU member states, is an important step toward a more uniform assessment of innovative high-risk medical devices, including digital health technologies. In preparing for the regulation's phased implementation from 2025 onwards, several national HTA bodies in Europe have recently joined forces with EU-level organisations, such as the European Network for HTA, to develop recommendations on harmonised evaluation guidelines for digital medical devices. For instance, in October 2022, a European taskforce was launched by nine EU Member States with the objective to reach a mutual understanding between national HTA agencies for digital medical devices in order to harmonise assessment criteria and clinical evidence requirements and improve access to digital health technologies in the EU.[26]

UK

The National Health Service ("NHS") funds the majority of digital health products and services provided to patients in the UK. In addition, there exists a smaller, but growing, private healthcare sector, which is funded through private insurance or directly by patients. There are a number of routes for products to be made available for reimbursement by the NHS, including selling directly to NHS trusts or primary care organisations, or procurement through the NHS supply chain or public tenders. In addition, digital health products can undergo a technology appraisal from the National Institute for Health and Care Excellence ("NICE"), and the NHS is obligated to fund and resource treatments recommended by NICE.

The NHS has published a "guide to good practice for digital and data-driven health technologies",[27] which is designed to help innovators understand the NHS requirements when the NHS buys digital and data-driven technology. NICE has published the "Evidence standards framework for digital health technologies",[28] which describes the standards for digital health technologies to demonstrate their value in the UK healthcare system.

Data privacy and data use

Data and digital health go hand-in-hand, whether they involve the analysis of large and complex datasets by an AI/ML tool or the collection of an individual's health and lifestyle data through a wearable device. As such, navigating the complex and continually evolving web of privacy and cybersecurity laws is critical to the deployment of any digital health solution.

US

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulates the use and disclosure of sensitive health information. Specifically, the HIPAA requires certain "covered entities" to comply with privacy and security requirements, including providing notice of how an individual's protected health information ("PHI") will be handled as well as the statutory rights patients hold in relation to the handling of their PHI.

The data protection landscape is rapidly growing and evolving on a state level. For example, the California Consumer Privacy Act of 2018 requires companies that process information on California residents to make certain disclosures to consumers about their data collection, use and sharing practices. The law also allows consumers to opt out of certain data sharing with third parties and exercise certain individual rights regarding their personal information, providing a new private right of action for data breaches and penalties for noncompliance. In addition, the California Privacy Rights Act was recently passed and will impose additional data protection obligations on covered businesses, including additional consumer rights processes, limitations on data uses, new audit requirements for high-risk data and opt-outs for certain uses of sensitive data. Similar laws have been passed in Virginia, Colorado, Connecticut and Utah and have been proposed in other states and at federal level, reflecting a trend toward more stringent privacy legislation in the US.

Furthermore, the Federal Trade Commission ("FTC") and many state Attorneys General continue to enforce federal and

state consumer protection laws against companies for online collection, use, dissemination and security practices that appear to be unfair or deceptive. Recent FTC guidance on AI/ML has focused on the potential risks to fair and transparent consumer transactions represented by opaqueness in automated decision-making and predictive analytics. The FTC is also concerned about misleading representations to consumers regarding a company's data collection and handling practices that underwrite the data sets on which algorithms are trained. The FTC has highlighted the particular risks to healthcare consumers in unfair or deceptive data practices leveraging AI as an area of developing regulatory concern. Of particular relevance to the digital health sector are potential harms to patients introduced as a result of improper oversight when AI tools are used for automated decision-making, leading to discriminatory clinical or treatment outcomes.

EU

In the EU, the processing of personal data is primarily governed by Regulation (EU) 2016/679 ("GDPR"). The GDPR imposes comprehensive data-privacy compliance obligations in relation to the use or "processing" of information relating to an identifiable living individual or "personal data". The GDPR applies not only to entities established in the EU, but also to entities established outside the EU if they offer goods or services to EU individuals or monitor their behaviour. Organisations deploying digital health solutions to individuals across the EU and the UK may therefore need to comply with both the GDPR and the UK data protection regime. While the GDPR was intended to harmonise data protection laws across the EU, national implementing laws diverge in certain areas, such as the processing of personal data for public health or scientific research purposes. Therefore, companies must navigate not only the GDPR, but also national implementing and supplementary legislation as well as legal, ethical and professional rules designed to protect patient confidentiality.

Although the GDPR was enacted to be technology-neutral, the advent of the digital health industry has led to challenges in the interpretation and application of the GDPR. For example, some digital health applications such as wearables have led to questions on the distinction between health data (which is considered "special-category data" under the GDPR and subject to enhanced protections) and other non-health "lifestyle" data. This distinction, in turn, leads to potential compliance challenges, such as identifying appropriate legal bases for processing such health data and other personal data under the GDPR and ensuring that individuals are adequately informed of the processing of their data.

