TELEMEDICINE AND INFORMATION TECHNOLOGY– A CONCOCTION FOR MEDICAL FRAUDS?

Ramya Sankaran & Manoj Mohapatra[*]

Abstract

The outbreak of the Covid-19 pandemic has drastically changed the outlook of medical services globally. One of the most significant developments is the steady rise of telemedicine practice, which involves delivery of health care amenities using information and communication technologies. Telemedicine service is promising as it ensures access to health care from the comfort of the homes of patients who require medical aid. It safeguards both health care practitioners and patients from exposure to life threatening viruses and promotes their well-being. The technological tools that can be used to deliver and/or avail telemedicine services are widely subjected to regulation by legislation or guidelines, specific to their unique purpose and / or general framework governing information technology. These laws are intended to prevent commission of fraud by miscreants using information

[*] *Ramya Sankaran (Associate Partner) and Manoj Mohapatra (Legal Associate) at Gagrats, Advocates and Solicitors, Mumbai.*

technology tools, and impose obligations on the technology service providers to ensure prevention of such frauds. However, in India, neither the specific legislations governing telemedicine practice nor the general laws governing use of information technology, sufficiently address issues concerning misuse of technological tools, especially telephone/ mobile phone and chat platforms such as WhatsApp, Facebook Messenger, etc., for perpetrating medical frauds. This paper identifies the lacunae in the legal framework governing telemedicine practice in India, which is not sufficiently armed with measures that can address the dangers posed by use of telephones/ mobile phones and chat platforms to provide medical services. Furthermore, measures that can be implemented to safeguard patients from the grip of fraudulent practitioners offering telemedicine services have been evaluated and suggested, in this paper.

I. INTRODUCTION

Telemedicine is a mode of medical practice wherein health care services are delivered by health care professionals, using information and communication technologies.[1] It features the use of technology

[1] World Health Organisation Report on the Second Global Survey on eHealth, 'Telemedicine Opportunities and Developments in Member States' (*World Health Organisation*, 2010), para 1.1 <www.who.int/goe/publications/goe_telemedicine_2010.pdf> accessed 27 December 2020.

platforms specifically developed for this purpose. These include telemedicine mobile applications and websites, as also, other widely used modes of information transfer, such as telephone/ mobile phone, internet, chat platforms (viz. WhatsApp, Facebook Messenger, etc.) and data transmission systems (viz. Skype, email, fax, etc.).[2] A few examples of technological platforms which facilitate telemedicine consultations are Practo, mFine, DocsApp.

Telemedicine is a boon to the elderly, chronically ill and differently abled patients who may find it difficult to venture out of their homes to seek medical aid. It is a very useful tool for providing medical services to individuals who live in geographies where their nearest doctors are miles away. The wide range of telecommunication tools employed in telemedicine services, ensure access of medical aid to populations living in remote localities of the country where communication channels may not be well established and to people who do not own devices such as smart phones and computers that could support use of specific digital applications. The widespread use of telephone / mobile phone for audio calling and text messaging (including through WhatsApp) can help reach out to the masses, including those who are not aware of technology platforms that enable the provision of telemedicine services.

It is to be acknowledged that the practice of telemedicine can be subject to large scale misuse by fraudulent individuals who may, during a telemedicine consultation, represent themselves as a health care professional or even a patient. The risk of misuse of telephone/mobile phone and other chat platforms such as WhatsApp, Skype, etc., by fraudsters is greater than the risk of misuse of technology platforms, as the latter are subjected to increased obligations under the law to protect

[2] Board of Governors in Supersession of the Medical Council of India, 'Telemedicine Practice Guidelines Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine' (*Ministry of Health and Family Welfare*, 25 March 2020), para 1.4.1<www.mohfw.gov.in/pdf/Telemedicine.pdf> accessed 27 December 2020.

the interest of patients by *inter alia* preventing identity theft and medical fraud. For instance, the Telemedicine Practice Guidelines Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine of India[3] ("**Guidelines**"), requires technology platforms that work with a network of medical practitioners, enabling patients to consult via their platform, to conduct due diligence of these medical practitioners before listing them on their mobile application / website.[4] The Guidelines also contain plenary provisions which provide for blacklisting of these technology platforms in the event of any violation of the same.[5] However, telephone operators/ telecom service providers and chat platforms are not subjected to such oversight under the Guidelines. This disparity in regulation/oversight of the technology platforms on one hand and the telephone service providers and chat platforms on the other hand, has the potential to make the users of chat platforms and telephone services, vulnerable to medical frauds.

This paper aims to emphasize 'medical frauds' in the practice of telemedicine from the perspective of possible identity theft by individuals posing as Registered Medical Practitioners (as defined below); and breach/ misuse of confidential / medical information of patients due to such identity thefts. The paper further highlights the practical issues of identification and 'tracing' of fraudulent individuals in light of the inherent limitations of certain technological tools such as telephones/mobile phones and chat platforms. The authors also explore the enactment of a specific and more comprehensive preventive legislation as a solution to identity theft whilst availing telemedicine services.

[3] Board of Governors in Supersession of the Medical Council of India, 'Telemedicine Practice Guidelines Enabling Registered Medical Practitioners to Provide Healthcare Using Telemedicine' (*Ministry of Health and Family Welfare*, 25 March 2020) <www.mohfw.gov.in/pdf/Telemedicine.pdf> accessed 27 December 2020.
[4] ibid para 5.2.
[5] ibid para 5.7.

