iclg

Digital Health 2025

Sixth Edition

Contributing Editor:

Roger Kuan

Norton Rose Fulbright

glg Global Legal Group

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

India

Manisha Singh

Dr. Pankaj Musyuni

LexOrbis

1 Digital Health

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

Digital healthcare is a multidisciplinary concept that is located at the intersection of healthcare and digital technology. Digital healthcare revolutionises the delivery of healthcare services for providers through the use of comprehensive platforms, tools and services. Mobile health applications, telemedicine, enterprise resource planning (ERP), customer relationship management (CRM), electronic health records (EHRs) and health information systems (HIS) are among the numerous technologies that contribute to the transparency of patient data. "Digital health" is a comprehensive concept that entails the integration of digital technologies with the healthcare sector to improve efficiency and provide more personalised patient care. The Digital Information Security in Healthcare Act of 2018 (DISHA) defines "digital health data" as an electronic record of an individual's health-related information, despite the fact that the terms "digital health", "digital medicine" and "digital therapeutics" lack specific definitions in India. The term "said data" generally refers to relevant information about an individual's physical and mental health, the therapies they have received from healthcare providers, any donated body parts or biological materials, as well as the results of their testing and examinations. The integration of genetics and digital technologies exemplifies the concept of digital health, facilitating the early diagnosis and treatment of diseases. The World Health Organization (WHO) and the G20 India presidency introduced the Global Initiative on Digital Health (GIDH) during the Health Minister's Meeting at the G20 Summit, which the Government of India convened on August 19, 2023. The new GIDH initiative will function as a network and infrastructure under the WHO's supervision to facilitate the implementation of the Global Strategy on Digital Health 2020–2025.

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

Digital healthcare is a multidisciplinary concept that lies at the intersection of healthcare and digital technology. It incorporates a diverse array of technologies, such as telemedicine, ERP, CRM, EHRs and HIS, all of which enhance the transparency of patient data. The most significant emerging technologies in the field of digital health include m-health, digital pathology, telemedicine, health wearables, digital and social connectivity, big data analytics, virtual reality, ambupods, blockchain and electronic medical records. Increased awareness and adoption for the Internet of Things (IoT) and telehealth have made health-monitoring technology more accessible and cost-effective. The healthcare sector of India has undergone significant transformations as a result of the Digital India initiative. Initiatives like the Ayushman Bharat Digital Mission, CoWIN App, Aarogya Setu, e-Sanjeevani and e-Hospital have extended healthcare facilities and services to every corner of India.

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

The favourable legislation in India and the growing prominence of the digital healthcare industry have significantly improved the country's use of digital technology. Industry experts anticipate the digital health industry in India to expand at a compound annual growth rate (CAGR) of approximately 29.5% from 2024 to 2032. Leading experts anticipate that the digital health sector in India will reach a valuation of USD 3.88 billion in 2023 and rise to USD 39.7 billion by 2032. It is anticipated that the Indian digital health market will experience growth due to the increasing prevalence of chronic conditions during the projected period. According to a customer market insights survey, it is expected that the Indian digital health market will reach USD 8.7944 billion in 2024 and expand at a CAGR of 17.67% between 2024 and 2033, ultimately reaching USD 47.8069 billion. The objective of digital health is to enhance the quality, accessibility and delivery of medical services by integrating technology with healthcare. It encompasses a diverse array of applications, such as telemedicine, mobile health applications, EHRs and data-driven, AI-powered personalised care. Insights10, a healthcare-focused market research agency, anticipates that the Indian digital health market will experience accelerated growth in the coming years as a result of its size and favourable government policies.

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

Among the top five largest digital healthcare technology enterprises are Novartis, Stryker, Edwards Lifesciences, Centura Health and Hologic.

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

The more promising digital health start-ups and the fastest growing in India include 1mg, HealthifyMe, Netmeds, Cult.fit, Onsurity, HealthKart, PharmEasy and Innovaccer.