Other applications of digital health, such as AI/ML algorithms, have raised difficult questions regarding transparency and how data subjects can be informed in easy-to-understand terms of how the algorithm processes their data. Where personal data has been used to train an algorithm, withdrawal of a subject's consent (where consent has been used as the legal basis for such processing) to limit further use of their data may not be practical or possible and could affect the integrity of the algorithm. In such cases, the developer will need to consider whether it can continue to legitimately use that data, such as whether it has been effectively anonymised or aggregated. Ensuring data accuracy and the absence of bias are also key considerations for these types of tools.

Another increasingly tricky area for digital health operators is in relation to international data transfers. Where personal data are transferred from the EU to a country that is not considered to provide an "adequate" level of protection for the data, such transfer is prohibited unless a relevant derogation applies or certain safeguards are implemented. Recent legal developments in the EU have created complexity and uncertainty regarding such transfers, particularly in relation to transfers to the US.[29] The shifting sands of data transfers can be difficult to navigate and companies must pay close attention to the complex data flows that are often involved in digital health solutions.

Many digital health solutions, such as wearables and apps, may use cookies or other tracking technologies. While cookies that are strictly necessary for the device, site or app to function correctly can be used without opt-in consent, others such as analytics or advertising trackers will require specific opt-in consent under EU Directive 2002/58/EC ("ePrivacy Directive") and national implementing laws, which may not be straightforward depending on the nature of the device. User data collected from devices is also subject to the GDPR. The use of cookies, tracking technologies and user profiling is subject to increasing regulatory scrutiny and enforcement, particularly around the use of individuals' data for marketing and advertising.

Beyond the general requirements to ensure the security of personal data in the GDPR, there is a trend toward increasing regulation of cybersecurity through sector-specific or device-specific rules. For example, the MDR requires the manufacturing of certain devices to take into account information security principles. In addition, on November 28, 2022, the EU adopted Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU ("NIS-2 Directive"). The NIS-2 Directive establishes cybersecurity risk-management measures and reporting requirements for critical sectors, including manufacturers of medical devices. The draft EU Cyber Resilience Act also proposes a framework of consistent security standards for digital products, applicable through the whole product lifecycle.

In parallel with the trend toward increased regulation and scrutiny, there is a trend toward enabling greater sharing and reuse of data, particularly for research and innovation. For example, on May 3, 2022, the European Commission launched its proposal for a Regulation for the European Health Data Space to "unleash the full potential of health data", facilitating the systematic digitisation of health records and secondary use of clinical data for research purposes. In addition, the proposed EU Data Act, which seeks to regulate the sharing and use of data generated by connected devices, would include new rights for users of connected services, introduce data portability obligations, impose restrictions on the use of user data and regulate data sharing contracting.

Across the EU, there is a trend toward increasing enforcement of data protection laws and ever-larger fines. There is also increasing scrutiny and enforcement from a broader range of regulators – including data protection regulators, consumer protection authorities and competition regulators – and increasing coordination efforts around data and digital platforms.

UK

Following Brexit, the GDPR has been mirrored in UK law as the "UK GDPR", which together with the Data Protection Act 2018 form the UK's data protection regime. The UK Information Commissioner's Office has introduced specific data-transfer mechanisms to safeguard transfers of data out of the UK, namely the International Data Transfer Agreement and the International Data Transfer Addendum to the EU's standard contractual clauses.

The UK government has proposed wide-ranging reforms to UK data protection laws, set out in the UK Data Protection and Digital Information Bill (which was introduced to Parliament in July 2022). The bill largely maintains the GDPR framework in UK law, albeit with modifications reflecting the government's intention to move away from prescriptive requirements and

toward a more risk-based approach. While the UK has signalled a more business-friendly and flexible approach, which would be welcomed by operators in the digital health sector, it remains uncertain where the post-Brexit UK privacy landscape will land.

On June 29, 2022, the UK government published a policy paper titled "A plan for digital health and social care",[30] which sets out its far-reaching plans for the digital transformation of health and social care in England. The plan includes proposals for the systematic digitisation of health and social care records, and the creation of a life-long health and social care record. The proposal also aims to equip the NHS with the capacity to develop image-sharing and other technical capabilities based on AI, to enable "digitally-supported diagnoses" and to establish a network of trusted research environments to support research and development.