II. BRIEF OVERVIEW OF THE TELEMEDICINE PRACTICE GUIDELINES

Until recently, there was no legal framework governing the practice of telemedicine in India. In fact, the Hon'ble Bombay High Court in *Deepa Sajeev Pawaskar & Anr. v. The State of Maharashtra*,[6] had questioned the legitimacy of the practice of telemedicine in India, at least with respect to telephonic consultations. The Hon'ble High Court in the said case, *inter alia* held that prescription of medicines to patients, via telephone, without making sufficient inquiry regarding their symptoms constituted culpable negligence, attracting criminal liability under the Indian Penal Code, 1860 ("**IPC**").

In March, 2020, in wake of the Covid-19 pandemic the Ministry of Health and Family Welfare, Government of India[7] ("**MoHFW**") notified the Guidelines, containing overarching principles and practical framework, to enable Registered Medical Practitioners to provide healthcare services through information and communication technologies. India followed the practice of introducing the said Guidelines as a non-legislative measure, similar to the practice adopted in Singapore[8] and Australia.[9]

[6] SCC OnLine Bom 1841

[7] Ministry of Health and Family Welfare Government of India (2020) <www.mohfw.gov.in/> accessed 27 December 2020

[8] Ministry of Health Singapore, 'National Telemedicine Guidelines' (2015) <www.moh.gov.sg/docs/librariesprovider5/resources-statistics/guidelines/moh-cir-06_2015_30jan15_telemedicine-guidelines-rev.pdf> accessed 27 December 2020; The Ministry of Health of Singapore ("MoHS").

[9] Medical Board of Australia, 'Guidelines for Technology Based Consultations by Patients' (16 January 2012) <www.medicalboard.gov.au/Codes-Guidelines-Policies/Technology-based-consultation-guidelines.aspx> accessed 27 December 2020.

However, to provide statutory validity to the Guidelines, the Board of Governors in the Super Session of Medical Council of India adopted the Guidelines vide the Indian Medical Council (Professional Conduct, Etiquette and Ethics) (Amendment) Regulations, 2020[10] ("**Amendment Regulation**"), which amended the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 ("**Regulation**"). By virtue of the Amendment Regulation, Registered Medical Practitioners under the IMC Act, have been authorised to provide telemedicine consultations in accordance with the Guidelines,[11] which have now been made part of the Regulation by its incorporation in Appendix 5 thereof. It is pertinent to note that the Regulation was issued under Section 20A read with Section 33(m) of the Indian Medical Council Act, 1956 ("**IMC Act**") which authorizes the Indian Medical Council to make regulations prescribing standards of professional conduct, etiquette and ethics for medical practitioners. Therefore, the incorporation of the Guidelines as Appendix 5 of the Regulation, makes any violation of the terms of the Guidelines on part of a physician, a professional misconduct, attracting disciplinary action in terms of Chapter 7 of the said Regulation.

As per the Guidelines, 'Telemedicine' involves delivery of health care services by Registered Medical Practitioners using information and communication technologies. These include:

(x) communication leveraging information technology platforms (viz. Voice, Audio, Text & Digital Data exchange);[12] and

[10] Medical Council of India, 'Board of Governors in Super Session of Medical Council of India Notification' (Medical Council of India, 25 March, 2020) <www.mciindia.org/CMS/wp-content/uploads/2019/10/Public_Notice_for_TMG_Website_Notice-merged.pdf> accessed 26 June 2020 (link not active).
[11] ibid para 3.8
[12] Board of Governors (n 2) para 1.2.

(y) telemedicine tools such as (i) telephone, (ii) video, (iii) devices connected over LAN, WAN or internet, (iv) chat platforms (viz. WhatsApp, Facebook Messenger etc.), (v) mobile app, (vi) internet based digital platforms for telemedicine or (v) data transmission systems (viz. Skype/ email/ fax etc.)[13]

The Guidelines define a Registered Medical Practitioner ("**RMP**") as a person enrolled in the State Medical Register or the Indian Medical Register maintained in accordance with the IMC Act.[14] Furthermore, Sub- Regulation 1.1 of Regulation 1(B) of the Regulation which deals with character of a physician, describes a physician as, a doctor having a qualification of MBBS or an MBBS with a post graduate degree/ diploma or an equivalent qualification in any medical discipline.[15] The Regulation also provides that no person other than a doctor who has the requisite qualifications as prescribed by the Medical Council of India ("**MCI**"), and who has registered himself/herself with the Indian Medical Council / State Medical Council, shall practice medicine.[16] Therefore, unless the aforementioned criteria are met, no person can practice telemedicine in India.

The Guidelines cover telemedicine consultations as between (a) a patient and an RMP,[17] (b) a patient and an RMP through a caregiver,[18]

[13] ibid para 1.4.1.
[14] ibid para 1.3. See also Code of Criminal Procedure, 1973, s 53 Ex. (b) - which defines a "registered medical practitioner" as "*a medical practitioner who possesses any medical qualification as defined in clause (h) of section 2 of the Indian Medical Council Act, 1956 (102 of 1956) and whose name has been entered in a State Medical Register*."
[15] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
[16] ibid, para 1 (B) (1.1.3). See also Indian Medical Council Act, 1956, s 23.
[17] Board of Governors (n 2) para 4.1.
[18] ibid para 4.2; A caregiver, for the purpose of the Guidelines, could either be a family member of the patient or any member who the patient authorizes to represent him/her.

