Page 1465 - 1481 **DOI:** *https://doij.org/10.10000/IJLSI.112062*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 6 | Issue 3

2024

Data Security and Telemedicine: A Legal Perspective

HARDIK TOKAS[1]

ABSTRACT

Telemedicine has emerged as a promising solution to enhance healthcare access and reduce costs, particularly in geographically diverse countries like India. However, the rapid digitization of healthcare has raised significant data security and privacy concerns. This paper examines the regulatory framework governing telemedicine in India and the associated data security challenges. Key regulations include the I.T. Act 2000, SPDI Rules 2011, NMC Act 2020, and Telemedicine Practice Guidelines 2020. These aim to provide legal guidelines for telemedicine practices and address data protection issues. The paper highlights the importance of patient consent, data confidentiality, and cybersecurity measures in telemedicine. While existing regulations provide a foundation, there is a pressing need for comprehensive legislation tailored explicitly to telemedicine's unique challenges. The upcoming Personal Data Protection Bill is expected to strengthen data privacy provisions. However, additional measures are required to regulate data encryption, secure storage, and protect against cyber threats. The paper concludes that a collaborative approach involving policy-makers, healthcare providers, technology companies, and legal experts is crucial to addressing data security challenges in telemedicine. Regular audits and assessments should be mandated to ensure compliance with data security standards. As telemedicine continues to grow in India, robust data security and privacy measures will be essential to build patient trust, foster innovation, and fully leverage the potential of digital healthcare in the country.

I. INTRODUCTION

Successful telemedicine applications have increased patient access to treatment while decreasing healthcare expenses. Around 61% of U.S. healthcare facilities and 40%-50% of U.S. hospitals adopted telemedicine in 2016. 1 In 2013, the telemedicine industry had a 60% increase in revenue compared to the previous year. However, the low reimbursement rates and differences in licence and practise across states have hampered its wider adoption. According to the World Health Organization (WHO), telemedicine is the "delivery of health care services, where distance is a critical factor, by all health care professionals using information and

[1] Author is an Advocate at Varistha Law Offices, New Delhi, India.

 [ISSN 2581-9453]

communication technologies for the exchange of valid information for the diagnosis, treatment, and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers." Telemedicine is used to diagnose, treat, and prevent diseases and injuries and for research and evaluation.

Ancient Telemedicine

Greek and Roman civilizations circa 500 B.C. displayed the first examples of telemedicine. Human couriers carried information and goods between settlements, including medicines and medical guidance. Smoke signals and light reflections sent medical information. Particularly at greater distances, they were used to announce significant health-related occurrences such as births, deaths, and epidemics. Evidence suggests that various forms of intermediate communication, such as smoke signals and light reflections, have been utilised to convey medical information. The frequency of infections and the announcement of significant health events like births and deaths have been tracked via various forms of electronic communication. Similarly, American Indian communities in ancient Greece employed smoke signals to alert others of medical and health emergencies.[2]

First steps to modern telemedicine and recent applications

The Netherlands laid the groundwork for contemporary telemedicine in the early 1900s and became the first country to transmit heart rhythms. By the 1920s, this expanded to include transmissions to radio consultation centres throughout Europe.[3] Since then, telemedicine has made enormous strides toward becoming an integral part of modern medicine and health care. The extensive use of telemedicine is the distinguishing characteristic of this field. Early pioneers in telemedicine mainly depended on their intuition when introducing telemedicine services. To them, it seemed apparent that telemedicine would make it possible for patients in far-flung locations to have access to medical specialists. The quick availability of information for doctors on both sides of the consultation would cut down on waste and duplication in medical treatment. Additionally, it seemed apparent that telemedicine would make it possible for patients in far-flung locations to have access to medical specialists.[4]

In the early 1900s, various ideas were devised for transmitting stethoscope-related data through communication lines, and these ideas were explored by several different people (telephone,