Conclusion

Digital health companies must stay attuned to the emerging trends in the global regulation of these technologies, with the recognition that the frameworks are continuing to evolve. As demonstrated in the US, EU and UK, a myriad of legal requirements create a spider's web for companies and investors to carefully navigate in order to avoid compliance issues and maintain momentum in a competitive marketplace. By remaining aware of the key legal constructs and staying abreast of proposed changes in these frameworks, stakeholders can play a part in shaping the legal regimes applicable to their digital health solutions. Moreover, they can reduce the risk of a compliance misstep, which may be more likely in an industry in which technological advancements outpace the legal frameworks and innovators, in many cases, operate in uncharted territory under the law.

Endnotes

1. 21 U.S.C. § 321(h)(1) (2022).
2. *Id.* § 360j(o).
3. U.S. Food & Drug Admin. (FDA), Policy for Device Software Functions and Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/80958/download.
4. U.S. FDA, General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff (2019), https://www.fda.gov/media/90652/download.
5. U.S. FDA, Clinical Decision Support Software: Guidance for Industry and Food and Drug Administration Staff (2022), https://www.fda.gov/media/109618/download.
6. U.S. FDA, *Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence (last visited Jan. 21, 2023); U.S. FDA, *About the Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence/about-digital-health-center-excellence (last visited Jan. 21, 2023).
7. *See, e.g.,* U.S. FDA, *Artificial Intelligence and Machine Learning in Software as a Medical Device*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device (last visited Jan. 29, 2023).
8. Med. Device Coordination Group (MDCG), Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR (2019), https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf.
9. Eur. Comm'n, Manual on Borderline and Classification in the EU Regulatory Framework for Medical Devices (2022), https://health.ec.europa.eu/latest-updates/manual-borderline-and-classification-community-regulatory-framework-medical-devices-september-2022-2022-09-07_en.
10. European Medicines Agency (EMA), Guideline on Quality Documentation for Medicinal Products When Used with a Medical Device (2021), https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-quality-documentation-medicinal-products-when-used-medical-device-first-version_en.pdf.
11. Medicines and Healthcare Regulatory Products Regulatory Agency (MHRA), Consultation on the Future Regulation of Medical Devices in the United Kingdom (2021), https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom.
12. MHRA, Software and AI as a Medical Device Change Programme – Roadmap (2022), https://www.gov.uk/government/publications/software-and-ai-as-a-medical-device-change-programme/software-and-ai-as-a-medical-device-change-programme-roadmap.
13. American Medical Association (AMA), *Digital Health Implementation Playbook Series*, https://www.ama-assn.org/practice-management/digital/digital-health-implementation-playbook-series (last visited Jan. 30, 2023).
14. AMA, *Augmented Intelligence in Medicine*, https://www.ama-assn.org/practice-management/digital/augmented-intelligence-medicine#:~:text=The%20AMA%20House%20of%20Delegates%20uses%20the%20term%20augmented%20intelligence,intelligence%20rather%20than%20replaces%20it (last visited Jan. 30, 2023).
15. AMA, *Policy: Augmented Intelligence in Health Care*, https://www.ama-assn.org/system/files/2019-08/ai-2018-board-policy-summary.pdf (last visited Jan. 30, 2023).
16. Interstate Medical Licensure Compact, https://www.imlcc.org/ (last visited Jan. 30, 2023).
17. Psychology Interjurisdictional Compact (PSYPACT), https://psypact.org/page/About (last visited Jan. 30, 2023).
18. Eur. Comm'n, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Telemedicine for the Benefit of Patients, Healthcare Systems and Society (2008), COM(2008)0689 final, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008DC0689.
19. Eur. Comm'n, Market Study on Telemedicine (2018), https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf.
20. *Id.*
21. Eur. Comm'n, Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (2022), COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197 (The original Article 8 set out that: "If a Member State accepts the provision of telemedicine services, it shall, under the same conditions, accept the provision of similar services by healthcare providers located in other Member States.").
22. World Health Org. (WHO), Consolidated Telemedicine Implementation Guide (2022), https://www.who.int/publications/i/item/9789240059184 (last visited Jan. 26, 2023).