(c) a health worker and an RMP[19] and (d) an RMP and another RMP/ specialist.[20] For the purpose of this paper, the authors will however, restrict their analysis to consultations as between an RMP and a patient.

Under the Guidelines, an RMP is entitled to provide telemedicine consultations to patients from across any part/ region of India.[21] The Guidelines mandates RMPs providing telemedicine services to uphold the same professional and ethical norms and standards as are generally applicable to in-person treatments, but within the inherent limitations of the practice of telemedicine.[22] In addition to prescribing medicines to patients, an RMP is also permitted under the Guidelines to provide health education and counselling to its patients.[23] Imparting health education would include information pertaining to diet, physical activities, hygiene practices, etc.[24] Counselling would be a more specific advice given to patients depending upon their underlying condition such as food restrictions, home physiotherapy etc.[25] The ambit of telemedicine services as under the Guidelines is hence broad in nature.

The Guidelines necessitate obtaining a patient's consent by the RMP, in case of any telemedicine consultation.[26] A patient's consent can either be implied or explicit.[27] In case the patient contacts an RMP and wishes to obtain consultation, then in such a scenario the patient's consent is implied.[28] However, if it is an RMP who wishes to initiate a

[19] ibid para 4.3; A "health worker", for the purpose of the Guidelines "*could be a Nurse, Allied Health Professional, Mid-Level Health Practitioner, ANM or any other health worker designated by an appropriate authority*".
[20] Board of Governors (n 2) para 4.4
[21] ibid para 1.3.1
[22] ibid para 1.3.2
[23] ibid para 3.7
[24] ibid para 3.7.2
[25] ibid para 3.7.3
[26] ibid para 3.4
[27] ibid para 3.4
[28] ibid para 3.4.1

consultation, then an explicit consent from the patient has to be obtained.[29] An RMP should aim to obtain sufficient medical information pertaining to the patient before making a professional judgment.[30] Upon taking a holistic view of the situation, an RMP should be reasonably comfortable as to whether a telemedicine consultation would be in the interest of the patient.[31] If physically examining a patient is necessary to obtain critical information for the purposes of consultation, then an RMP should not proceed with the consultation unless the patient is physically examined.[32] Furthermore, in cases of emergency, the Guidelines provide that all patients must be advised to obtain immediate in-person consultation with the RMP.[33] However, if the RMP is of the opinion that a patient's condition can be appropriately managed through a telemedicine consultation, an RMP can proceed to, as discussed above, prescribe medicines, provide health education and/or counselling.[34] Here, it is extremely pertinent to note that an RMP cannot prescribe to a patient any medicine that is listed in Annexure 1 of the Guidelines.[35]

Furthermore, under the Guidelines, it is incumbent on an RMP to *inter alia* maintain from time to time (a) a record of the telemedicine interaction with a patient which may include phone logs, text messages etc., (b) patient records, reports, (c) a record of prescriptions that the RMP may have provided to the patient.[36] The Guidelines require every RMP to display his/her registration number as designated by the State Medical Council or the Indian Medical Council on prescriptions,

[29] ibid para 3.4.2
[30] ibid para 3.5
[31] ibid para 3.1.1
[32] ibid para 3.5.1
[33] ibid para 4.5
[34] ibid para 4.1.1.2
[35] ibid para 3.7.4; Para 3.7.4 also includes "*Medicines listed in Schedule X of Drug and Cosmetic Act and Rules or any Narcotic and Psychotropic substance listed in the Narcotic Drugs and Psychotropic Substances, Act, 1985*"
[36] ibid para 3.7.2

electronic communication etc. given to the patients.[37] Additionally, the Guidelines also impose an obligation on an RMP to protect patients' privacy and confidentiality.[38] An RMP bears the responsibility of being cognizant of the data protection and privacy laws and should fully abide by such laws in order to protect the confidentiality of his/her patient similar to the way in which they would protect patient information in in-person care.[39] However, RMPs shall not be responsible for breach of confidentiality of the patient if there is reasonable evidence to show that such a breach was a result of either a technology breach or a breach by a person other than the RMP.[40]

As stated above, the Guidelines permit an RMP to provide telemedicine consultations *inter alia* using tools such as telephones, chat platforms, technological platforms, such as mobile applications and websites, etc.[41] Thus, various modes of communication devices could be employed in rendering telemedicine consultations. However, these technological tools have certain limitations which have been identified to an extent under the Guidelines. Firstly, in the cases of communication done through 'audio' mode, such as by the use of telephones / mobile phones, the Guidelines *inter alia* provide that the said mode could be used by imposters who may represent themselves as the real patients.[42] In this regard, it is pertinent to note that in addition to the risk of imposters representing themselves as the real patients, there is also an additional risk of imposters exhibiting themselves as an RMP over the telephone which has not been identified in the Guidelines. Secondly, in the case of 'text-based' communication, such as the use of WhatsApp, SMS etc., the Guidelines *inter alia* provide

[37] ibid, para 3.2.5
[38] ibid para 3.7.1.1
[39] ibid para 3.7.1.2
[40] ibid para 3.7.1.3
[41] ibid para 1.4.1.
[42] Board of Governors (n 2) para 2.

that there cannot be any surety of the identity of a doctor or a patient.[43] Thirdly, in the case of 'video' based communication done through the use of video facilities, for instance on chat platforms, the Guidelines *inter alia* stipulates that a patient's privacy can be compromised.[44] Hence, in light of these limitations, one must not ignore the possibility of large scale misuse by fraudulent individuals who may choose to represent themselves as RMPs, and exploit the discrepancies/ limitations inherent in the use of these technologies.