2 Regulatory

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

The Central Drugs Standard Control Organisation (CDSCO) is the primary regulatory body responsible for the enforcement of the Drugs and Cosmetics Act, 1940, and "rules made thereunder" (DCA). Furthermore, the Medical Council of India oversees the practice of medicine. Additionally, the Copyright Office is responsible for copyright, while the Office of the Controller General of Patents, Designs and Trademarks is responsible for intellectual property protection. The Department for Promotion of Industry and Internal Trade comprises both divisions. The Indian Council of Medical Research has also made significant contributions to the promotion of research in support of the National Digital Health Blueprint from the Ministry of Health and Family Welfare (MoHFW).

The following key acts typically govern the legal and regulatory framework:

- In 2011, the Information Technology Act (IT Act), consisting of the Information Technology Rules (IT Rules) of 2011 and the Sensitive Personal Data or Information (SPDI) Rules, came into effect.
- Requirements for other service providers under the New Telecom Policy of 1999.
- The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations of 2002 and the Indian Medical Council Act of 1956.
- The Drugs and Magic Remedies Act of 1954 and the Drugs and Magic Remedies Rules of 1955.
- The Unsolicited Commercial Communications Regulations of 2007 and the Commercial Communication Customer Preference Regulations of 2010.
- The Clinical Establishments Act of 2010.
- The Digital Personal Data Protection Act (DPDP Act).

The Indian government is responsible for enforcing rules regarding digital health. These rules come from: the DCA; the IT Act and Rules, especially Sections 2(w), 43A and 79; the Clinical Establishments (Registration and Regulation) Act, Section 38(1) and 38(2); and Rules 3, 4(1), 5(1), 5(3), 5(7) and 7 of the IT Act. The regulatory authorities are responsible for enforcing reasonable security practices and procedures for SPDI, as outlined in: the Data Protection Rules; Rule 3 of the IT (Intermediaries Guidelines) Rules; the Medical Devices Rules; the DNA Technology (Use and Application) Regulation Bill; and the DPDP Act.

In order to protect the confidentiality of health-related information, it is imperative that medical professionals and patients implement data security measures. This information includes recommendations and outcomes. The Intermediaries Guidelines of 2011, the Data Protection Regulations of 2011 and the IT Act of 2000 are all intended to address this need and should be consulted in all circumstances. However, the rigorous compliance requirements have led to the establishment of no standards mandating the implementation of data security and protection. The rise of digital and other healthcare technology has raised patient privacy and data security concerns. When transmitting personal data, the most critical factors to consider are the preservation of confidentiality, the regulation of data transmission, the assurance of security and privacy, and the consideration of knowledge, trust, accountability and responsibility.

The MoHFW has proposed the National Digital Health Authority (NeHA) to facilitate the development of India's Integrated Health Information System (IHIS). On August 11, 2023, the ratification of the DPDP Act, 2023, transformed India into a legal nation. India has implemented a new law to govern the administration of personal data. In addition to establishing a framework for the governance and accountability of data, one of its objectives is to preserve the privacy of individuals. The DPDP Act will have a substantial impact on the Indian healthcare industry, despite the fact that it is still in the early phases of digital transformation. The DPDP Act primarily focuses on digital personal data and does not address non-personal data. The implementation of the DPDP Act will render Section 43A of the IT Act and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011. These pieces of legislation address the legal and ethical concerns related to digital health.

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

The IT Act and the SPDI Rules govern the current legislative framework for e-health protection in India, offering some protection for the acquisition, disclosure and transmission of sensitive personal data, including medical records and histories. The government and the MoHFW published a blueprint, recommending the establishment of a National Digital Health Ecosystem, and announced the National Digital Health Mission (NDHM). This ecosystem will enable the interoperability of digital health systems at the patient, hospital and ancillary healthcare provider levels. The MoHFW implemented the Health Data Management Policy for the ecosystem. Furthermore, the MoHFW implemented the DPDP Act in India with the primary goal of promoting accountability and responsibility among enterprises operating within the country. Reproductive Child Healthcare, the Integrated Disease Surveillance Program, the IHIS, e-Hospital, e-Sushrut, the Central Government Health Scheme, the Integrated Health Information Platform, the National Health Portal, the National Identification Number and the Online Registration System are among the numerous digital health initiatives that the MoHFW is currently implementing. As health is a state responsibility, the National Health Mission provides funding to states for related services, such as hospital information systems, telemedicine, teleradiology, tele-oncology and tele-ophthalmology.