[2] "History of Telemedicine & Telehealth: When Did It Start - eVisit" (*eVisit*) <https://evisit.com/resources/history-of-telemedicine> accessed June 19, 2024
[3] Dossetor, J.B. "Beyond the Hippocratic Oath: A Memoire on the Rise of Modern Medical Ethics. Canada:" The University of Alberta Press, 301 p (2005)
[4] *Ibid*

radio, etc.). Despite this, not a single one of their efforts was successful. It wasn't until the latter half of the 1950s and the early 1960s that researchers published their first findings on telemedicine in transmitting video, still images, and complex medical data. Interactive telemedicine was used for the first time in 1959 by the University of Nebraska to broadcast neurological examinations; this is considered one of the first instances of a live video telemedicine consultation. Applications created expressly for transmitting medical data, such as the findings of a fluoroscopy, an x-ray, a stethoscope reading, or an electrocardiogram (ECG), are also often used in educational settings. This data may be shown on a computer or a tablet.[5] These early projects were aimed to achieve the following:

- Providing access to health care in rural areas.
- Urban medical emergencies.

Studies demonstrate that in the 1960s, the National Aeronautics and Space Administration (NASA), Lockheed Corporation, and the United States Indian Health Service worked together to construct the STARPAHC project, a significant turning point in the development of telemedicine. Telemedicine programmes on a massive scale, such as Space Technology Applied to Rural Papago Advanced Health Care (STARPAHC), are now being created. A medical community member was able to provide telemedicine services to a Native American tribe by using the same equipment that was designed specifically for use by astronauts when they were in orbit. Telemedicine is reportedly used in several programmes that get funding from either the government or grants, including:[6]

- Delivering healthcare services to geographically isolated scientific outposts in the Arctic and Antarctic regions.
- Delivering healthcare services within a conflict-affected area.
- Medical care should be provided to correctional facilities without requiring inmate transportation to external healthcare facilities.
- The utilisation of digital technology for the transmission of radiology images.

The field of radiology was the first in medicine to use telemedicine completely. The medical community has widely accepted teleradiology after grant-funded experiments demonstrated its efficacy and trustworthiness. It was in the 1980s that some radiologists decided to employ tele-radiology technology to receive pictures for telemedicine consultations. Almost all of the first

[5] *Ibid*
[6] *Ibid*

telemedicine deployments were huge initiatives, studies show, necessitating substantial changes in personnel and organisational structure.[7]

The telemedicine deployments made use of specialised gear and software. Therefore, the typical patient had no direct contact with telemedicine technology since the cumbersome equipment could only be operated by experienced personnel. A tele-presenter was in charge of the set-up and patient interaction instead. The development of technology and other causes have resulted in significant alterations to the original designs of many pioneering endeavours. When discussing the first iterations of telemedicine, the term "telemedicine" is used.

In the 1960s, the transmission of video, pictures, and other medical data began, generally seen as the beginning of the modern concept of telemedicine as it is practised today. It was not until 1959 that physicians at the University of Nebraska became the first persons to employ video communication to provide medical care. They were able to transmit neurological evaluations via the use of interactive telemedicine, and additional systems like this quickly followed.

Completing a successful government initiative involving the Internet Health Service and NASA was a pivotal moment in expanding telemedicine as a field of practice. Space Technology Applied to Rural Papago Advanced Health Care was the project's name (STARPAHC). It used the same technology that astronauts use during space flights to deliver telemedicine services to the Native Americans who live on the Papago Reservation in Arizona.[8]

Over the subsequent decades, the STARPHAC initiative piqued several individuals' attention in telemedicine. The rapid expansion of telemedicine technology may be attributed to the participation of many educational institutions, medical facilities, and research businesses that came up with increasingly innovative and audacious ideas.

Today, because of telemedicine programmes, the number of people hospitalised for mental health issues decreased by more than 40% (as per a survey in 2012), while the number of people hospitalised for heart failure decreased by 25%, and the number of people hospitalised for diabetes and chronic obstructive pulmonary disease decreased by 20%. In 2015, around 677,000 veterans accessed approximately 2.1 million telehealth sessions.[9]

II. TELEMEDICINE AND THE INTERNET

The advent of the Internet in the 1990s led to several consequences, including information

[7] Freiburger, Gary, Mary Holcomb, and Dave Piper. "The STARPAHC collection: part of an archive of the history of telemedicine." Journal of telemedicine and telecare 13.5 (2007): 221-223.
[8] *Ibid*
[9] Ebad, Ryhan, and K. S. A. Jazan. "Telemedicine: Current and future perspectives telemedicine: Current and future perspectives." International Journal of Computer Science Issues 10.6 (2013): 242-249.

