Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Digital Healthcare 2021

India
Anoop Narayanan and Sri Krishna
ANA Law Group

practiceguides.chambers.com

INDIA

Law and Practice

Contributed by:
Anoop Narayanan and Sri Krishna
ANA Law Group see p.15

CONTENTS

1. DIGITAL HEALTHCARE OVERVIEW

1.1 Difference between Digital Healthcare and Digital Medicine

Although the concepts of "digital health" and "digital medicine" have been operational in India for some time and their growth has been increasing in the past couple of years due to the COVID-19 pandemic, from a legal and regulatory perspective, these concepts are not defined under the existing Indian laws. Digital health is understood as defined by the World Health Organization as a broad umbrella term encompassing eHealth, as well as emerging areas, such as the use of advanced computing sciences in big data, genomics and artificial intelligence. The digital health platforms include the information and communication tools (digital medicine products) used for improving and enhancing healthcare services.

1.2 Regulatory Definition

Existing Indian laws do not define the terms "digital health" or "digital medicine". However, the proposed law in this regard, which is the Digital Information Security in Healthcare Act, 2018 (the DISHA Bill) defines "digital health data" as an electronic record of health-related information about an individual, including information regarding:

- an individual's physical and mental health condition;
- health service provided to an individual;
- the donation by an individual of any body part or any bodily substance;
- testing and examination data of an individual's body part or bodily substance;
- data collected in the course of providing health service to an individual; or
- details of the clinical establishment accessed by an individual.

Further, the Telemedicine Practice Guidelines (TPG), issued by the Government of India in March 2020, has adopted the World Health Organization's definition of telemedicine as "The delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities."

1.3 New Technologies

The following are some of the key emerging technologies in India in the field of digital healthcare.

Telemedicine

There has been significant growth and advancement in the field of telemedicine in India. This includes the use of information and communications tools for healthcare services with the virtual presence of both the patient and the healthcare-provider. The tools are used for carrying out technology-based patient consultation communication via video, audio and text. The Ministry of Health and Family Welfare of India (MoHFW) issued the TPG in March 2020.

Wearable Devices

India has witnessed a tremendous increase in the use of wearable devices for health monitoring. Although these digital technologies have existed and have been used for several years, their use for more specific purposes, and also as an alternative to the conventional physical health monitoring, has increased because of the COVID-19 pandemic. The preliminary screening of one's health data without having to visit a hospital or a diagnostic centre has been a major support and growth for digital technologies. Several wearable devices are now available in India, featuring heart-rate trackers, blood oxygen-level

tracker, and other parameters, including water consumption, weight, sleep, diet, etc.

Online Pharmacies

Online delivery of medicines to the patient's doorstep. There has been a significant rise in the number of online pharmacies in India, more so during the pandemic.

Artificial Intelligence (AI)

AI-based systems have witnessed significant growth in India for the diagnosis of disease and also for treatment purposes.

1.4 Emerging Legal Issues

One of the major emerging issues is that the increasing number of digital and other new technologies in the health care industry is giving rise to concerns on data protection and the privacy of patients.

Although most of the data collection, storage and usage by healthcare-providers will comply with India's applicable data privacy laws, there are critical issues on the misuse of this data for other commercial purposes and also the breach of privacy obligations. The absence of adequate training and awareness-building with regard to aspects of data privacy among the people collecting, processing and handling such data on the digital health platform also aggravates the situation.

Additionally, the absence of a specific law to regulate these aspects is a major concern. Although the MoHFW has issued the DISHA Bill, it has not as yet become the law. The DISHA Bill proposes to establish national and state health authorities to enforce privacy and security measures for health-related data. Further, the MoHFW has issued a Health Data Management Policy to promote National Digital Health Mission, which lays down principles for the protection of an individual's digital health data privacy.

1.5 Impact of COVID-19

COVID-19 has led to a significant rise in the adoption and use of digital healthcare technologies in India, especially in the telemedicine area. As non-COVID-19 patients were forced to stay at home during the nationwide or state-specific lockdowns, healthcare practitioners provided remote consultations with the help of video/audio calls and text messages. Technology-based consultations, remote monitoring and treatments were also extended to COVID-19 patients with mild symptoms and where hospitalisation was not required. As one of the measures to support telemedicine, the MoHFW issued the TPG in March 2020 as a temporary measure, and allowed doorstep delivery of medicines. The Government of India also came up with a mobile application, Aarogya Setu, to trace COVID-19 hotspots in India and the number of people affected with COVID-19 in a particular user's geographical area. The government has also recently introduced another digital application, the CO-WIN portal, to carry out the COVID-19 vaccination drive in India.

2. DIGITAL HEALTHCARE AND CLIMATE CHANGE

2.1 Digital Healthcare and Public Health Dangers Related to Climate Change

Digital healthcare technologies, such as those monitoring temperature variations, air and other types of pollution, climate change-based variations in disease-carrying insects, health data sensors, wearable devices and other similar tools, may help diagnose diseases that are a consequence of climate change.

3. HEALTHCARE REGULATORY ENVIRONMENT

3.1 Healthcare Regulatory Agencies

The MoHFW

The MoHFW is the apex authority in the organisational structure of the healthcare system in India. The MoHFW is comprised of two departments, (i) the Department of Health and Family Welfare (DoHFW), which is responsible for organising and delivering all national health programmes; and (ii) the Department of Health Research (DoHR), which is responsible for the promotion of health and clinical research, development of health research and ethics guidelines, grants for research trainings, etc, in India.

The AYUSH

The Ministry of Ayurveda, Yoga and Naturopathy, Unani, Siddha and Homeopathy (AYUSH) develops and promotes research in alternative medicine practices. The central government's responsibilities include policy-making, planning, guiding, assisting, evaluating and co-ordinating the work of the various state-level health authorities, and providing funding to implement national health programmes.

The Central Drugs Standard Control Organisation

The Central Drugs Standard Control Organisation (CDSCO) is the National Regulatory Authority of India, and is responsible for the approval of drugs, conducting clinical trials, laying down the standards for drugs, and control over the quality of imported drugs in India. The Drug Controller General of India (DCGI) is the head of the CDSCO and is responsible for licensing and controlling the functions of the CDSCO.