In this regard, it is pertinent to note that the Guidelines impose an obligation on the RMP to put in place a mechanism, whereby the RMP's credentials and contact details could be verified by a patient availing telemedicine consultation. Furthermore, in relation to telemedicine services provided via technological platforms (which are specially designed to provide telemedicine services) such as Mobile Apps, websites that work across a network of registered RMPs, the Guidelines additionally impose an obligation on the technology platforms to ensure that consumers are consulting with duly registered RMPs.[45] This is done by imposing obligations on technology platforms to conduct due diligence (i.e. comprehensive measures of verification) before listing any RMP on their platforms.[46] Furthermore, for consumers' ease of reference, platforms are mandated to provide details such as name, qualification, registration number and contact details of all the RMPs listed on their respective platforms.[47] In case any non-compliance with respect to the same is noted, technology platforms are bound to report to the Board of Governors in supersession of the MCI, who may then choose to take appropriate action.[48]

[43] ibid
[44] ibid
[45] ibid para 2.5.1
[46] ibid para 2.5.2
[47] ibid para 2.5.2
[48] ibid para 2.5.3 - For present list of Board of Governors in supersession of the MCI *See*, 'Board of Governors', Medical Council of India (2020)

Importantly, the Guidelines also mandate the technology platforms to have adequate mechanisms in place to address grievances or queries of consumers.[49] The rigidity of the Guidelines in regulating the technology platforms can further be substantiated on the basis that, any violation by the technology platform may lead to the said platform being blacklisted, and in such an event, no RMP would be permitted to use the said platform to provide telemedicine services.[50]

However, in relation to other modes of telecommunication, such as telephone, WhatsApp, skype, etc. the obligation to establish a mechanism through which a patient can verify an RMP's credentials is solely imposed on such RMP.[51]

III. ANALYSIS OF THE INFORMATION TECHNOLOGY LAWS APPLICABLE TO TELEMEDICINE PRACTICE

Apart from the IMC Act and the Regulation, the information technology laws in India also play a pivotal role in the practice of telemedicine since telemedicine consultations are provided by RMPs using different forms of information technologies mentioned above. In this regard, the Guidelines do expressly stipulate that the information technology aspect is primarily governed by the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, in addition to the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,

<https://www.mciindia.org/CMS/about-mci/office-bearers> accessed 27 December 2020. Link not active

[49] Board of Governors (n 2) para 2.5.6.

[50] ibid para 5.7

[51] ibid para 3.2.2

the authors are of the opinion that the Information Technology (Intermediaries Guidelines) Rules, 2011 ("**IT IG Rules**)" would play an equally important role in the regulation of the information technology aspect in India. It is essential to note that the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 ("**Draft Rules**") were published by the Ministry of Electronics and Information Technology on 24th December, 2018, but are yet to come into force. However, assuming that the Draft Rules come into force in the present manner, reference would be made to the Draft Rules, in this paper, as and when relevant for the purposes of this article.

In this section, the authors have examined certain relevant provisions of the information technology that are applicable to the practice of telemedicine. The analysis in this section is restricted to only those sections that are crucial to the discussion in this paper.

In order to understand the applicability of information technology laws to the practice of telemedicine, emphasis needs to be laid on some of the salient provisions of the IT Act. The expressions 'addressee'[52], 'originator'[53] and 'intermediary'[54] as defined in the IT Act would bring clarity in understanding the context in which communication would take place between an RMP and a patient. In the practice of

[52] An addressee "*means a person who is intended by the originator to receive the electronic record but does not include any intermediary*"; The Information Technology Act 2000, s 2(1)(d).

[53] An originator "*means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary*"; The Information Technology Act 2000, s 2(1)(za).

[54] *Intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes*. The Information Technology Act 2000, s 2(1)(w).

telemedicine, an 'originator' or an 'addressee' could either be an RMP who disseminates information to people about him/her offering telemedicine services or a prospective patient who contacts an RMP to obtain telemedicine consultation. For example, if a prospective patient sends a text message to an RMP to obtain telemedicine consultation, then in that scenario, the person sending the text message would be the 'originator' and the RMP receiving the text message would be the 'addressee'.

However, it is pertinent to note that the said transfer of information between the RMP and a prospective patient is facilitated by a medium i.e., an intermediary. The expression 'intermediary' is defined in the IT Act, and means any person who receives, stores or transmits any electronic record[55] on behalf of another person. It is essential to state that the definition of an 'intermediary' as under the IT Act is inclusive in nature and includes telecom service providers, web-hosting service providers etc. Some examples of telecom service providers would include Airtel, Vodafone etc. and web-hosting service providers would include GoDaddy, Hostinger etc. In light of the said definition, it can be safely assumed that the majority of tools of telemedicine as prescribed under the Guidelines, such as telephones, mobile phones, chat platforms such as WhatsApp,[56] Facebook Messenger, technology

[55] "*Electronic record*" means "*data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche*"; The Information Technology Act 2000, s Section 2(1)(t); and "*data*" means "*a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer*"; The Information Technology Act 2000, s 2(1)(o)

[56] The Ministry of Electronics and Information Technology in a response to a Lok Sabha question responded by stating that "*WhatsApp is intermediary within the definition of the Information Technology (IT) Act, 2000*"; Lok Sabha, 'Unstarred question no. 1415' (*Lok Sabha,* 27 November 2019)

platforms such as Mobile apps and websites, would fall within the purview of an 'intermediary' as under the IT Act. The said assumption can be derived from the fact that all of the afore stated tools would act as the medium to receive, store or transmit any form of communication between the RMP and a patient.