explosion. Utilizing the protocols of the internet made it feasible to support all of the information and traffic that is required for telemedicine; the information includes:

- Educational levels of the patient (text, images, video).
- Medical images such as x-rays and scans (DICOM image standards).
- Real-time audio and video consultation.
- Vital signs and other body measurements (ECG, temperature, etc.).[10]
- The expansion of the internet was driven by forces unrelated to health care, such as globalisation, content creation, consumer demand, and other considerations. Because of this expansion, a significant amount of money and technical work has been put into improving the Internet's infrastructure,[11] including:
- Accessibility Many online services use backup servers and may dynamically start more servers as demand increases.
- AWS hosts virtual servers for the Cloud.
- Communication rates—bandwidth and latency—are discussed.
- Databases and object stores may store huge items like photographs and movies.
- Digital cameras, scanners, and other devices digitise analogue data.
- Encryption, passwords, access levels, and other security procedures are discussed.
- MP4 and PNG are data transfer formats.

The enhancements mentioned above to the Internet have impacted health care and telemedicine. The existing tools and frameworks for web applications made creating a healthcare software application for sharing and storing clinical data simpler and cheaper than ever. The move to EMRs, or electronic medical records, has been facilitated by the United States government's incentives (and potential penalties) as a pioneer in e-health. Most current EMR providers facilitate healthcare practitioners' and patients' access to medical records over the Internet. Patients are increasingly turning to online "portals" where they can access their medical records and securely communicate with their doctors about test results, medication refills, and health concerns. Both doctors and people are becoming more educated about

[10] "Telemedicine & Telehealth: How the Internet Is Helping Healthcare Evolve" (*Pediatrics on Demand*, April 1, 2020) <https://pedsondemand.com/blog/telemedicine-telehealth-how-the-internet-is-helping-healthcare-evolve/> accessed June 27, 2024

[11] *Ibid*

healthcare.[12]

III. THE INFRASTRUCTURE USED IN TELEMEDICINE

Telemedicine Application Areas

Care for patients in the comfort of their own homes, rapid reaction to medical emergencies, and data analysis are all areas in which telemedicine excels. Tele-consultation is sharing clinical information with a medical professional through the Internet to get a second opinion on a patient's condition. Teleradiology is the transmission and exchange of diagnostic X-rays and other images; telepathology is the management of patient records and electronic clinical histories; Tele dermatology makes use of video conferencing or image transmission to assist dermatologists; telepsychiatry makes use of video conferencing and chats to help patients experiencing mental health issues, and telemedicine is utilised in virtually every field of medicine (telecardiology). In addition, surgical procedures may be assisted, monitored, and even conducted remotely by integrating the resources of telemedicine with those derived through virtual reality, robotics, and artificial intelligence. Telemedicine, robots, and artificial intelligence (tele-surgery).[13]

Telemedicine Benefits

The age structure of contemporary civilizations has been progressively affected by socio-economic shifts over the last several decades. Better food and hygienic conditions, together with more effective health policies and health systems, contribute to a demographic change in which the percentage of adults rises and the proportion of children falls. The rising expenditures on health care, a direct result of the increased incidence of chronic illnesses, present significant difficulties in this context. One of the greatest difficulties is ensuring the long-term financial viability of health systems, which is particularly important in nations where the government primarily funds health care. Evidence suggests that the current model of intensive use of health care resources during the final stage of life is shifting to increased expenditure in preventing and treating chronic diseases due to lower death rates and longer life expectancy. However, this is still a topic of active research. Now that ICTs are being implemented at the social assistance level, there is a chance to provide complete support and follow-up for chronic patients and low-prevalence illnesses while also enabling education in preventive medicine and public health.[14]

---

[12] *Ibid*

[13] Mishra, Sanjaya & Basnet, Rajesh & Singh, Kartar. "Current telemedicine infrastructure, network, applications in India" (2006).