The National Medical Commission and the National Health Authority

The recently constituted National Medical Commission (NMC) regulates and governs the medical practice in India. Besides these, the MoHFW has recently established the National Health Authority (NHA), which is the apex body responsible for implementing public health assurance schemes, to design strategy, build healthcare technological infrastructure and implement the "National Digital Health Mission" in India. Additionally, the MOHFW proposes to establish the National Digital Health Authority (NDHA), which will be responsible for developing a health-data system for telemedicine and other digital healthcare mechanisms in India. The NDHA will also be primarily responsible for regulating and maintaining eHealth and patient health-data privacy and security in India. Also, the Department of Telecommunications governs the applications of service-providers, including telemedicine service-providers, in India.

The National Pharmaceuticals Pricing Authority

The National Pharmaceuticals Pricing Authority (NPPA) is the authority for controlling and monitoring the prices and availability of medicines.

State-Level Authorities

At the state level, each state has separate Ministries of Health and Family Welfare, Directorates of Healthcare Services and Departments of Health and Family Welfare, which are responsible for organising and delivering healthcare services, consisting of participants from both the public and private sectors. The State Drug Standard Control Organisation (SDSCO) is responsible for regulation of the manufacture, sale and marketing of drugs in each of the Indian states.

The organisational structure consists of administrative subordinate offices at regional/zonal, district and sub-district level. The public healthcare

system consists of primary (community health centres), secondary (sub-district hospitals), and tertiary (district hospitals and medical colleges) care centres. Primary and secondary care hospitals are in the public sector, whereas the tertiary care hospitals arein either the public or private sector. Apart from these, there are several clinics and diagnostic centres set up by individual medical practitioners.

The services provided by the private sector are registered and regulated under national/state councils constituted under the Clinical Establishment (Registration and Regulation) Act, 2010, while the public sector comes under the authority of the MoHFW and state health ministries. At the district level, Panchayati Raj institutions (local self-government bodies) are responsible for establishing primary health centres in rural areas.

3.2 Recent Regulatory Developments

The following are the key regulatory developments pursuant to the rise of digital healthcare in India and which are expected to create the most impact for the governance and the growth of digital healthcare:

- the Government of India issued the Telemedicine Practice Guidelines (TPG) in March 2020, which covers the norms and standards of registered medicine practitioners to consult patients via telemedicine. Telemedicine includes all channels of communication with the patient that leverage information technology platforms, including voice, audio, text, and digital data exchange;
- the government proposed the DISHA Bill in 2018 to standardise and regulate the processes related to the collection, storing, transmission and use of digital health data, and to ensure the reliability, data privacy, confidentiality and security of that digital health data;
- the government also issued the Health Data Management Policy in October 2020 to impose standards for data privacy protection in India.

These regulations will address many ambiguities from the legal, regulatory and compliance perspectives, for the service-providers as well as the consumers. More accountability, governance and grievance-redressal mechanisms which have comparable speed, ease and efficiency to that of the digital healthcare services are some other primary needs for this sector.

3.3 Regulatory Enforcement

The MoHFW enforces laws relating to healthcare in India. The National Medical Commission enforces the provisions related to medical education and practice under the National Medical Commission Act 2019.

The CDSCO and the SDSCO enforce regulations relating to the import, manufacture, distribution and sale of drugs and cosmetics under the Drugs and Cosmetics Act 1940 (DCA). The central government can confiscate, regulate or restrict or prohibit the manufacture, sale or distribution of some drugs and impose a ban on certain drugs. The court can further impose penalties and sentence of imprisonment for offences under the DCA.

4. NON-HEALTHCARE REGULATORY AGENCIES

4.1 Non-healthcare Regulatory Agencies, Regulatory Concerns and New Healthcare Technologies

Currently, there are no digital healthcare-specific non-healthcare regulatory agencies.

The new healthcare technologies, while providing fast and convenient services to the con-

sumers, pose several questions and concerns as well. In addition to the protection under consumer protection laws, more specific regulatory regime with respect to data privacy and an expert regulatory body in each state, as well as at the national level for grievance redressal, are some of the immediate requirements.

5. SOFTWARE AS A MEDICAL DEVICE

5.1 Categories, Risks and Regulations Surrounding Software as a Medical Device Technology

The MoHFW issued a notification on 11 February 2020 (the 'MoHFW Notification') specifying that medical devices be treated as drugs with effect from 1 April 2020. Therefore, all the regulations and compliances applicable for drugs are also applicable for medical devices. The MoHFW Notification stipulates that medical devices include an instrument, apparatus, appliance, implant, material or other article, including a software or an accessory for the purposes of:

- diagnosis, prevention, monitoring, treatment or alleviation of any disease or disorder;
- diagnosis, monitoring, treatment, alleviation or assistance for, any injury or disability;
- investigation, replacement or modification or support of the anatomy or of a physiological process;
- supporting or sustaining life;
- disinfection of medical devices;
- control of conception.

The DCGI is responsible for the administration and approval of manufacturing, importing or marketing of medicinal products and medical devices in India. As the medical device now includes software, the DCGI is also responsible for software as a medical device. The DCA and the Drugs and Cosmetics Rules 1945 (DCR), and the Medical Devices Rules 2017 (MDR) govern approvals and categorise whether a product is categorised as a drug or any other category.

The CDSCO classifies the medical devices into four main categories, based on the risk of use.

However, currently, there are no specific regulatory frameworks or guidelines to categorise or classify software as a medical device in India. Therefore, it is difficult to ascertain which computer software/mobile application qualifies software to be a medical device, which is a common challenge faced by application service-providers, developers and stakeholders in India.

Similarly, there is no clarity whether the Prices Control Order, which is applicable for drugs, will also apply to medical software applications, and whether they will be able to control of the prices of their digital health-related software products.

Also, there is currently no specific legal framework for software based on AI and machine learning in India.

It is the common consensus of stakeholders in India that the government should adopt effective regulatory frameworks based on risk of use, and AI/machine learning, similar to the International Medical Device Regulation Forum's (IMDRF) medical software device framework and the US FDA's Artificial Intelligence and Machine Learning (AI/ML) Software as a Medical Device Action Plan.