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

It is imperative to establish regulations that safeguard the privacy, confidentiality and security of patients' medical and health records. Monitoring data protection and violations

is crucial, as confidentiality agreements safeguard private health information and records solely for data interpretation in market analysis, marketing and regulatory sharing. In India, telemedicine and teleconsultation, wearable devices, online pharmacies and artificial intelligence (AI) are among the most significant emerging technologies in the field of digital healthcare.

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

The CDSCO, a part of the Directorate General of Health Services (MoHFW), is India's major medical device and diagnostics regulating organisation. The Drug Controller General of India (DCGI) leads the CDSCO. The DCGI approves specific medications (vaccines, large-volume parenterals, blood products and r-DNA-derived products), medical devices and novel drugs. The DCA governs the manufacture, importation, sale and distribution of medical equipment in India. Only the following notified medical devices listed below as "drugs" are currently under the DCA's control in India:

(i) substances used for *in vitro* diagnosis and surgical dressings; surgical bandages, surgical staples, surgical sutures, ligatures, blood, and blood-component collection bags with or without anticoagulant; and

(ii) substances, including mechanical contraceptives (condoms, intrauterine devices and tubal rings).

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

There are currently no official provisions.

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

There are currently no official rules.

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

There are currently no official provisions.

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

There are currently no official rules.

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

There are currently no official rules.

3 Digital Health Technologies

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

- **Telemedicine/Virtual Care**
  - A. Adoption of technology.
  - B. Evidence.
  - C. Technical training.
  - D. Record-keeping and data management.
  - E. Data privacy.
- **Robotics**
  - A. Energy storage.
  - B. Ethics and security.
  - C. Confidentiality.
- **Wearables**
  - A. Cost of device.
  - B. Battery life.
  - C. Safety, security and privacy.
- **Virtual Assistants (e.g. Alexa)**
  - A. Lack of accuracy.
  - B. Lack of analytical interpretation.
  - C. Data privacy and confidentiality.
- **Mobile Apps**
  - A. Competitive market.
  - B. Promotion and marketing.
  - C. Data management and privacy.
- **Software as a Medical Device**
  - A. Software development lifecycle.
  - B. Product safety and security.
  - C. Data collection, analysis and privacy.
- **Clinical Decision Support Software**
  - A. Development lifecycle.
  - B. Product safety and accuracy.
  - C. Data analysis.
- **Artificial Intelligence/Machine Learning-Powered Digital Health Solutions**
  - A. Lack of precision.
  - B. Lack of interpretation.
  - C. Irregularity in analytics.
  - D. Reliance.
  - E. Transparency and governance.
  - F. Long-term cost.
- **IoT (Internet of Things) and Connected Devices**
  - A. Compatibility of operating systems.
  - B. Identification and authentication of devices and technologies.
  - C. Integration of IoT products and platforms.
  - D. Connectivity.
  - E. Data analytics, security and privacy.
  - F. Consumer awareness.
- **3D Printing/Bioprinting**
  - A. Piracy.
  - B. Misinterpretation of results.
  - C. Lack of training skills.
- **Digital Therapeutics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
- **Digital Diagnostics**
  - A. Lack of accuracy.
  - B. Lack of interpretation and understanding.
  - C. Misinterpretation of results.
  - D. Lack of training skills.