[14] Dusseux E, "Infrastructure Needed for Telemedicine Services" (*Physicians Practice*)

However, problems may be traced back to more than simply the state of the economy. There are huge gaps in access to vital health treatments even within the same country and health care system. According to figures from 1999, the number of primary care physicians per 100,000 inhabitants in the north varied from 39 to 113, while the number of specialists per 100,000 persons in the south ranged from 12 to 69. Even for the most basic medical care, it is necessary for most rural Indians, who live more than 8 kilometres away from the closest medical centre, to go at least that far. The remaining 11% of rural Indians, however, must travel far further. A disproportionate amount of the health care budget is eaten up by travel and hotel expenses incurred in locations with convenient access to medical services. In Barcelona, residents have easy access to a neurologist at a tertiary care centre. Still, in other regions of the nation, they may have to travel more than 70 kilometres to reach the referral hospital.[15]

Because of this, telemedicine has an effect on education and competency at both the primary health care and hospital levels; it shortens waiting times (both for diagnosis and treatment), thereby preventing more serious complications; it enables remote consultation from primary care to the referral hospital, thereby reducing the number of referrals; and it makes it easier for everyone, regardless of location, to have equitable access to medical care services. These contexts use concepts such as comprehensiveness and interoperability in healthcare organisations. Other examples include continuity of treatment and patient-centred health care.[16]

Development of the Telemedicine Service

After discussing the strategic, organizational, and public policy facets of telemedicine service implementation, we move on to the service development phase, which centres on the internal explanatory factors of healthcare organisations and their descriptions of telemedicine use. At this point, we can already see the value of telemedicine implementation. It serves as a roadmap for the development of telemedicine, focusing on four crucial factors, namely:

Legal, regulatory, and security issues: For telemedicine to succeed, regulatory concerns must be addressed. When launching and expanding a telemedicine service, assessing the current regulatory landscape is crucial. In general, these regulatory aspects are:

- Protection of data;
- Privacy and confidentiality of data; and

<https://www.physicianspractice.com/view/infrastructure-needed-telemedicine-services> accessed June 27, 2024

[15] *Ibid*

[16] "ACM Digital Library" (*ACM Digital Library*) <https://dl.acm.org/doi/10.1145/3173574.3173958> accessed June 27, 2024

- Issues related to responsibility for data.

For instance, the unwarranted spread of a potentially life-threatening clinical ailment might have devastating consequences for those who contract it. Thus, the telemedicine service implementation plan has to identify what the protection measures are and firmly define acceptable compliance for private medical protection to guarantee patients' rights and obligations, for example:

In a setting in which there is decentralization, the standards for the responsible preservation of data and a variety of electronic records, such as clinical or medical papers on a single health event and the medical record that comprises the patient's entire clinical development, need to be outlined clearly and concisely.

It is of the utmost importance that you designate which of the linked users of the telemedicine service are granted permission to view the data.

Determine whether or not it is required to give numerous degrees of access to information for professionals participating in the telemedicine service being launched, and then carry out this action if necessary.

All professionals who are dealing with this problem must be familiar with the most recent clinical standards relevant to it; as a result, it is vital to establish a training programme in this respect.

- **Technological and infrastructure issues:** The healthcare business has numerous legacy systems built on proprietary technology with a great deal of recorded information, making telemedicine one of the most challenging situations to adopt. Implementing a telemedicine service requires careful consideration of many factors, including interoperability and technology infrastructure:
- **Organizational interoperability:** For the effective deployment of telemedicine services, meaningful collaboration across various organisations, institutions, and internal processes is necessary. As a result, the purpose of ensuring that organisations can communicate with one another via interoperability is to guarantee that services are discoverable, consistent and centred on the objectives of end customers.
- **Syntactic and semantic interoperability:** Interoperability in data formats is called syntactic interoperability. In contrast, interoperability in terms of the exact meaning of information is called semantic interoperability. Semantic interoperability ensures that any application can understand information, regardless of whether or not it was initially

developed for a particular purpose. Through semantic interoperability, the systems can merge the information they have received with that obtained from other sources and then process both sets of data so that they may be readily understood.