6. TELEHEALTH

6.1 Role of Telehealth in Healthcare

India follows the definition of "telehealth" in the New England Journal of Medicine (NEJM) Catalyst, which defines "telehealth" as the delivery and facilitation of health and health-related

services including medical care, provider and patient education, health information services, and selfcare via telecommunications and digital communication technologies. Telehealth is a broader term used for technology for health and health-related services, including telemedicine.

Telehealth is a solution for providing timely and faster access. It will also reduce costs and efforts associated with travel, especially for people in rural India. Telehealth plays an important role where there is no need for patients to physically visit a hospital or a doctor. The telecommunication technologies can also maintain records of a patient's health history, and can help patients to manage their medication and diseases better. Telehealth has proven to be an advantageous solution in India, especially during the COVID-19 pandemic.

There have been various efforts made to promote telehealth in India. The India Virtual Hospital, a medical technology service in India, launched the Patient Care App, which enables doctors to track a patient's health and recovery. Another health-tech company has recently launched an online platform, iCliniq, where users can get medical advice from doctors/medical practitioners, physicians and therapists from the US, the UK, UAE, India, Singapore, Germany, etc, using emails, chats, video and audio calls. Another Indian company set up a virtual hospital for cancer patients in 2019 for online consultation, treatment planning, and cancer treatment management.

6.2 Regulatory Environment

India currently does not have specific legislation which regulates telehealth or the use of online platforms in respect of telehealth.

As a result of the COVID-19 pandemic in India, the Government of India has issued the Telemedicine Practice Guidelines (TPG). These guidelines are issued to enhance healthcare services and enable access to all. The guidelines are meant for registered medical practitioners and prescribe the norms and standards to consult patients, including all channels of communication with the patient that leverage IT platforms, including voice, audio, text and digital data exchange.

The guidelines specifically exclude specifications for hardware or software, infrastructure building and maintenance, data management systems that are involved, standards and interoperability, the use of digital technology to conduct surgical or invasive procedures remotely, other aspects of telehealth such as research and evaluation and the continuing education of healthcare workers and consultations outside the jurisdiction of India.

These guidelines mandate a registered medical practitioner to obtain consent from the patient before the telemedicine consultation. If the patient voluntarily initiates the telemedicine consultation, the consent is implied.

The principles regarding medical ethics, data privacy and confidentiality will apply to the registered medical practitioners.

6.3 Payment and Reimbursement

The TPG prescribes that the telemedicine consultations must be treated the same way as in-person consultations, from a fee perspective. The registered medical practitioner must also provide a receipt/invoice for the fee charged for providing the telemedicine consultation.

7. INTERNET OF MEDICAL THINGS

7.1 Developments and Regulatory and Technology Issues Pertaining to the Internet of Medical Things

The internet of medical things (IoMT) includes digital medical devices and software applications used to provide effective and efficient services to patients, and reduce the cost of healthcare. Recent technologies such as sensors, wearable devices, health apps, telemedicine, artificial intelligence, oxygen and heart detectors, etc, are in extensive use in India. The IoMT technologies make it easier for doctors and medical practitioners to track the progress of treatment and recovery in real time.

The rise of COVID-19 has led the medical establishment to urge people to adopt the IoMT for tele-consultations, remote monitoring and treatment of patients, eliminating the hospital visits. The Government of India has encouraged hospitals to adopt EHR (electronic health records) which will contain the patient's health history and records.

An increase in IoMT technologies also brings an increase in the data privacy risks and issues, due to a lack of adequate and specific regulations, a lack of awareness among the users and the service-providers' lack of compliances in the absence of a comprehensive legal framework in the country. Technological issues such as the compatibility of hardware and software with cloud services is also an factor to be taken into consideration.

8. 5G NETWORKS

8.1 The Impact of 5G Networks on Digital Healthcare

The 5G network is expected to be launched in India in 2021 or 2022. The higher speed and connectivity and low latency in the 5G network may boost the advanced telehealth solutions in India and improve the healthcare system in India. The 5G network will ensure more effectiveness and efficiency in tele-consultations and remote monitoring of patients and the handling of patients health data.

The 5G network can help more in the rural areas of the country where the telecom infrastructure has inadequacies, for faster transmission of large health data files, high-quality video/audio telecommunications between the doctors and the patient, improve the use of augmented and virtual reality and enhance the use of artificial intelligence in healthcare devices.

9. DATA USE AND DATA SHARING

9.1 The Legal Relationship between Digital Healthcare and Personal Health Information

The personal information relating to a person's health is categorised as sensitive personal information under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (the Privacy Rules). The Privacy Rules lay down mandatory principles of data privacy to be followed by the body corporates that are handling and processing sensitive personal information. The primary requirement for body corporates under the Privacy Rules is to obtain a written consent from the information-provider before collecting and processing the sensitive personal data. Prior consent is also required for

sharing the sensitive personal data with third parties.

The information-provider must be informed of the fact that the sensitive personal data is being collected, the intended purpose of its use and whether it will be transferred to any third parties, along with the contact details of the agency collecting the information. It is also mandatory under the Privacy Rules for the body corporates to have a privacy policy containing the type of sensitive personal information collected, the purpose of collection, disclosure of that information, and the reasonable security practices and procedures to be implemented by the body corporates. India does not as yet have a comprehensive data protection law. However, the government had issued the Personal Data Protection Bill, 2019 (PDP Bill), which is intended to become a comprehensive data protection law in the country.

There is no separate legislation in India to regulate data privacy issues for digital health. However, the proposed DISHA Bill aims to address the data privacy issues relating to digital health in India, which is mostly based on the principles laid down under the PDP Bill. The MoHFW has also issued the Health Data Management Policy, which lays down principles for the protection of an individual's personal digital health data privacy.

The DISHA Bill proposes that a clinical establishment may, by obtaining written (on paper or in electronic form) consent (in a prescribed manner) from the owner, and lawfully collect the required health data, after informing the owner of the data of the following:

- the rights of the owner, including the right to refuse to give consent to the generation and collection of their data;
- the purpose of the collection of their health data;
- the identity of the recipients to whom the health data may be transmitted or disclosed, after being converted into a digital format; and
- the identity of the recipients who may have access to that digital health data, on a need-to-know basis.