- **Electronic Medical Record Management Solutions**
  A. Lack of training skills.
  B. Data collection, analysis and privacy.
  C. Data privacy and confidentiality.
- **Big Data Analytics**
  A. Lack of interpretation and understanding.
  B. Misinterpretation of results.
  C. Lack of training skills.
- **Blockchain-based Healthcare Data Sharing Solutions**
  A. Lack of interpretation and understanding.
  B. Lack of training skills.
  C. Data collection, analysis and privacy.
- **Natural Language Processing**
  A. Understanding of natural language.
  B. Reasoning about multiple documents.
  C. Identification of data and evaluation of problems.

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

In general, digital platform providers are preoccupied with the assessment and supervision of the transitional phase of introducing new technologies to the market, as well as the mitigation of risk. Consequently, digital platform providers should prioritise personnel training, understand the importance of market demand and in-line supply, improve IT systems and exhibit strong leadership.

4 Data Use

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

A fragmented and ambiguous legal and regulatory framework currently governs digital health in India. Additionally, there is a scarcity of legal scholarship on digital health in India. This is particularly challenging because digital health encompasses a wide range of aspects, such as data aggregation and processing, business models and technological advancements. Consequently, the regulatory system is fragmented. In the utilisation and application of personal data, data privacy is of the utmost importance. India implemented the initial EHR Standards in 2013. The importance of international EHR standards in India facilitated their incorporation through the selection of the most qualified candidates. Consequently, healthcare organisations and providers disseminated and made the 2016 EHR Standards paper accessible for deployment in national IT systems. The MoHFW is fostering the adoption of standards, including the Systematised Nomenclature of Medicine-Clinical Terminology in India by providing them at no cost and establishing an interim National Release Centre to oversee the clinical terminology standard. Global healthcare IT stakeholders are gradually acknowledging this standard. The MoHFW is committed to the regulation of the storage and exchange of EHRs, the enforcement of privacy and security protocols for electronic health data, and the promotion and implementation of e-health standards.

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

Indian law does not control health data management. The IT Act, 2000, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011, are important laws. The Computer Emergency Response Team, an Indian cybersecurity regulator, has released rules. The rules apply to all body corporates, including sole proprietorships, companies and other professional groupings. Most healthcare providers – hospitals, clinics and independent practitioners – are body corporates and are regulated.

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

Research organisations, hospitals and technology service providers are among the entities that are involved in the exchange of information, record-keeping and data collection. Furthermore, these procedures further may be adjusted in response to continuing issues and experiences that arise during the consumer–service provider transition, latency period and linkage.

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

These regulations outline the standards for "sensitive health-related information" and "sensitive personal information", setting the extent of information use with the approval of both the beneficiary and the service provider.

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

Contracts serve as the most effective method to ensure the confidentiality and concealment of all aspects of the investigation, including the acquisition and utilisation of data, from public view. It is advised that employees and other influential individuals who participate in the research sign personal privacy and non-disclosure agreements. Moreover, if participants breach predetermined contractual obligations, they should have access to a wider range of alternatives. Conversely, there are no specific laws or regulations that govern the collection or utilisation of personal health data.

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

It is essential to establish a comprehensive legislative framework that regulates the acquisition and dissemination of personal data in order to resolve concerns regarding data

inaccuracy, bias and/or discrimination. The DPDP Act now regulates the processing of digital personal data in India, irrespective of its original digital or non-digital format before digitisation. Nevertheless, the practical insights are not yet apparent in practice.

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

Regulations designed to safeguard sensitive personal data include the EHR Standards for India, 2016, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011. Disclosures under these regulations are contingent upon consent. The Data Security Council of India has developed the DSCI Privacy Guide for Healthcare, which outlines a range of data categories, including personal health data and information. The National Ethical Guidelines for Biomedical and Health Research Involving Human Participants, the Assisted Reproductive Technology (Regulation) Act, 2021, the ICMR Guidelines for Good Clinical Laboratory Practices, the Telemedicine Practice Guidelines and the Indian Medical Council's (Professional Conduct, Etiquette and Ethics) Regulations, 2002, are additional sector-specific guidelines. The objective of these regulations is to guarantee the privacy and protection of personal health information in India.