- **Technical interoperability:** This refers to the technical factors involved in bringing multiple pieces of I.T. equipment together, such as open interfaces, data connectivity services, data integration, data display, and exchange, as well as accessibility and security services.
- **ICT Infrastructures:** The degree of technological advancement required for the telemedicine service operation must be considered. If a technology is needed, that is still in the early phases of development or has not been well tested, this should be seen as a significant risk for the deployment of the service. If someone is using the service for the first time, they could run into several issues, or at the least, they need to be completely informed of the potential hazards before using it.
- **eHealth Infrastructures:** Along with more fundamental concerns about information and communications technology, it is essential to identify and secure the specialized eHealth infrastructures required to develop the telemedicine service. It is necessary to remember that the service will integrate some sort of health information system connected to others for the interchange of health information at various levels, both with providers and with patients.
- **National Research and Education Networks (NRENs):** The National Research and Education Network (NREN) is a specialized provider of high-speed Internet services that helps meet the interconnection needs of research and education communities within a nation and with research networks located all over the world by leveraging the appropriate infrastructure for the exchange of data.

IV. DATA SECURITY CHALLENGES IN TELEMEDICINE

Telemedicine Security

When devices and systems connect and exchange data via the internet, there is a possibility that security holes may be introduced. The COVID-19 pandemic has brought additional attention to telemedicine, a practice that has existed for millennia but has gained popularity in the last few months. It is essential to rethink healthcare cyber security in light of the growth of telemedicine. 2018 was a year in which cyber security was one of the most pressing issues for the healthcare industry (Healthcare Executive Group, 2018). Since then, the extensive use of

telemedicine during the pandemic has brought attention to the challenges in healthcare security. The National Institute of Standards and Technology predicts that by 2020, fewer than half of all healthcare providers will have attained the level of cybersecurity preparation recommended.[17]

According to a recent survey, the most common victims of the epidemic have been healthcare workers and patients (Microsoft, 2020). Telemedicine platforms and services have been increasingly mentioned on the dark web, a portion of the internet not indexed by search engines that is rife with illegal activities (Security Scorecard, 2020). Hackers use the dark web to make money off compromised medical records. On the dark web, a valid medical licence may fetch over USD 1,000, which is significantly more than the value of a credit card number. Attackers may target the healthcare sector in a more lucrative and riskier way. To restore access to your files and data, ransomware demands payment. At least 18,069,012 individuals' protected health information was compromised in at least 92 healthcare ransomware attacks in 2020. While exact costs from ransomware attacks on the healthcare sector are difficult to predict, they are projected to reach $31 billion between 2016 and 2020.[18]

Those who are geographically distant from one another may still get quality medical treatment thanks to telemedicine, which delivers medical interventions using electronic information and communication technology. One of the most crucial and challenging areas of e-governance is telemedicine.[19] Telemedicine projects have to face challenges like

- integration with the medical practice and the healthcare system,
- identification with the e-governance vision and policies of the nation,
- Its economic implications and
- it's social impact. Apart from these, there are several other challenges like sustainability, security,
- legal and ethical issues still related to telemedicine.

Implications of Cyber Attacks on Telemedicine Network

Patients who use telemedicine express anxiety that their identities could be revealed in an electronic medical record that is sent. Patients' medical records must be unavailable to anyone

[17] "Fact Sheet: Medicaid & CHIP and the COVID-19 Public Health Emergency | CMS" (*CMS*, June 14, 2021) <https://www.cms.gov/newsroom/fact-sheets/fact-sheet-medicaid-chip-and-covid-19-public-health-emergency> accessed June 27, 2024

[18] "Solutions for Challenges in Telehealth Privacy and Security" (*Journal of AHIMA*) <https://journal.ahima.org/page/solutions-for-challenges-in-telehealth-privacy-and-security> accessed June 29, 2024

[19] Cynergistek (September 17, 2020). Moving forward: Setting the direction. 2020 Annual Report.

not authorised to see them to protect their privacy, integrity, and confidentiality. One example of this is when a confidential list of all of the AIDS patients in the state of Florida was posted online in plain sight. The availability of this list of around 4,000 persons has further intensified concerns surrounding the confidentiality of people's medical information. In addition to ensuring that patient data is correct and up to date at all times and that its validity, origin, and integrity can be validated, it is of the utmost importance that this data be freely available to any authorised healthcare providers. If an electronic medical record is manipulated in any manner, a patient's life might be in danger. Because of this, any electronic healthcare network must safeguard the C-I-A (confidentiality, integrity, and availability) of patient health data. Recent advancements, such as wireless networking, have further complicated the previously challenging issues of e-healthcare and telemedicine security. Because of this, it is essential to analyse the possible harm that a cyber attack on a network might cause.[20]

According to the nature of the impediment they provide to the flow of regular information, attacks may be divided into one of four kinds:

- **Interruption**: This is an attempt to prevent information from being made available. The information is either rendered inaccessible or lost entirely.
- **Interception**: This is an intrusion into the confidentiality of the information (C). A third party that should not have access to the information does so.
- **Modification**: This threatens the truthfulness and reliability of the information. Not only does an unauthorised third party access the material, but they also modify it without permission.
- **Fabrication**: This constitutes a challenge to the reliability of the information. A fabricated message is introduced into the information by a third party that is not authorised to do so.