Further, the clinical establishment or any other entity must furnish a copy of the consent form to the owner of the data.

The current regulations do not specifically regulate the sharing of personal health data by a wearable healthcare device.

The Privacy Rules do not prescribe for de-identification or anonymisation of data. However, the DISHA Bill and Health Data Management Policy defines "anonymisation" as the process of permanently deleting all personally identifiable information from an individual's digital health data, and defines "de-identification" as the process of removing, obscuring, redacting or de-linking all personally identifiable information from an individual's digital health data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and that, if necessary, makes it possible for the data to be linked to the owner again.

The DISHA Bill proposes that de-identified or anonymised data must be used only for the following purposes:

- to improve public health activities and facilitate the early identification and rapid response to public health threats and emergencies, including bio-terror events and infectious disease outbreaks;
- to facilitate health and clinical research and healthcare quality;

- to promote the early detection, prevention, and management of chronic diseases;
- to carry out public-health research, review and analysis, and policy formulation; and
- to undertake academic research and other related purposes.

The Health Data Management Policy prescribes that data fiduciaries may make anonymised or de-identified data in an aggregated form available for the purpose of facilitating health and clinical research, academic research, archiving, statistical analysis, policy formulation, the development and promotion of diagnostic solutions and any other purposes that may be specified by the National Digital Health Mission (NDHM).

The NDHM must set out a procedure through which any entity seeking access to anonymised or de-identified data will be required to provide relevant information, such as its name, purpose of use and nodal person of contact and, subject to approval being granted under this procedure, the anonymised or de-identified data must be made available to that entity on whatever terms may be stipulated on its behalf.

Any entity which is provided access to de-identified or anonymised data must not, knowingly or unknowingly, take any action which has the effect of re-identifying any data principal or the effect of any such data no longer remaining anonymised.

The data fiduciary that is undertaking to anonymise or de-identify data must be responsible for ensuring compliance with the procedure for the anonymisation or de-identification as set out by the NDHM. The de-identification or anonymisation of data by a data fiduciary must be done in accordance with technical processes and anonymisation protocols which may be specified by the NDHM. The technical processes and anonymisation protocols must be periodically reviewed by the NDHM.

The Information Technology Act, 2000 prescribes that a body corporate, possessing sensitive personal data that is negligent in implementing and maintaining reasonable security practices and procedures, will be liable to pay damages by way of compensation. It also prescribes that if a body corporate has obtained sensitive personal data without the consent of the information-provider, and discloses the information to any other person, it will be punishable with a term of imprisonment for a maximum of two years or with a maximum fine of INR100,000 (approximately USD1,400), or both.

10. AI AND MACHINE LEARNING

10.1 The Utilisation of AI and Machine Learning in Digital Healthcare

New technologies are emerging in the digital health sector in India, including artificial intelligence/machine learning. Currently, India does not have any legislation to regulate technologies such as artificial intelligence/machine learning. However, the TPG prescribes that the telemedicine platforms based on artificial intelligence/machine learning are not permitted to counsel patients or prescribe any medicines to a patient. The technologies such as artificial intelligence, the Internet of Things and advanced data science-based decision support systems may be used only to assist and support the clinical decisions of the registered medical practitioner. In all cases, the final prescription or counselling must be delivered directly by the registered medical practitioner.

With the growth of artificial intelligence technologies in India, the Government of India authorised the public policy think tank the NITI Aayog (the

National Institution for Transforming India commission) to address strategy on artificial intelligence-based technologies/machine learning in agriculture and health sector. In June 2018, the NITI Aayog issued a discussion paper on national strategy for artificial intelligence for healthcare, agriculture, education, smart cities and infrastructure and smart mobility and transportation. The discussion paper recognised artificial intelligence combined with robotics and the internet of medical things as the new nervous system for healthcare in India, presenting solutions to address healthcare problems. Currently, the NITI Aayog is reportedly working with a large Indian hospital, the Tata Memorial Centre, to launch a digital pathology and imaging bio-bank for cancer detection.

The artificial intelligence/machine-learning technologies use and share medical conditions of a patient with the doctors/medical institutions, which is considered as sensitive personal data under the Privacy Rules. The Privacy Rules prescribe mandatory compliance of principles of data protection by body corporates which handle, store and process sensitive personal data.

In February 2021, the NITI Aayog issued principles for responsible artificial intelligence. The NITI Aayog has stated that the artificial intelligence solutions must comply with the principles of data protection laid down in the PDP Bill, such as consent, purpose limitation, rights to the information-provider, etc. Artificial intelligence solutions must maintain the privacy and security of medical information/data, which is sensitive personal data, and ensure sufficient safeguards.

Electronic health records can ensure the easy accessibility of a patient's records from anywhere at any time, easy storage, and can help in tracking the patient's progress. The DISHA Bill and Health Data Management Policy also promote electronic health records. The Government of India issued recommendations in 2016 on different EHR (electronic health records) standards for different purposes in respect of electronic health records. For example, ISO/TS 22220:2011 Health Informatics – Identification of Subjects of Health Care must be undertaken for obtaining basic identity details of patient, ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment must be undertaken to maintain basic data security and privacy requirements, and ISO TS 14265:2011 is for processing personal health information, etc.

The 2016 EHR standards recommendations stipulate that only those persons, including organisations, duly authorised by the patient may view the recorded data or part thereof. The term "security" refers to all recorded personally identifiable data, which will at all times be protected from any unauthorised access, particularly during transport (eg, from healthcare provider to provider, healthcare-provider to patient, etc). The term "trust" refers to that person, persons or organisations (doctors, hospitals, and patients). The 2016 EHR standards recommendations are based on the principles of data protection laid down under the Privacy Rules.

11. UPGRADING IT INFRASTRUCTURE

11.1 IT Upgrades for Digital Healthcare

As demonstrated in the preceding paragraphs, India is developing and adopting various technologies in the fields of telehealth, machine learning/artificial intelligence and the Internet of Things in order to adopt the digital healthcare system in India. India requires high-speed broadband networks such as 5G to support such high-end technologies. The IT infrastructure must be able to manage and secure large amount of health data collected by the devices.