23. CGS Medicare, *Multi-Jurisdictional Contractor Advisory Committee (MJCAC) Meeting Regarding Remote Physiologic Monitoring (RPM) and Remote Therapeutic Monitoring (RTM) for Non-Implantable Devices on February 28th, 2023 – 6:00 – 8:00 PM ET* (Nov. 10, 2022), https://www.cgsmedicare.com/partb/pubs/news/2022/11/cope3231.html (last visited Jan. 30, 2023).
24. Consolidated Appropriations Act, 2023, H.R. 2617, 117th Cong. (2022).
25. Office of Inspector General, U.S. Dept. of Health and Human Services (HHS), Special Fraud Alert: OIG Alerts Practitioners To Exercise Caution When Entering Into Arrangements With Purported Telemedicine Companies (2022), https://oig.hhs.gov/documents/root/1045/sfa-tele-fraud.pdf.
26. Haute Autorité de Santé (HAS), Towards a European Evaluation Framework for Digital Medical Devices (DMDs) in the European Union — Launch of a European Taskforce (2022), https://www.has-sante.fr/jcms/p_3382241/en/towards-a-european-evaluation-framework-for-digital-medical-devices-dmds-in-the-european-union-launch-of-a-european-taskforce (last visited Jan. 26, 2023).
27. Dept. of Health and Social Care (DHSC), U.K. Nat'l Health Serv., A Guide to Good Practice for Digital and Data-Driven Health Technologies (2021), https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (last visited Jan. 30, 2023).
28. Nat'l Inst. for Health and Care Excellence (NICE), Evidence Standards Framework for Digital Health Technologies (2022), https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies (last visited Jan. 30, 2023).
29. In March 2022, the US and EU announced a new regulatory regime intended to replace the invalidated Privacy Shield; however, this new EU-US Data Privacy Framework has not been implemented beyond an executive order signed by President Biden on October 7, 2022 (Administration of Joseph R. Biden, Jr., 2022 Executive Order 14086-Enhancing Safeguards for United States Signals Intelligence Activities, Daily Comp. Pres. Docs. 1 (2022)).
30. DHSC, U.K. Nat'l Health Serv., A Plan for Digital Health and Social Care (2022), https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care (last visited Jan. 30, 2023).

Eveline Van Keymeulen advises multinational companies and start-ups in the pharmaceutical, biotech, medical devices and digital health sectors on a broad variety of complex European, domestic and cross-border regulatory matters, including clinical trials, product approvals, regulatory incentives, market access, promotion and advertising, post-market obligations and general compliance matters. Eveline is widely recognised for her regulatory life sciences expertise by *Chambers* (2020–2022), *The Legal 500* (2018–2022) and *Who's Who Legal Life Sciences* (2016–2022). She was voted European "Advisory Lawyer of the Year" by *LMG Life Sciences* (2021) and won their "Impact Case of the Year" award (2021–2022) for her work in the groundbreaking CJEU Kanavape case, for which she equally received the *Financial Times* European Innovative Lawyer Award (2022).

Latham & Watkins
Boulevard du Régent, 43–44
Brussels, B-1000
Belgium

Tel: +32 2 788 6000 / +33 1 4062 2060
Email: eveline.vankeymeulen@lw.com
URL: www.lw.com

Elizabeth Richards advises clients in all facets of oversight and regulation by the FDA, helping clients navigate regulatory frameworks governing the digital health and medical device, pharmaceutical, biotechnology, food, dietary supplement and cosmetic industries. She is attuned to her clients' business objectives while guiding them through compliance, enforcement, transactional and legislative matters, traversing the legal labyrinth required to bring new products to market and maintain compliance once commercialised. Her practice spans all stages of the product life cycle, and she has been recognised as a leading industry lawyer by multiple publications, including *Chambers USA*, *The Legal 500 US*, *LMG Life Sciences* and *The Diversity Journal*.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2130
Email: elizabeth.richards@lw.com
URL: www.lw.com

Nicole Liffrig Molife advises emerging companies as well as commercial companies in the digital health, pharmaceutical, medical device and technology sector. She leverages her deep knowledge of fraud and abuse laws as well as telehealth and other healthcare regulatory laws to guide companies as they develop their product development and launch strategies and business models, providing solutions that mitigate regulatory risk while fostering innovation. Nicole's practice includes counselling on sales and marketing activities and relationships with referral sources, evaluating industry collaborations, structuring key commercial agreements at all stages of development and advising on life sciences transactions.

Latham & Watkins
555 Eleventh Street, NW, Suite 1000
Washington, D.C., 20004
United States

Tel: +1 202 637 2121
Email: nicole.liffrig@lw.com
URL: www.lw.com

Oliver Mobasser has particular expertise in the healthcare and life sciences sectors, advising multinational pharmaceutical, biotechnology and medical technology companies and their investors on complex licences, collaborations, acquisitions, divestments, commercial contracts, intellectual property matters and regulatory and privacy matters. Oliver's experience covers: product licensing and acquisitions; complex commercial contracts and collaborations; technology and life sciences transactions; business carve-out transactions; digital health; and data protection.

Latham & Watkins
99 Bishopsgate
London, EC2M 3XF
United Kingdom

Tel: +44 20 7710 4738
Email: oliver.mobasser@lw.com
URL: www.lw.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group