The use of a wide range of intermediaries'/ technological tools for the practice of telemedicine also raises a fear of its misuse by imposters exhibiting themselves as an RMP. The importance of intermediaries in facilitating the practice of telemedicine in India and a possible scope of their misuse warrants a question: 'How are intermediaries governed under the information technology laws of India?' The IT IG Rules lay down the mandatory procedures which all intermediaries would have to abide to. These mandatory procedures include observing due diligence when intermediaries publish their privacy policies, user agreements etc. on their platform.[57] Such privacy policies, user agreements etc. as published by intermediaries shall inform users of their platform to not host, display, publish, upload, modify, transmit, update or share any information which *inter alia* impersonates any person or violates any law for the time being in force.[58] Thus, in light of the same, telecom service providers, chat platforms and technology platforms, also being intermediaries in the practice of telemedicine, would be mandated to fulfill the above due diligence procedures.

It is questionable as to whether the above due diligence procedures of merely informing the users to not engage in certain practices would restrain imposters from carrying out fraudulent activities by acting in the guise of an RMP. In the opinion of the authors, such procedures may not cause restraint amongst imposters, however, they may in fact safeguard an intermediary from incurring any liability for the act of an

<http://loksabhaph.nic.in/Questions/QResult15.aspx?qref=7809&lsno=17> accessed 27 December 2020

[57]The Information Technology (Intermediaries Guidelines) Rules 2011, Rule 3

[58]The Information Technology (Intermediaries Guidelines) Rules 2011, Rule 3 (2)

imposter as under Section 79 of the IT Act. Section 79 of the IT Act exempts intermediaries from incurring liability in certain circumstances. For instance, intermediaries are not liable for hosting / making available information, data or communication links of third parties if either (a) the function of the intermediary was solely to facilitate access to a communication system or (b) the intermediary had no role in initiating the communication, selecting the receiver of the communication and selecting or modifying the information which was contained in the said communication or (c) the intermediary has observed the procedure of due diligence as under the IT Act and the IT IG Rules. Therefore, in the practice of telemedicine, for instance where the chat platform 'Facebook' is the intermediary, Facebook may evade liability for the act of an imposter who had accessed and misused its platform by establishing either that (a) it had merely facilitated access to its communication system or (b) it had no role in initiating the communication between the imposter and a patient, selecting the patient and selecting or modifying the information that the imposter and / or the patient had communicated with each other or (c) it had observed the procedure of due diligence (as discussed above) as under the IT Act and the IT IG Rules.

IV. DISPARITY IN THE REGULATORY FRAMEWORK

On a fair reading of the Guidelines, it is apparent that the chief purpose of the Guidelines is to safeguard the health and lives of the patients and also to prevent offenders from making use of information technology to defraud patients. Ancillary to this purpose is the protection of the privacy and confidentiality of the users availing telemedicine services.

As discussed earlier, due diligence of RMPs is required to be carried out by the technological platforms, in terms of the provisions of the Guidelines, prior to their listing therein, in order to ensure that the said RMPs are duly registered with the concerned medical councils and also

comply with the relevant laws. These technology platforms are also mandated to provide the names, qualifications, registration numbers and contact details of all the RMPs listed on their portal. These measures are intended to protect the users of telemedicine services from medical frauds ranging from identity theft (impostors claiming to be RMPs) to dissemination of incorrect credentials by RMPs to provide services which they are qualified to render.

It is relevant to note that although many RMPs may choose to register themselves with technology platforms in order to provide telemedicine services, a significant proportion of healthcare professionals may opt for providing such services individually, on their own account, by using tools such as telephones, chat platforms such as WhatsApp, Facebook Messenger etc. WhatsApp for instance is considered to be a quick, cost-effective and user-friendly tool in the clinical health sector.[59] However, unlike technology platforms, such tools are not subject to any scrutiny under the Guidelines. In defense of the Guidelines, telephones and chat platforms are designed for a broad array of services and not specifically for telemedicine practice and hence, cannot in any case either be subject to regulation under the Guidelines or fall under the regulatory purview of MoHFW/ MCI. Also, it may not be practically feasible for certain service providers that do not specifically create portals for telemedicine services to render the kind of security that the applications such as technology platforms can provide. Nevertheless, this leads to users who avail telemedicine amenities through telephone and other chat applications, not being guaranteed the same degree of protection by the Guidelines. Telephone operators/ telecom service providers and chat platforms are not required to particularly scrutinize the identity of the persons providing telemedicine facilities using their platform. This gap in the legal framework leaves open to the fraudsters an opportunity

[59] CJ Opperman and M Janse van Vuuren, 'WhatsApp in a Clinical Setting: The Good, the Bad and the Law' (2018) 11(2) South African Journal of Bioethics and Law 102.

to not only commit medical frauds, but also get hold of and misuse private and confidential data of the patients that use these tools of telemedicine.