Besides this, India requires a comprehensive data privacy and protection law to address the privacy and security risks relating to digital health data.

11.2 Cloud Computing

India has seen a rapid increase of cloud computing technology, such as telemedicine due to the COVID-19 pandemic. As non-COVID-19 patients were forced to stay at home during the nationwide shutdown, healthcare practitioners provided remote consultations with the help of video/audio calls and text messages. Over this period of time, the technology-based consultations were also extended to those COVID-19 patients with mild symptoms and to those for whom hospitalisation was not required. Due to the lack of a comprehensive data protection law in India, the issues relating to data protection and data privacy of digital health data need to be addressed.

12. INTELLECTUAL PROPERTY

12.1 Scope of Protection

Indian intellectual property laws allow for the protection of patents, copyrights, trade marks and designs. From the digital health standpoint, the key areas of development are in the field of software.

Patents Act 1970 (Patents Act)

In India, patents are examined, granted and administered by the Patents Act, which complies with the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement. India is also a signatory to the Paris Convention, in addition to the Patent Co-operation Treaty. A digital health mechanism is essentially a software/computer program. Although the Patents Act excludes protection for standalone computer programs (Section 3(k) of the Patents Act), a piece of software claimed in conjunction with a novel hardware element will be patentable in India (Guidelines for Examination of Computer-Related Inventions 2017). Further, the Delhi High Court has recently held that a computer program that demonstrates a technical effect or a technical contribution will be patentable in India. Software patents are subject to other restrictions under the Patents Act, including Section 3(i) of the Patents Act, which excludes patent protection for any process for medicinal, surgical, curative or other treatment of human beings or animals.

The Patent Office has granted several patents for software programs that involve the hardware elements. Therefore, digital health mechanisms, including computer software/programs embedded in mobile software applications, wearable devices, etc, may be protected in India, as long as they involve a novel hardware element.

Copyright Act 1957 (CRA)

The CRA provides for copyright protection in India. The CRA provides that a copyright subsists in the form of original literary, dramatic, musical or artistic work, cinematograph films and sound recordings. Although copyright registration is not mandatory for protection in India, a copyright registration will serve as an evidence of the copyright in the work. The CRA covers computer programs under the purview of literary work, and therefore, the literary portions of a computer program, including the source code, are protected under the CRA.

Trade Secrets

Currently, there is no legislation or statutory protection for trade secrets in India. However, different courts in India have extended protection for trade secrets and confidential information in India, provided that information's confidentiality is reflected in contractual documents, such as Confidentiality Agreements, Non-Disclosure

Agreements and reasonable and legally enforceable non-compete clauses in the agreements.

Finally, there is no specific legislation or statutory protection for databases in India, nor in respect of data and databases used in machine learning. However, the CRA provides protection to a computer database under the purview of literary work. The CRA also provides protection for databases, by granting rights associated with the labour involved in compiling and presenting data in a particular form.

12.2 Research in Academic Institutions

The ownership of IP in India varies under different IP laws. As regards copyright, the employer (university or healthcare institution) will be the first owner of the copyright, not the physician or inventor. However, this will not apply in the case of an independent contractor-developed copyright. As regards the patents, the inventor will be the first owner, irrespective of whether it is an employee or a contractor.

12.3 Contracts and Collaborative Developments

In India, the institutions or universities or employers enter into development agreements with their employees. Standard development agreements normally provide that all the IP developed by the employees/inventors/researchers under the agreement will be assigned to and owned by the employers.

13. LIABILITY

13.1 Patient Care

The TPG prescribes that the platforms based on artificial intelligence/machine learning are not permitted to counsel patients or prescribe any medicines to a patient. However, technologies such as artificial intelligence, the Internet of Things and advanced data science-based decision support systems may be used only to assist and support the clinical decisions of the registered medical practitioner. In all cases, the final prescription or counselling has to be delivered directly by the registered medical practitioner. Therefore, the liability falls on the doctors or other medical service-providers. Consumers can claim compensation from doctors/hospitals under the Consumer Protection Act, 2019. Criminal liability can be imposed on the doctors, on grounds such as causing death by negligence, an act endangering the life or personal safety of others, causing hurt by an act endangering the life or personal safety of others and causing grievous hurt by an act endangering the life or personal safety of others.

13.2 Commercial

The third parties supplying products and services to healthcare institutions can be imposed with civil and criminal liabilities, penalties and also actions under the Consumer Protection Act 2019, and can be held liable for penalties prescribed under the IT Act for data breach.

14. HOT TOPICS AND TRENDS ON THE HORIZON

14.1 Hot Topics That May Impact Digital Healthcare in the Future

India is currently waiting for the parliament to enact the PDP Bill. After the enactment of this comprehensive data protection law in the country, the government will adopt the principles of data protection from the PDP Bill and enact the DISHA Bill and the Health Data Management Policy, which will impact significantly the medical and pharmaceutical industries by introducing comprehensive laws on digital healthcare in India.

ANA Law Group is a full-service law firm based in Mumbai; its team of experienced and committed professionals has broad industry knowledge and specialises in a wide spectrum of laws. Founded on traditional values, with prominent cross-border exposure and a solution-oriented approach, the firm provides significant value to clients internationally, acclaimed for its client servicing model, each client receiving the required attention to provide practical legal solutions. The firm has significant experience in counselling international clients on data protection and privacy in India, acting for many businesses in complicated transactions, thus attaining in-depth knowledge of all aspects of industries such as banking and insurance, financial institutions, luxury goods, consumer goods, and healthcare. In addition to data protection and privacy, the firm assists international companies on global privacy law involving Indian projects, drafting and negotiating contracts with their Indian counterparts, preparing data protection and privacy policies for those companies' Indian subsidiaries, compliant with major international privacy laws. Specifically, the firm advises clients on data processing and all aspects of data security, including handling cross-border data flows, security breaches and compliance with all regulatory requirements.