5 Data Sharing

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

Critical legal and regulatory considerations in the exchange of personal data include the adaptability of data collection and transfer, the protection of personal information and privacy during the transformation process, the dissemination of information, trust, responsibility and accountability.

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

There is no uniform handling of personal health data sharing regulations, and all the provisions are under the purview of the IT Act, 2000, and the IT (Reasonable Security Practices and Procedures and SPDI) Rules, 2011.

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

The total number of participants, patient data and scientific entities significantly influence these critical variables. In addition, the objective of utilising data protection and privacy to expedite the acquisition of answers may affect data sharing, a critical factor that all parties should consider at each stage of the process.

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

There are no specific provisions and standard regulations set by the government yet. However, the Indian government has launched the NDHM, which aims to digitise all of the country's medical information. The National Institution for Transforming India (NITI Aayog) has proposed the National Health Stack, a forward-thinking digital platform.

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

Ensuring data sovereignty, meeting regulatory standards and enhancing trustworthiness are critical concerns for healthcare data sharing.

6 Intellectual Property

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

India adopted and enacted the Patents Act of 1970, which provides patent protection and complies with the Agreement on Trade-Related Aspects of Intellectual Property Rights. To qualify for patent protection in India, an invention must satisfy the criteria of novelty, innovative steps and industrial applicability and must also be exempt from Sections 3 and 4 of the Patents Act. Section 3(k) of the Patents Act precludes the patenting of a computer program in isolation, as digital health applications are dependent on software and computer programs. Additionally, the Delhi High Court asserted that not all computer programs are exempt from Section 3(k), and that an innovation can receive patent protection if it demonstrates a "technical effect" or "technical contribution". Section 3(i) of the Patents Act says that you cannot get a patent for a program or method that is "a process for the medicinal, surgical, curative, preventative, or other treatment of human beings or any analogous treatment of animals to render them disease-free or enhance the economic value of their products". Nonetheless, the apparatus and methodology for executing an *in vitro* mechanism are eligible for patent protection.

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

The Copyright Act of 1957 safeguards intellectual property in India. Copyright safeguards original literary, dramatic, musical or artistic works, cinematographic films and audio recordings. Although copyright registration is not mandatory, it serves as primary evidence to support a legal claim. Copyright laws protect digital health apps and technology, which are fundamentally software, as "computer programs".

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

India lacks a specific statute regulating the management of sensitive information and trade secrets pertaining to digital

health technologies. The emerging digital health sector frequently utilises non-disclosure and confidentiality agreements to safeguard sensitive information.

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

The concept of academic technology transfer is still in its infancy in India. The overwhelming majority of enterprises have not adopted this methodology, despite the fact that colleges and certain corporations have established guidelines for the strategic implementation of innovations and the recognition of inventors. The digital health sector is currently in the early phases of intellectual property protection; however, it is experiencing rapid growth, and academic and research organisations are becoming more aware of its significance. It seems that this approach is acquiring momentum and resulting in improved results. The intellectual property of the proposed invention is safeguarded, and the most suitable partner is identified for the licensing and commercialisation of the technology and its functionalities. Additionally, the invention is evaluated for patentability and commercialisation. The dissemination of academic technology is a component of these endeavours.

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

Section 3(k) of the Indian Patents Act prohibits the patentability of computer programs in general. The Delhi High Court has elucidated that Section 3(k) does not apply to all computer programs, allowing for their patentability if they exhibit a "technical effect" or "technical contribution". Section 3(i) of the Patents Act prohibits the granting of a patent for a program or process that involves "a medicinal, surgical, curative, prophylactic, or other treatment of human beings or any process for a similar treatment of animals to render them disease-free or to increase their economic value or that of their products". The *in vitro* mechanism's apparatus and method of use are patentable.

Since digital health applications are essentially software, Indian law should classify them as "computer programs" and grant them copyright protection. Class 9, which encompasses computer software and computer programs, also allows for trademark registration.

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

In India, it is not possible to identify an AI device as the inventor of a patent. The Indian Patents Act and associated patent forms explicitly acknowledge humans as inventors, and they do not apply to AI applications or devices unless explicitly stated.