Furthermore, as discussed above, the Guidelines solely leave it to the RMPs to ensure that there is a mechanism for a patient to verify their credentials and contact details when tools such as telephones, mobile phones, chat platforms, etc. are used to render telemedicine services. In this regard, the Frequently Asked Questions on Telemedicine Practice Guidelines[60] issued by the Board of Governors in supersession of the MCI provide that RMPs should mention/ display their Indian Medical Councilor State Medical Council registration number for teleconsultations. It further provides that the patients may, if they desire, cross verify the registration details of the RMPs on the websites of relevant medical councils. However, it is pertinent to note that the websites of the medical councils contain only the names of the RMPs and their registration details, such as registration number, qualification, registration date and validity.[61] Since the aforesaid websites do not provide a mechanism to a patient to verify the contact details of an RMP, the patient would be unable to ascertain if they are indeed in contact with the RMP as listed / displayed therein.

Thus, there is clearly a disparity in regulation of provision of telemedicine services when, on one hand, specific technological platforms are used and on the other hand, common telecommunication

[60] Board of Governors in Supersession of the Medical Council of India, 'Frequently Asked Questions [FAQs]on Telemedicine Practice Guidelines', Medical Council of India.
<https://mciindia.org/MCIRest/open/getDocument?path=/Documents/Public/Portal/LatestNews/Final_FAQ-TELEMEDICINE%20%206-4-2020..pdf>accessed 26 June 2020.

[61] Maharashtra Medical Council, Mumbai, 'RMP Information' (2020) <https://www.maharashtramedicalcouncil.in/frmRmpList.aspx> accessed 27 December 2020.

channels such as telephone/ mobile phones and other chat platforms are used.

V. RISK OF IDENTITY THEFT AND BREACH OF DATA PRIVACY

The aforesaid loophole in the regulation of telemedicine practice in India can lead to issues of identity theft of RMPs and breach of data privacy of the patients who avail such services.

The term identity theft connotes a crime wherein a person's personal data is wrongfully obtained by another and is used by the latter for fraudulent or deceptive purpose, typically for economic gain.[62] In India, there is no legislation that specifically defines the term identity theft. Section 66C of the IT Act[63] lays down the punishment for identity theft and stipulates that fraudulent and dishonest use of electronic signature, password or any other unique identification feature of any other person, would be punishable with imprisonment extending up to a period of three years and fine up to Rupees 1 lakh. Section 66D of the IT Act provides punishment for cheating by personation by using any communication device or computer resource.[64] Though the aforesaid

[62] The United States Department of Justice, 'Identity Theft' (16 November 2020) <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> accessed 27 December 2020

[63] *S 66C- "Punishment for identity theft. – Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh"*

[64] *S 66D- "Punishment for cheating by personation by using computer resource. – Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees"*

provisions of the IT Act penalize the offense of identity theft, they are preventive provisions which can safeguard the interest of patients.

Use of telephone/mobile phones and chat applications, being intermediaries, pose a real danger of identity theft. The details of the RMP which are available on the websites of the relevant medical council can be conveniently misused by an imposter. This could jeopardize the health and lives of persons seeking medical aid using telecommunication devices and platforms other than specialized telemedicine apps. Furthermore, apart from the aforesaid, any information provided by the users of these telecommunication devices / platforms to such imposters could also be appropriated for fraudulent and dishonest use.

VI. 'TRACING' OF IMPOSTORS AND ITS LIMITATIONS

The IT IG Rules impose certain obligations on the intermediaries, wherein intermediaries are, when required by a lawful order, obliged to provide information or any assistance to authorized Government agencies for investigative, protective and cyber security activity.[65] The Draft Rules, assuming that they will come into force in the present manner, aim to further expand this obligation of the intermediaries by requiring them to enable tracing of originators of information on their platform.[66] Therefore, under the Draft Rules, if required by lawfully

[65] (7) *When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.*;

[66] *"(5) When required by lawful order, the intermediary shall, within 72 hours of communication, provide such information or assistance as asked for by any*

authorized Government agencies, intermediaries will be bound to trace the originators who have used their platform to transmit disputed information. In the sphere of telemedicine services, a telecom service provider (in case mobile phone has been used by an imposter to communicate with a customer over a mobile call), chat platforms (in case such platform has been used by an imposter to communicate with a customer) or technology platforms may be required by any lawfully authorized Government agency to trace the originator of any disputed information.

This novel concept of 'tracing' as under the Draft Rules can here be interlinked with the disparity as maintained by the Guidelines in solely overseeing/regulating technology platforms and not telephones/mobile phones or chat platforms. It can be noted here that tracing of the originator by a technology platform can be successfully undertaken since technological platforms are mandated to conduct due diligence of RMPs before listing them. In case a technology platform fails to conduct such due diligence, they may be blacklisted.

The primary question that needs to be addressed then is: "*How far is 'tracing' an imposter a possibility, particularly when the more convenient/easily accessible tools of telephones/mobile phones and chat platforms have been put to use in the practice of telemedicine*?". It is clear that if an imposter is successfully traced, the provisions governing identity theft under the IT Act, as discussed above, can be exercised to punish the imposter for his/her fraudulent act. However, considering the large possibility of imposters (a) obtaining stolen SIM cards or (b) purchasing SIM cards by providing fake or incorrect details

government agency or assistance concerning security of the State or cyber security; or investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto. Any such request can be made in writing or through electronic means stating clearly the purpose of seeking such information or any such assistance. The intermediary shall enable tracing out of such originator of information on its platform as may be required by government agencies who are legally authorized.

or (c) using fake caller ID information,[67] it would be practically impossible for telecom service providers to trace the originator of the information. Furthermore, chat platforms like WhatsApp feature End-to-End Encryption ("**ETEE**"). An ETEE feature allows only the originator and the addressee to view and read what is sent and received by them. Even WhatsApp cannot have any access to such information which the originator and addressee have shared amongst themselves.[68] An ETEE feature would therefore make it impossible to track the originator of information, unless a mechanism of traceability is built in the said platform.[69] The requirement of 'tracing' may in fact be technically impossible to satisfy for many intermediaries.[70]

Therefore, even if the mechanism of 'tracing' as envisaged under the Draft Rules comes into force, it may be very unlikely to get a grip on imposters practicing telemedicine on a large scale across India using tools such as telephone/mobile phones and chat platforms.

