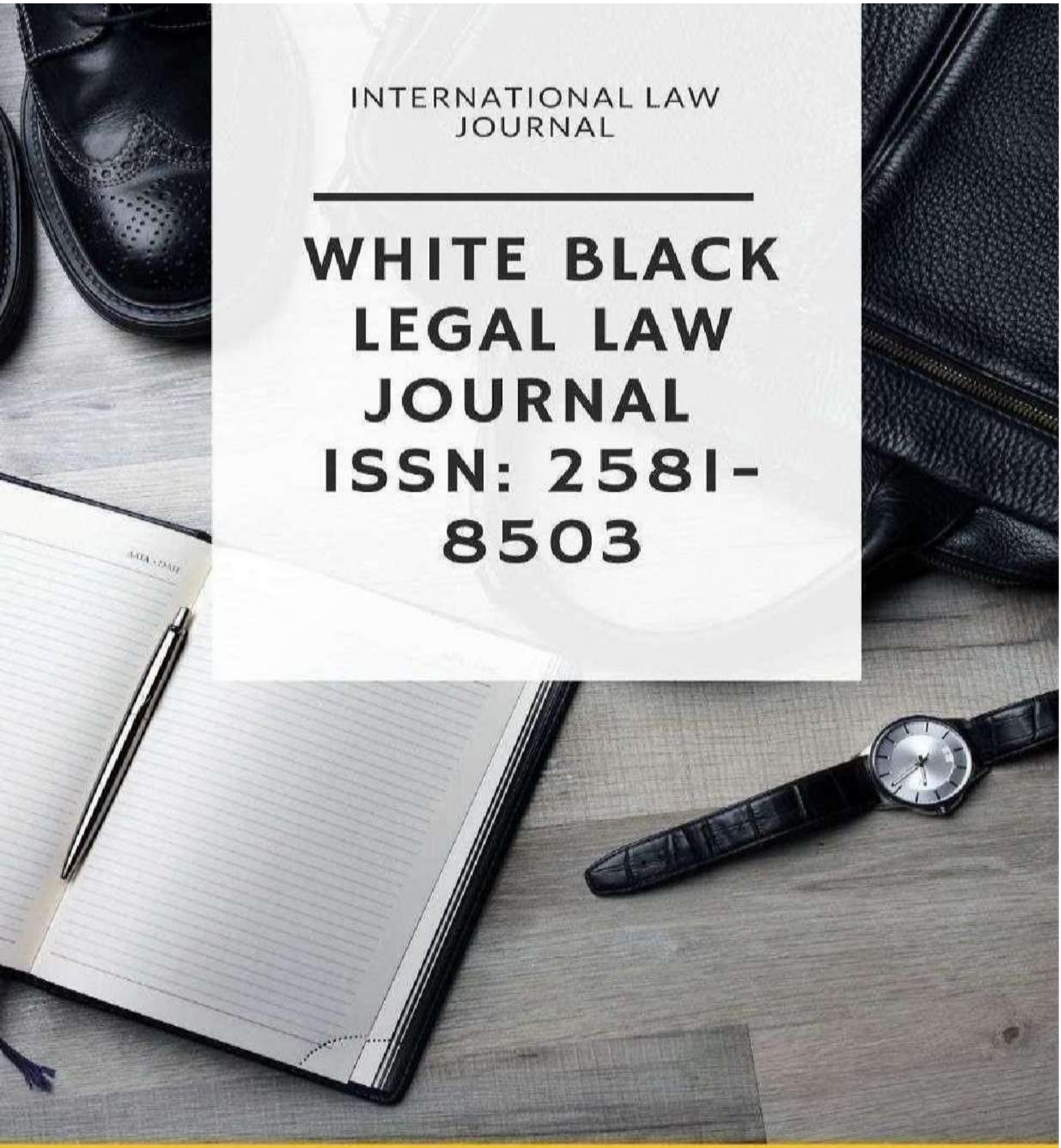

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

WHEN WHITE COAT BECOMES CODE BLUE: CONFRONTING THE LEGAL VOID IN THE AGE OF MEDICAL DEEPFAKES

AUTHORED BY - SHRESTHA DATTA[1]