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

There are currently no specific regulations for government-funded inventions.

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

There are no specific cases for digital health innovations yet.

7 Commercial Agreements

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

In order to guarantee the success of collaborative improvements, it is possible to evaluate a number of factors, such as the primary objectives of the collaboration, information regarding all eligible members and parties involved, governance and contract management, confidentiality, an evaluation of the current intellectual property and technology transfer procedures, and data on existing intelligence.

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

Healthcare and non-healthcare organisations adhere to profoundly distinct workflow methodologies and principles with respect to internal communication and the provision of services externally. However, client fulfilment is the primary concern in both sectors. It is imperative to assess the confidentiality protocol for data exchange, data protection, security and privacy, in addition to the approaches to information sharing, when reviewing agreements.

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

It is essential to monitor and analyse the design, consistent protocols for data collection, structured reporting, and advanced methodologies for detecting bias and concealed stratification. Furthermore, it is imperative to execute a non-disclosure agreement.

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

Companies should avoid integrating sensitive information or personal data into generative AI tools. Data protection regulations may prohibit the input of such data into a generative AI tool, or it may violate a third-party confidentiality agreement. Furthermore, it is imperative to safeguard the privacy of data and its interpretation.

8 Artificial Intelligence and Machine Learning

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

India currently lacks a regulator with a specific focus on AI/machine learning (ML). As a result, the Ministry of Electronics & Information Technology serves as the executive agency responsible for AI-related strategies and has established committees to establish a policy framework for AI. India has programmes and recommendations for responsible AI development, but no AI legislation exists. The NITI Aayog provides guidelines, and the National Strategy for Artificial Intelligence outlines AI research for various sectors. The DPDP Act was passed in 2023, and the Global Partnership on Artificial Intelligence includes India. Indian authorities are developing AI rules and drafting AI standards, focusing on climate change, global health and societal resilience.

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

There are currently no regulatory schemes that are specific to the situation. No specific legislation addresses AI in healthcare. We anticipate that the implementation of the DISHA in India will address certain issues. The legal system, clinicians and patients may interpret the law contextually and hold varying perspectives in the final analysis.

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

This is not currently applicable in India. Furthermore, algorithms are not patentable in India.

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

The authenticity of licensed data, permission for multiple users and beneficiaries, consideration for purposes such as "know your customer", restriction and limited access across multiple locations and multiple users, data privacy and security, quality, user rights, and term and termination are all important factors to consider.

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

There are no specific regulations yet and accordingly the practical insights have yet to come.

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

Companies should refrain from incorporating sensitive information or personal data into generative AI tools. Data protection regulations may prohibit the entry of such data into a generative AI tool, or it may contravene a confidentiality agreement that was granted to a third party. Additionally, it is crucial to preserve the privacy of data and its interpretation. There are no specific regulations for generative AI yet.

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

Though there is no specific model or guidelines yet, the usual rules under data protection are applicable, such as operations that involve these technologies must adhere to standard IT laws and regulations in India, as there are no specific AI, cloud computing or ML regulations. It would be advantageous to establish a confidentiality agreement between the licensee and the data proprietor, as well as a strategy for the data's utilisation.

9 Liability

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

The liability for negative consequences may be civil or criminal, and it varies between service providers, such as institutes and internet service providers, and service practitioners. In addition to filing a legal complaint, the Consumer Protection Act can implement its remedies in civil proceedings. In the event of a doctor's negligence, a consumer may also submit a complaint to the ethics committee of the Medical Council of India. The Indian Penal Code, an essential component of digital health solutions, also addresses criminal responsibility.

9.2 What cross-border considerations are there?

It is important to use data programs and customise data.

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

The process entails the following: the establishment of work groups to supervise it; the education and training of leaders; the definition of AI policy; the revision of privacy policy; and the execution of security assessments. Confidentiality and privacy should also be maintained.

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

There are no specific models/theories yet.