According to the nature of the attack, breaches in telemedicine networks may be divided into one of two main types:

- **Active attacks:** There are three distinct types of these assaults, and they include either the alteration, interruption, or creation of patient information:

[20] Zain. J. and Clarke. M. (2005). "Security In Telemedicine: Issues In Watermarking Medical Images". 3rd International Conference: Sciences of Electronic

- **Masquerade**: The information's confidentiality (C) and integrity (I) may be compromised due to this. In this scenario, an entity is attempting to trick a system by falsely representing themselves and acting as if they are another entity.
- **Modification of messages:** In other words, information integrity (I) is compromised. This happens when an authorised communication is modified in part or when authorised messages are withheld and then replicated in an unauthorised manner.
- **Denial of service:** The accessibility of data is compromised by the assault. An adversary might prevent authorised users from accessing or managing their networks by overloading a system's processing or memory resources.
- **Passive attacks:** During these attacks, information may be stolen, but the information is not altered. These attacks include monitoring a system while it does business to steal sensitive information. Participating in such activities may entail overhearing conversations, sniffing the air, or observing traffic flow. An information leak or the transfer of data files to an adversary is known as a passive attack, and it occurs without the user's knowledge or consent.

V. REGULATORY FRAMEWORK GOVERNING TELEMEDICINE

National Medical Commission Act, 2019

The National Medical Commission Act, often known as the "NMC Act," will become the primary statute that regulates medical education and the practice of medicine in India as of September 2020, according to an official announcement made by the Ministry of Health and Family Welfare ("Health Ministry"). Patients in India may only be treated by medical professionals who meet the requirements of the NMC Act, which stipulates that they must have a degree in medicine from an institution that has been granted accreditation and be in good standing with a state medical council. The Indian Medical Council Act, 1956 (also known as the "IMC Act"), which controlled the medical business up until September 2020, was eventually replaced by the National Medical Council Act (NMC Act).

The IMC Act's rules and regulations will continue to exist and be fully functional, thanks to transition measures made available by the NMC Act. These measures will remain in place until the NMC Act's successor standards and requirements are outlined. The rules are considered to have been issued in conformity with the NMC Act provisions pertinent to the subject matter. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (also known as the "MCI Code") is one of the standards that were framed under the IMC Act;

it outlines the professional and ethical guidelines that physicians should adhere to when interacting with patients, pharmaceutical companies, and other colleagues. The MCI Code was enacted in 2002. The MCI Code is to be adhered to in the same manner as if it were published following the NMC Act while we wait for a new guideline on medical ethics to be formed under the NMC Act.

Telemedicine Practice Guidelines Issued under the MCI Code

The National Institution for Transforming Healthcare (NITI Aayog) collaborated with the Board of Governors to develop the Telemedicine Practice Guidelines. The Indian government established the Board of Governors to regulate medical education and the medical profession. NITI Aayog was responsible for creating the guidelines (in place of the Medical Council of India). Due to the inclusion of these guidelines in the MCI Code, all medical practitioners in allopathic medicine are now legally required to adhere to these standards.

These suggestions will continue to apply, and we will treat them as if they were approved under the NMC Act until the NMC Act is amended to create new rules. Because the Telemedicine Practice Guidelines detail the sorts of therapy that are authorised and how they should be administered, medical professionals may employ telemedicine regardless of their physical location. For example, it describes the circumstances in which an audio/video/text consultation should be used (emergency, non-emergency, and doctor-to-doctor) and the procedures that should be followed for each kind of consultation. In addition, the TPG categories pharmaceuticals into "List O," "List A," and "List B," as well as a "Prohibited List," and it outlines the circumstances under which each kind of medication may be administered (covered in detail in Section IV sub-heading 8).