AUTHORS

Anoop Narayanan is a leading Indian lawyer in corporate law, intellectual property law, and information technology with more than 27 years of experience as an attorney. Focusing on a broad range of intellectual property, IT, outsourcing, employment, technology, data protection, telecommunications and entertainment law matters, his practice encompasses both litigation and commercial or transactional advice. He has worked with India's highest-profile companies, as well as global corporates in the manufacturing industries, banking and finance sectors, and telecommunications and technology companies. His experience and expertise in TMT and data privacy was invaluable in setting up the Indian operations of large global technology companies and handling several India-bound outsourcing transactions with the major Indian IT companies. He and his team assist many international clients, advising multinational banks on Indian privacy and data protection law, outsourcing, bank secrecy, and related matters in connection with outsourcing transactions. He has spoken at several Indian and international forums on his areas of practice and has published many articles on several areas of Indian law.

Sri Krishna is an associate working in the firm's TMT and IP practice group. He regularly advises international clients on intellectual property, healthcare and pharmaceuticals-related issues in transactional, compliance and regulatory matters.

ANA Law Group

303 Madhava Premises
Bandra Kurla Complex
Bandra East
Mumbai
400 051
India

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: anoop@anaassociates.com
Web: www.anaassociates.com

Trends and Developments

Contributed by:
Anoop Narayanan and Sri Krishna
***ANA Law Group** see p.23*

Introduction

The past year has been one of the most challenging years for the Indian healthcare industry and economy alike, amid the COVID-19 pandemic. Unfortunately, the Indian healthcare sector and frontline workers continue to face many challenges with the second wave of COVID-19, which hit India around the last week of March 2021.

However, on the bright side in the healthcare sector, the pandemic has led to an unprecedented rise in the adoption and use of digital healthcare technologies in India, as discussed below.

Emerging Technologies in Digital Healthcare in India

Telemedicine

Telemedicine has introduced in India the use of various information and communications tools for healthcare services, with the virtual presence of both the patient and the healthcare-provider. Telemedicine includes the tools used for carrying out technology-based patient consultation communication via video, audio and text. Although telemedicine has been in use in India for quite some time, the coronavirus pandemic has given a significant push to telemedicine. A survey from Practo, a popular Indian health-tech company, has recently estimated that there was a 67% dip in clinic visits and a massive 500% growth in online medical consultations just between 1 March 2020 and 31 May 2020.

As regards the regulatory framework, the Ministry of Health and Family Welfare of India (MoHFW) introduced the Telemedicine Practice Guidelines (TPG) in March 2020. The TPG were introduced to assist medical practitioners in pursuing a sound course of action to provide effective, safe and fast medical care online. The TPG prescribe rules relating to the physician-patient relationship, issues of liability and negligence, evaluation, management and treatment, informed consent, continuity of care, referrals for emergency services, medical records, privacy and security of the patient records and exchange of information, prescribing, and reimbursement, health education, and counselling. The TPG are applicable to the registered medical practitioners (ie, who are enrolled in the State Medical Register or the Indian Medical Register under the erstwhile Indian Medical Council Act, 1956 and current National Medical Commission Act, 2019 (NMC Act)). Under the existing framework, the TPG do not apply to registered medical practitioners outside India.

With multiple lockdowns and restrictions on movement throughout the country, healthcare workers and doctors have been using telemedicine solutions for providing timely and faster access to patients, as it was cost-effective and could significantly reduce the efforts associated with travel. Telemedicine has been playing an important role where there is no need for patients to visit a hospital or a doctor in person. The advancement of telecommunication technologies in India also helped to maintain records of a patient's health history, and can help patients to manage their medication and diseases better.

During the nationwide lockdown last year, as patients were forced to stay at home, the healthcare practitioners started providing remote consultations with the help of video/audio calls and text messages. Over the period of lockdown, technology-based consultations were

also extended to COVID-19 patients with mild symptoms and where hospitalisation was not required.

Additionally, as was the case globally, there was an increase in mental health issues among the people who were affected by COVID-19 and having to quarantine, and other non-affected people staying at home during the lockdown. In this regard, many healthcare organisations and doctors have been providing online counselling for people.

Further, there have been various efforts made to promote telehealth in India. The India Virtual Hospital, a medical technology service in India, had launched a Patient Care App that enabled doctors to track patient's health and recovery periodically. Another health-tech company has recently launched an online platform, iCliniq, where users can get medical advice from doctors/medical practitioners, physicians and therapists from the US, the UK, the UAE, India, Singapore, Germany, etc, using e-mails, chats, video and audio calls. Another Indian company has set up a virtual hospital for cancer patients in 2019 for online consultation, treatment planning, and cancer treatment management.

The advancement of digital technology has been helping to ease various issues in the healthcare sector, ranging from diagnostic tests to the promotion of treatments.

For the first time in India, the Indian Council of Medical Research (ICMR) has recently approved a self-COVID-test kit, called CoviSelfTM COVID-19 Rapid Antigen Self-Test Kit, which enables users to conduct COVID-19 tests at home and obtain results within 20 minutes, through a mobile application. However, the CoviSelfTM mobile application has yet to be launched in India. Therefore, many specific aspects of the application, such as how any such service-providers will handle the patient's health data, the patient's personal data, legal consequences for inaccurate results, how the service-provider will indemnify users in the case of inaccurate results, and quantum of damages in such cases, etc, have still to be resolved.

The telemedicine platforms are currently governed under the NMC Act, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (IMC Regulations), the Drugs & Cosmetics Act, 1940 (D&C Act), the Drugs & Cosmetic Rules 1945 (D&C Rules), the Clinical Establishment (Registration and Regulation) Act, 2010, the Information Technology Act, 2000 (IT Act), and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules).

Further, in the case of medical negligence, a patient may lodge a complaint before the relevant consumer forum under the Consumer Protection Act, 2019, a civil suit for damages, a criminal petition under the Indian Penal Code, 1860, or lodge a complaint with the National Medical Commission (NMC). There is no specific law in India currently that governs online consultations provided by foreign medical practitioners.