10 General

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

A persistent concern in the field of digital health is the exorbitant cost of developing and maintaining health information technology, as well as the preservation of confidentiality and privacy when storing data. Another factor to consider is the security and privacy of data management during the different stages of the transformation process.

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

It is imperative that non-healthcare businesses comprehend the healthcare industry's commitment to secure manufacturing and marketing standards, as well as its exceptional financial planning and data protection and security measures. Additionally, the healthcare sector is subject to consumer protection laws.

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

Venture capital and private equity firms should evaluate numerous critical factors prior to investing in digital healthcare enterprises. These encompass a comprehensive business plan, strategic relationships, market opportunities, an understanding of the company's financial and key metrics, potential risk, an estimated valuation, regulatory compliance and intellectual property protection.

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

The key impediments to the widespread implementation of digital health technology in clinical settings are data interoperability, particularly for health records, data security and privacy.

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

Currently, there are no such certifying bodies.

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

There are currently no explicit reimbursement standards or formal accreditation for solution providers.

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

Some of the primary obstacles to the successful implementation of digital transformation in healthcare organisations include data security, resistance to change, high implementation costs and a remote workforce.

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

India is anticipated to experience growth in a diverse range of industries, such as genomics, wearables, telemedicine and personalised medicine. Healthcare providers and organisers are adopting advanced technologies, including AI, cloud computing, extended reality and the IoT, in order to create and distribute innovative treatments and services. These technologies facilitate the development of personalised and data-driven medical remedies, as well as improved healthcare delivery and patient experiences. The government is actively building a fully integrated digital health ecosystem.

Digital health records necessitate effortless accessibility without the need for paper. Government initiatives in India, such as the NDHM and Made in India, are accelerating the pace of healthcare digitisation. As the government prioritises digital innovation, healthcare manufacturers and companies will benefit from an increase in opportunities, which will further enhance patient outcomes. The NDHM dedicates itself to developing the necessary infrastructure for the establishment of the nation's integrated digital health ecosystem. The healthcare industry in India is currently experiencing a digital revolution, as evidenced by these patterns. They have the capacity to enhance the delivery of healthcare, patient outcomes and care access. It is imperative to resolve concerns such as infrastructure shortages, data protection, legislative frameworks and equitable access.

Manisha Singh is the Founder Partner of LexOrbis. Manisha is known and respected for her strong expertise in prosecution and enforcement of all forms of IP rights and for strategising and managing global patents, trademarks and designs portfolios of large global and domestic companies. She is also known for her sharp litigation and negotiation skills for both IP and non-IP litigations and dispute resolution. She is involved in a large number of IP litigations with a focus on patent litigations covering all technical fields – particularly pharmaceuticals, telecommunications and mechanics. She is an active member of many associations such as INTA, APAA, AIPLA, AIPPI, LES and FICPI, and is actively involved in their committee work. She is an active writer and regularly authors articles and commentaries for top IP publications.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi 110001
India

Tel: +91 11 2371 6565
Email: manisha@lexorbis.com
LinkedIn: www.linkedin.com/in/manisha-singh-509b698

Dr. Pankaj Musyuni is an Advocate registered with the Bar Council of India and a Patent Agent. Having over 13 years of experience in handling taxonomy of invention, particularly in portfolio management such as the life cycle of the invention, including preliminary patentability assessment, drafting, filing, prosecution, oppositions and pre-grant representations and leading efforts for understanding requirements of domestic and international clients. Pankaj has experience in handling patent applications in the areas related to chemical, pharmaceutical, agrochemical and biotech domains. He also has experience in handling documentation and assisting in regulatory audits related to GMP, ISO and FDA requirements for the pharmaceutical, veterinary, FMCG and pesticide sectors.

LexOrbis
709–710 Tolstoy House
15–17 Tolstoy Marg
New Delhi 110001
India

Tel: +91 11 2371 6565
Email: pankaj@lexorbis.com
LinkedIn: www.linkedin.com/in/pankaj-musyuni-b34631258

iclg International Comparative Legal Guides

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

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

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

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