Government Policies Regulating Health Data

The government of India is making strenuous efforts to establish a centralised healthcare system, with the intention of one day digitally recording the medical records of each Indian person. The implementation of the National Health Policy, 2017, which was the first step toward achieving the policy's stated goal of providing citizens with access to high-quality medical care through the development of a national digital health ecosystem, was the first step in realising the policy's stated objective ("NDHE"). Since then, both the Ministry of Health and the NITI Aayog, which is the think tank of the Indian government, have given their sets of instructions for the establishment of the NDHE. These regulations, which comprise the National Health Stack and the National Digital Health Blueprint Report, describe the core architecture and structure of the National Digital Health and Education Exchange (NDHE).

The National Digital Health Mission (NDHM), a critical digital health initiative, will get off the ground on August 15, 2020, according to an announcement by the government of India. Every person in India will be given a Health ID as part of the NDHM's plan. The National Data Health Model (NDHM), which includes the Health Data Management Policy (also known as the "HDM Policy"), was recently released for public study and comment. Patients, healthcare practitioners, clinical institutions, pharmaceutical firms, insurance providers, and others have responsibilities and rights spelt out in the HDM Policy, which addresses data protection and privacy concerns related to health data.

The Information Technology Act, 2000 ("I.T. Act"), The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, and the Information Technology (Intermediaries Guidelines) Rules, 2011

Through the use of telemedicine, both the patient and the attending physician may have an ongoing dialogue with one another. The medical records of the patient and any other personal information are both instances of "Sensitive Personal Data or Information," which is a term used in the Data Protection Rules ("SPDI"). When such information is collected, kept, transmitted, or processed by a company, the requirements outlined in the Data Protection Rules become active and become effective. In most cases, individuals must consent before their personal information may be collected or used in any way since this is a requirement of the Data Protection Rules. Additionally, according to the Data Protection Rules, companies must put suitable security measures into place to ensure that the data are kept in a safe environment.

Telecom Commercial Communication Customer Preference Regulations, 2018

SMS communication with patients and other users of a telemedicine platform may be required. According to the TCCP Regulations, it is against the law to transmit unsolicited commercial communications over voice or SMS. Users may only get promotional messages after registering with an access provider if they have already consented to receive these types of communications by selecting the appropriate box. However, sending business-related calls or information or making such calls is not against the law. A transactional message is triggered by a transaction completed by the recipient of the message provided that the receiver is a customer of the sender and the message is delivered within 30 minutes of the transaction being conducted and is directly connected to it.

Additionally, the message must be directly connected to the transaction. The transmission of a one-time password (OTP) or the provision of payment details for goods and services are both

instances of transactional communications. After obtaining the recipient's permission, any further communications, regardless of how closely connected they may be to the shipment of items, must be transmitted in a format registered with the access provider.

Telemedicine Practise Guidelines, 2020

No laws or norms have existed in India regarding the use of telemedicine through video, phone, or Internet-based platforms (web/chat/apps, etc..). Medical practice in India is primarily governed by the Indian Medical Council Act,1956; the Indian Medical Council (Professional Conduct, Etiquette, and Ethics Regulation 2002); the Drugs & Cosmetics Act, 1940 and Rules 1945, the Clinical Establishment (Registration, and Regulation) Act of 2010, and the currently, legal provisions pertaining to data privacy comes under the ambit of I.T. Act, 2000 and adjoining rules. Both physicians and patients, as well as their data, are put at risk when there are loopholes in the laws or when the standards are unclear. To mitigate this issue, Telemedicine Practise Guidelines were issued in 2020 to provide practical advice to doctors to encourage the widespread adoption of telemedicine into standard medical practice across all services and models of care. These guidelines help doctors make the best decisions for their patients and themselves by basing their care on the most recent research, appropriate technology, and individual circumstances.

Salient features

- **Doctors can choose the medium of teleconsultation:** A consultation with a patient may be conducted by any of the various modes of communication, including but not limited to face-to-face meetings, video conferences, Skype, email, fax, and even social media platforms like Facebook and Twitter. Before beginning a teleconsultation session with a patient, the attending physician must use the utmost discretion to evaluate whether or not such a consultation is appropriate and serves the patient's best interests. In such a case, the physician will need to choose which mode of communication will be the most effective during the teleconsultation.
- **The doctor must maintain the same standard of care during tele-consultation as during in-person consultation: The Telemedicine Guidelines recommend that doctors** treat patients with the same level of respect and care during teleconsultations as they would during in-person meetings. In other words, using a mobile application, email, or phone to conduct a tele-consultation by a doctor is not an acceptable defence if a medical negligence claim is brought against the doctor. If a teleconsultation is

required, medical professionals must be aware of the constraints imposed by the medium and formulate their recommendations and prescriptions accordingly.