Wearable devices

The use of wearable devices has been increasing in India. Several wearable devices are now available in India, such as heart-rate trackers, blood oxygen-level tracker, and other parameters, including water consumption, weight, sleep, diet, etc. These devices allow the patients to self-detect various physiological changes in the body and also alert the patients in the case of arising issues. All medical devices are regulated under the NMC Act, the IMC Regulations, the Medical Devices Rules, 2017, the IT Act and the Privacy Rules. Although there are

no specific rules or regulations that pertain to wearable devices, the foregoing rules will also apply to wearable devices. Under the current regulatory framework, these medical wearable devices require registration and approval from the Central Drugs Standard Control Organisation (CDSCO) in India.

For instance, the CDSCO has very recently approved three medical wearable devices in India, namely, Smart Vital, Vital 3.0 and Vital EGC, from GOQii, a California-based fitness company, which measures body temperature, pulse, ECG, tracks sleep, blood pressure, steps taken, exercise, etc.

Online pharmacies

The pandemic has accelerated the operation of online pharmacies in India, primarily for the online purchase and physical delivery of medicines to the patient's doorstep. There has been a significant rise in the number of online pharmacies in India in the past few years, more so during the pandemic. Although the manufacture and sale of medicines are regulated by the D&C Act, the D&C Rules, the Clinical Establishment (Registration and Regulation) Act, 2010, the NMC Act and the IMC regulations, there is currently no law in India that specifically governs online pharmacies. The MoHFW issued a notification in August 2018 to amend the D&C Rules to bring online pharmacies under its purview (Draft Rules).

The Draft Rules include provisions for sale of drugs by e-pharmacies. Further, the Draft Rules define the term "e-pharmacy" as the business of distribution or sale, stock, exhibit or offer for sale of drugs through a web portal or any other electronic mode. The Draft Rules contain provisions for the registration and validity of e-pharmacies, conditions for registration imposed on the e-pharmacies such as location, disclosure of information, procedure for distribution and sale, etc. While the Draft Rules are pending to be enacted, e-pharmacies in India currently require registration with the CDSCO.

Further, the online pharmacies will also have to adhere to the Privacy Rules in relation to the collecting, handling and processing of a patient's sensitive personal information, including financial information, bank account details, physical, physiological and mental health data, sexual orientation, medical records and history, and biometric information.

Artificial intelligence (AI)

The AI-based systems are used for the diagnosis of disease and also for treatment purposes. Robotic surgeries allow doctors to perform complicated procedures with the help of automated machines. AI is also used for vaccine development, thermal screening, CT scans, etc. The AI-based systems are also regulated by the NMC Act, the IMC Regulations, the Medical Devices Rules, 2017, the IT Act and the Privacy Rules. India is home to several globally well-known multi-speciality hospitals and patient-care centres, which are equipped with highly sophisticated technologies. With the increasing role of robotic surgeries and AI in healthcare in India, the Insurance Regulatory and Development Authority of India (IRDAI) issued the Guidelines on Standard Individual Health Insurance Product in January 2020, directing the insurers to cover robotic surgeries under standard health insurance policies.

Electronic health records (EHR)

Digital health data records help with easy accessibility for doctors to view a patient's medical history and make relevant consultations and recommendations, all in an efficient and time-saving manner. Digital health records also eliminate duplication of tests and save costs significantly. Many private multi-speciality and super-speciality hospitals in India maintain EHR databases;

however, most government hospitals have not yet upgraded their systems.

The MoHFW originally notified the Electronic Health Record (EHR) Standards, 2013, and also revised these standards in December 2016, by issuing the new Electronic Health Record (EHR) Standards, 2016 (EHR Standards). All the EHR technologies must comply with the EHR Standards. These EHR Standards are largely based on the principles of data protection laid down under the Privacy Rules. Most recently, the Indian state of Kerala has successfully deployed an efficient EHR system, by collecting and storing the electronic health records of over 25.8 million people as part of its eHealth project. This initiative has allowed patients to walk into any government hospital without carrying any paper records. With the increasing demand for contactless procedures, especially since the pandemic began, several state governments are in the process of adopting these EHR systems and other such digital mechanisms to maintain health records.

Online aggregators for health services

There are several new online platforms in India that allow users to search for doctors with different specialities in a particular region. These platforms also allow users to book online appointments with doctors and provide reviews and ratings to these doctors for their services and guidance. Currently, there is no specific law in India which regulates online health-aggregator platforms. However, the MoHFW issued a direction in January 2021 to all the state governments to regulate the online health-aggregation platforms. Moreover, under the existing regulatory framework, these online health-aggregator platforms will require registration with the CDSCO in the same way as online pharmacies.

The increasing number of technologies collecting health data gives rise to concerns relating to data protection and privacy of patients. The personal information relating to a person's health is categorised as sensitive personal information under the Privacy Rules. The Privacy Rules lay down mandatory principles of data privacy to be followed by the body corporates that are collecting, handling and processing sensitive personal information. India does not currently have a comprehensive data protection law. The Government of India issued the Personal Data Protection Bill, 2019 (PDP Bill), which is intended to become a comprehensive data protection law in the country.

There is no specific law in India, so far, to regulate digital health tools and digital health data. However, the government has taken several new initiatives to address the privacy concerns relating to digital health in India, as explained below.

Healthcare Regulatory Developments in India

The Government of India notified the draft Digital Information Security in Healthcare Act, 2018 (the DISHA Bill), to protect the digital health data of its citizens. The DISHA Bill defines the term "digital health data" as an electronic record of health-related information about an individual. The government proposed the DISHA Bill in 2018 to standardise and regulate the processes related to the collection, storing, transmission and use of digital health data, and to ensure reliability, data privacy, confidentiality and security of digital health data. However, India has yet to adopt any legislation to regulate and govern digital health tools in India.

As a temporary measure, the Government of India issued the TPG in March 2020, which contain norms and standards for registered medical practitioners to consult patients via telemedicine. The TPG regulate all channels of communication with the patient that leverage information technology platforms, including voice, audio, text, and digital data exchange.

The Government of India also issued a Health Data Management Policy in October 2020 to impose standards for data privacy protection in India. The DISHA Bill and the Health Data Management Policy are both based on the data privacy principles laid down under the PDP Bill.