---

[67] Andrew Johnson, 'Scammers can fake caller ID info*'* (*Federal Trade Commission Consumer Information*, 4 May 2016) <https://www.consumer.ftc.gov/blog/2016/05/scammers-can-fake-caller-id-info> accessed 27 December 2020

[68] "*Security by Default*
WhatsApp's end-to-end encryption is available when you and the people you message use our app. Many messaging apps only encrypt messages between you and them, but WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages."; WhatsApp, 'WhatsApp Security' (2020) <https://www.whatsapp.com/security/> accessed 27 December 2020

[69] Press Trust of India, 'WhatsApp Reject's India's Demand for Message Traceability' (*NDTV*, 23 August 2018) <https://www.ndtv.com/india-news/whatsapp-rejects-indias-demand-for-message-traceability-1905217> accessed 27 December 2020

[70] Software Freedom Law Centre, 'The Future of Intermediary Liability in India' (2020) <https://sflc.in/future-intermediary-liability-india> accessed 27 December 2020

VII. WILL SINGLE-MODALITY COMMUNICATION INCREASE SCOPE OF MEDICAL FRAUDS?

Single-modality communication involves communication primarily through one mode of communication (i.e., solely through telephonic conversations (audio) or text messages, email exchanges etc. (text) or skype etc. (video)), as opposed to multi-modal communication which involves use of more than one mode of communication (i.e., video consultations with patients along with text communication).[71] On a fair reading of the Guidelines, it is clear that telemedicine consultations in India can be provided through either single-modal and/or multi-modal communication.

It is relevant to note that in the States of Oklohoma[72] and Maine[73] of the United States of America, the definition of 'telemedicine' expressly

---

[71] General Medical Council, 'Regulatory Approaches to Telemedicine' (1 March 2018) <www.gmc-uk.org/about/what-we-do-and-why/data-and-research/research-and-insight-archive/regulatory-approaches-to-telemedicine> accessed 27 December 2020

[72] Telemedicine "*means the practice of health care delivery, diagnosis, consultation, evaluation and treatment, transfer of medical data or exchange of medical education information by means of a two-way, real-time interactive communication, not to exclude store and forward technologies, between a patient and a physician with access to and reviewing the patient's relevant clinical information prior to the telemedicine visit*." Furthermore, "*Telemedicine" and "store and forward technologies" shall not include consultations provided by telephone audio-only communication, electronic mail, text message, instant messaging conversation, website questionnaire, nonsecure video conference or facsimile machine*"; 'Enrolled Senate Bill 726' (*Oklahoma Medical Board*, 17 May 2017) <www.okmedicalboard.org/download/877/sb726_Telemedicine_Law_Nov_1_2017.pdf> accessed 27 December 2020

[73] Telemedici*ne "means the practice of medicine or the rendering of health care services using electronic audio-visual communications and information technologies or other means, including interactive audio with asynchronous store-and-forward transmission, between a licensee in one location and a patient in another location with or without an intervening health care provider. Telemedicine includes*

excludes medical services that are provided solely through audio-only communication, text messages, instant messaging communication etc. Therefore, in these states, telemedicine services cannot be provided through single-modality communication. The regulator in the said states mandates communication in telemedicine services to be multi-modal. One of the reasons for such an approach, in the age of enhanced use of information technologies, could be the difficulty in verifying the person's identity who is acting as an RMP.

As discussed above, higher risks of medical frauds such as identity theft in the practice of telemedicine may surface from the use of telephone/mobile phones and chat platforms. The risk of medical frauds by imposters are likely to be more prevalent in cases where telemedicine consultations are provided through single-modality communication. The Guidelines do obligate RMPs to exercise their professional judgment in determining whether a telemedicine consultation is appropriate in the first place and whether the circumstances warrant an in-person consultation with the patient.[74] An RMP may, upon considering the circumstances, use his/her best judgement in determining mode of technology to be used to offer telemedicine consultations.[75] However, it is pertinent to note that the said scrutiny as under the Guidelines are for RMPs. An imposter acting under the guise of an RMP may either not be aware of the Guidelines or even if he/she is, such Guidelines are unlikely to restrain him/her from committing medical frauds.

---

asynchronous store-and-forward technologies, remote monitoring, and real-time interactive services, including teleradiology and telepathology. Telemedicine shall not include the provision of medical services only through an audio-only telephone, e-mail, instant messaging, facsimile transmission, or U.S. mail or other parcel service, or any combination thereof.; Government of Maine, 'Telemedicine Standards of Practice' (2016) <www.maine.gov/md/sites/maine.gov.md/files/inline-files/Chapter_6_Telemedicine%20.pdf> accessed 27 December 2020

[74] Board of Governors (n 2) para 3.1.1

[75] Board of Governors (n 2) para 3.3.3

In light of the same, it seems fair to conclude that the concerns of 'identity theft' in the practice of telemedicine in India can to an extent, in instances where a patient can identify the doctor on sight, be eliminated by excluding single-modality communication, since patients would then be more capable of ensuring that the person providing them telemedicine services is an RMP. However, it is essential to note that not many people in India may be possessing mobile phones with a camera so as to enable them to obtain video consultation. Also, even if a person is possessing a mobile phone which does have a camera, issues concerning internet connectivity may make it difficult to obtain a video consultation. Thus, although the Guidelines seem to allow use of either single-modal and/or multi-modal communication, excluding single-modal communication would exclude a large proportion of the Indian population from availing telemedicine services. Additionally, considering the fact that not all patients would be aware of the physical appearances of RMPs from whom they wish to avail telemedicine services, requiring mandatory multi-modal communication under the Guidelines would not be of much help.