- **The patient is responsible for the accuracy of information:** During a teleconsultation, if the doctor asks for any relevant information, the patient is responsible for giving the doctor the correct information. The Telemedicine Guidelines clarify that verifying the accuracy of any data transmitted to the doctor rests on the patient, not the doctor. In any situation, however, the doctor still has to gather all relevant medical data before making a diagnosis or treatment plan for the patient since the standard of care remains the same whether the consultation is conducted in person or remotely. If a doctor receives information from a patient that conflicts with what they already know, or if the doctor lacks sufficient confidence in the information at hand to make a professional decision, the doctor is within their rights to request additional documentation or testing as they deem appropriate as per the doctor's professional judgement.
- **The caregiver is deemed to be authorized on behalf of minor or incapacitated patients:** If the patient is 16 or younger, or if the patient is unable to provide informed consent due to mental incapacity (such as dementia) or physical impairment, it is presumed that the caregiver has the patient's permission to consult on their behalf. If the patient is over 16, the caregiver must obtain the patient's consent (such as an accident). The Telemedicine Guidelines make it abundantly apparent that a caregiver can teleconsultation with a patient even if they are not physically present in the room under such circumstances.
- **No fixed Format for issuing a prescription:** The process of prescribing a teleconsultation does not adhere to any particular pattern. The Telemedicine Guidelines have provided a format recommendation, although you are not required to follow the recommendations. On the other hand, the physician must provide a picture, scan, or digital copy of a signed prescription or an e-prescription to the patient using any messaging service or email. It is essential to remember that for a physician to transfer a prescription to a pharmacy, they must first get the patient's unequivocal agreement.
- **Invoice for fees:** Medical professionals may charge the necessary costs for tele-consultations. The patient needs to be provided with either a receipt or an invoice after the fees have been paid.

 [ISSN 2581-9453]

VI. Conclusion

Telemedicine has emerged as a potentially effective strategy to enhance the accessibility and provision of healthcare services, particularly within a geographically expansive and culturally diverse nation such as India. However, particular emphasis has been placed on the significance of data security and privacy within the rapidly advancing digital healthcare environment. The adoption of telemedicine in India hinged on patient privacy and autonomy. The prevailing regulations, such as the I.T. Act, 2000, SPDI Rules, 2011 TCCP Regulations, 2018 and the NMC Act, 2020, along with government guidelines and policies, such as National Health Policy, 2017 and NDHM, 2020, aim to provide a legal framework for telemedicine practices and address data security concerns. The SPDI Rules 2011 mandate the need for informed consent and patient's right to control their personal health information.

Additionally, since there is a lack of full-fledged legislation governing the matters pertaining to telemedicine, the Government of India, in association with the Medical Council of India, has introduced 'Telemedicine Practise Guidelines, 2020' to encourage doctors and health professionals to use telemedicine as a standard practice. With all the rapid development in the telemedicine and e-healthcare industry, there is an urgent need for healthcare providers to comply with these regulations and ensure the confidentiality, integrity, and availability of patient data. Existing rules are a good start, but more needs to be done to make and enforce special data security laws that deal with the unique problems that telemedicine brings. This law needs to regulate the encryption of patient data and its safe storage and contain strict provisions for cyber security to keep patient information secure from online threats and unauthorized access. Overall, there is a clear need for a collaborative approach involving policy-makers, healthcare providers, tech companies, and legal experts to address the data security challenges in telemedicine and birth a comprehensive set of regulations to mitigate the same. This regulation must also include regular audits and assessments for the entities involved in telemedicine to evaluate compliance with data security standards and identify areas for improvement. In conclusion, as telemedicine continues to grow in India, it will be essential to keep data secure and private to build patient trust, encourage innovation, and use digital healthcare to its fullest potential.

*****

 [ISSN 2581-9453]