Other Emerging Trends and Developments in India

Rise in digital solutions

Besides the use of telemedicine/tele-health in the Indian healthcare sector, there has been a rapid increase in digital payments during the COVID-19 pandemic. People of all age groups have accustomed themselves to carrying out digital payments to reduce physical contact. There has been an astonishing increase in mobile applications and online platforms that allow doorstep delivery of groceries, medicines and other products and services.

The Work-from-Home (WFH) policy and online meetings through Zoom, Google Meet and Microsoft Teams have been adopted across every industry, and have seen a tremendous rise since the beginning of the pandemic. Many healthcare professionals and non-frontline workers, including therapists, psychiatrists, dieticians, etc, have been conducting programmes/seminars and consultations using these online platforms.

5G network in India

India is in the process of launching the 5G network in India. The rapid increase in the use of digital solutions demands higher speed and connectivity. The 5G network will ensure more effectiveness and efficiency in tele-consultations and remote monitoring of patients and handling patients health data as well.

The 5G network will help faster transmission of large health-data files, and will assist better video/audio telecommunications between doctors and patients, improve the use of augmented and virtual reality, and will enhance the use of artificial intelligence in the healthcare devices.

Role of social media platforms

Social media platforms, such as Facebook, Instagram, Twitter and WhatsApp, have been very popular in India, and their use has only increased since the pandemic in India. A sudden onslaught of a second wave of infection in India has resulted in a shortage of oxygen cylinders and hospital beds throughout the country. Social media platforms have been instrumental in connecting people and amplifying information on the availability of oxygen cylinders and hospital beds in India. Social media platforms have also enabled patients to connect with relevant organisations such as NGOs that supply and deliver oxygen cylinders and other ICU set-ups at home. Additionally, many healthcare professionals and doctors in India have been consistently posting useful information and sharing videos on social media, providing free consultations and guidance to people in order to tackle the virus.

In this regard, the Government of India has been regularly discouraging people from taking unsolicited and unprofessional COVID-19-related advice on social media. However, many reputable health experts and physicians still continue to provide such advice on social media, which are not currently prohibited by the government. It appears that government organisations are allowing professional and genuine healthcare experts to provide COVID-19 advice on social media. The Government of India has from to time ordered social media platforms, including Twitter, Facebook, Instagram and YouTube, to remove posts that were fake and misleading, and those which were critical of its handling of the pandemic.

The Ministry of Electronics and information Technology (MEITY) notified the Information

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, on 25 February 2021, which require digital media platforms to implement grievance-redressal mechanisms, to appoint resident grievance officers, active monitoring of content on the platforms, monthly compliance reports, self-regulation mechanisms, and also an oversight mechanism deployed by the MEITY.

Online legal proceedings

During the COVID-19 pandemic, the courts, and tribunals, including the Trade Marks Registry, the Patent Office, the Design Office, etc (IP Offices), in India have been conducting hearings and other meetings through video conference (VC) facilities. For instance, the VC hearings in the IP offices have helped in faster disposals of pending IP applications and opposition proceedings. The Delhi High Court has also issued specific rules for conducting VC proceedings.

These VC proceedings have made the administrative and legal procedures much faster and efficient, allowing companies, brand-owners, inventors, and other stakeholders to obtain faster protection of their intellectual property and to resolve legal disputes in an effective manner.

Extension of statutory limitation periods

Due to the pandemic, the Supreme Court of India has been periodically extending all the relevant statutory limitation periods and timelines, to prevent additional burdens on the parties and to keep the parties' legal rights alive during the pandemic.

Conclusion

Considering the country's size, the demography, and the amount of rural population without adequate access to healthcare infrastructure, India has significant scope to do and develop more and more digital healthcare technologies and platforms. As regards the legal regime, India has not thus far enacted a robust law on digital healthcare. Currently, India is in the process of enacting specific laws on digital healthcare, information security and personal data protection. A robust and unified digital heath law may also evolve very soon, considering the pace of transformation in the healthcare sector.

Contributed by: *Anoop Narayanan and Sri Krishna,* ***ANA Law Group***

ANA Law Group is a full-service law firm based in Mumbai; its team of experienced and committed professionals has broad industry knowledge and specialises in a wide spectrum of laws. Founded on traditional values, with prominent cross-border exposure and a solution-oriented approach, the firm provides significant value to clients internationally, acclaimed for its client servicing model, each client receiving the required attention to provide practical legal solutions. The firm has significant experience in counselling international clients on data protection and privacy in India, acting for many businesses in complicated transactions, thus attaining in-depth knowledge of all aspects of industries such as banking and insurance, financial institutions, luxury goods, consumer goods, and healthcare. In addition to data protection and privacy, the firm assists international companies on global privacy law involving Indian projects, drafting and negotiating contracts with their Indian counterparts, preparing data protection and privacy policies for those companies' Indian subsidiaries, compliant with major international privacy laws. Specifically, the firm advises clients on data processing and all aspects of data security, including handling cross-border data flows, security breaches and compliance with all regulatory requirements.

AUTHORS

Anoop Narayanan is a leading Indian lawyer in corporate law, intellectual property law, and information technology with more than 27 years of experience as an attorney. Focusing on a broad range of intellectual property, IT, outsourcing, employment, technology, data protection, telecommunications and entertainment law matters, his practice encompasses both litigation and commercial or transactional advice. He has worked with India's highest-profile companies, as well as global corporates in the manufacturing industries, banking and finance sectors, and telecommunications and technology companies. His experience and expertise in TMT and data privacy was invaluable in setting up the Indian operations of large global technology companies and handling several India-bound outsourcing transactions with the major Indian IT companies. He and his team assist many international clients, advising multinational banks on Indian privacy and data protection law, outsourcing, bank secrecy, and related matters in connection with outsourcing transactions. He has spoken at several Indian and international forums on his areas of practice and has published many articles on several areas of Indian law.

Sri Krishna is an associate working in the firm's TMT and IP practice group. He regularly advises international clients on intellectual property, healthcare and pharmaceuticals-related issues in transactional, compliance and regulatory matters.

ANA Law Group

303 Madhava Premises
Bandra Kurla Complex
Bandra East
Mumbai
400 051
INDIA

Tel: +91 22 6112 8484
Fax: +91 22 6112 8485
Email: anoop@anaassociates.com
Web: www.anaassociates.com