VIII. RECOMMENDATIONS – PREVENTION OF MISUSE OF GENERAL MODES OF TELECOMMUNICATION IN TELEMEDICINE PRACTICE

In light of the issues identified in the sections hereinabove, the authors suggest implementation of the following preventive measures in the Regulation:

(i) Making identity verification of RMPs Mandatory

This can be done through providing photo identification of RMPs along with their other details in the websites of the relevant medical council and in a website / mobile application created specifically by the relevant authority to create awareness about telemedicine services. Restricting use to only registered phone numbers and verified chat applications accounts and messengers accounts for provision of telemedicine services – the details of dedicated phone numbers and chat application account details that are verified by the relevant medical council should be displayed on the aforesaid website / mobile application devoted specifically to create awareness regarding telemedicine services.

To address the possibility of an RMP changing his / her phone number over the course of time, provisions must be made regarding immediate notification and updating of any change of such information in (a) the websites of the relevant medical council and (b) in the website / app created to provide general awareness to the users of the telemedicine services.

For remote areas of the countries and users who do not have devices that support use of the aforesaid mobile applications / websites that contain details of the RMPs, dedicated toll-free number must be provided where patients can receive details regarding RMPs who can provide telemedicine services in their locality and their registered telephone numbers / verified chat application accounts.

The aforementioned safeguards should also be implemented with respect to telemedicine services provided using specific telemedicine mobile applications/ websites. It is pertinent to note that, providing photo identification and details of the registered phone numbers of RMPs on the websites of the relevant medical councils would also significantly axe the drawbacks of single-modality communication in telemedicine practice.

(ii) Sensitizing the users of telemedicine services to only deal with verified RMPs

The users of the telemedicine services should be sensitized to receive medical help only from verified phone numbers and chat applications accounts of the RMPs, and only after confirming the same on the toll-free number allotted in their area/locality or dedicated mobile application / website established for this purpose.

Users should also be sensitized on availing medical facilities on unregistered numbers and the dangers of identity theft and data piracy.

(iii) Dissemination of information regarding telemedicine apps and toll-free numbers

The users should be made aware of the website / mobile application specifically established for facilitating telemedicine facilities where the phone numbers and the identities of the RMPs can be cross verified. The toll free numbers where patients can call to receive details regarding doctors in their area who provide telemedicine services should also be widely distributed publicly from a reliable source.

Media, government notices, government messages, pamphlets etc. could be employed for disseminating details of the aforesaid.

(iv) Enactment of Specific Preventive Legislation

A comprehensive legislation should be enacted to prevent exploitation of patients who use telemedicine services. This legislation should be specific to the issues of telemedicine, and seek to prevent medical malpractice, and fraud in use of the telecommunication tools as well as protect the privacy and confidentially of the patients availing such telemedicine services. The authors are of the opinion that such legislation would effectively address information technology nuances

specific to the practice of telemedicine when compared to having two legislations enacted – one dealing with the medical aspect and the other dealing with the information technology aspect.

(v) Establishment of New Administrative Bodies

The practice of telemedicine is at a nascent stage but has the potential for rapid growth in India. However, in order for the benefits of telemedicine to reach the masses without being subject to frauds, new administrative bodies both at National and State/District levels need to be established to *inter alia* (a) provide assistance to both RMPs and patients in providing and availing telemedicine services, respectively; (b) address grievances of users availing telemedicine services; and (c) monitor the practice of telemedicine in general.

IX. CONCLUSION

Unlike other forms of frauds, medical fraud has the potential to risk lives and health of many people. Ensuring that only an RMP is providing telemedicine service is extremely essential in order to maintain public confidence in the practice of telemedicine, especially in today's world where telemedicine consultations have become the need of the day. The MoHFW and the MCI have a crucial role in making telemedicine services safe and accessible to the Indian population, some of whom are technologically and geographically challenged.

The authors are of the opinion that the aim, currently, should be to introduce measures that prevent medical frauds such as identity thefts. It is insufficient to merely leave it to the general legislation on information technology to identify (i.e., trace) and punish fraudulent individuals committing such identity thefts as only prevention thereof

can safeguard the lives and health of millions of patients from the danger of getting wrong treatment. This is vital in a country like India considering the fact that laws regarding identity theft are still upcoming and yet to be comprehensively explored.

Furthermore, general legal framework on information technology and IPC contain provisions relating to data privacy, punishment for identity theft, fraud etc., but only a special statute, specific to telemedicine practice and frauds perpetrated in relation thereto would be able to address the nuances of the field by stipulating preventive measures as recommended by the authors in the previous section.

In light of the aforesaid, the authors suggest that a comprehensive telemedicine legislation should be enacted and an administrative body to oversee the telemedicine practice in India should be established to effectively tackle the upcoming and growing need of telemedicine services.