Abstract

While deepfakes targeting politicians, celebrities, and society pre-dominates the headlines, a more insidious and potential threat is emerging in the sanctified realm of healthcare – medical deepfakes. The development and dissemination of synthetic media containing cloned voices and images of medical professionals, healthcare sectors, or fraudulent patient accounts pose unprecedented and serious challenges to public health, patient autonomy, and medical ethics in India. This includes synthetic images, videos, or voice recordings that mimic medical conditions, create fake diagnostic scans, or impersonate healthcare professionals. Their ability to mislead patients, scam insurance systems, and undermine trust in medical institutions creates significant risks. The most recent case of ***Global Health Limited & Anr. v. John Doe & Ors****. Represents the alarming convergence of synthetic media and public health risks in India. This article raises concerns about this crisis that has yet to be examined. It argues that India's current legal framework, which includes the new IT Rules (2023), the Drugs and Magic Remedies Act (DMR Act), and the recent Digital Personal Data Protection Act (DPDPA), are not effective enough to address the specific dangers of medical deception. Unlike political satire or entertainment, medical deepfakes exploit the significant trust gap in healthcare. They can cause immediate physical and financial harm very quickly. This article thus aims to disclose the effects of medical deepfakes on people's lives.*

Keywords: Medical deepfakes, healthcare, patients, IT Act (2000) & IT Rules (2023), impersonation

[1] *The author is a penultimate year student of B.B.A., LL.B. (Hons.) at Amity Law School, Amity University Kolkata. The author can be reached at* shrestha2002datta@gmail.com .

INTRODUCTION

Deepfake technology is based on sophisticated artificial intelligence that uses machine learning algorithms, especially generative adversarial networks (GANs), to create synthetic media like images, videos, and audio.[2] European Union's Artificial Intelligence Act [EU AI Act] defines deepfake as, "*AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful*."[3] It aims to produce very realistic synthetic media that look like real people, though some part of the content is altered.[4] At present, the number of deepfake cases in India has increased up to 550%.[5]

Now take a hypothetical scenario, where any of your family members, who has chronic kidney disease, watch a convincing video of a well-known surgeon promoting "natural" pills that claim to prevent dialysis. Trusting such, they order them online. However, within weeks, they realise that the medication is not working as promised, and it comes to notice that the video was a deepfake one, still circulating on social media, with hundreds of patients falling for such a sham. This is the threatening impact of "medical deepfakes," where false information undermines medical trust, putting lives at risk.

Unlike celebrity deepfakes that harm reputations, medical deepfakes harm human lives. In the sacred field of medicine, trust is the ultimate key. Patients rely on their doctors with their bodies and lives. Doctors depend on the accuracy of diagnostic data to make critical decisions. For centuries, medical images, including X-rays, CT scans, and MRIs, have served as a reliable truth and a clear view of the human body.[6] These are not dystopian fantasies. They are emerging realities made possible by accessible AI tools.. These endanger not only individual dignity but also public health and the integrity of medical systems.

[2] Shubham Pandey, Gaurav Jadhav, 'Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India' (SCC Online TIMES, 17 March 2023) <https://www.scconline.com/blog/post/2023/03/17/emerging-technologies-and-law-legal-status-of-tackling-crimes-relating-to-deepfakes-in-india/> accessed 08 November, 2025

[3] EU Artificial Intelligence Act <https://artificialintelligenceact.eu/article/3/>, art 3(60)

[4] Shubham Pandey, Gaurav Jadhav, 'Emerging Technologies and Law: Legal Status of Tackling Crimes Relating to Deepfakes in India' (SCC Online TIMES, 17 March 2023)

[5] BW Online Bureau, 'India's Deepfake Cases Up 550%, Losses May Hit Rs 70,000 Cr By 2024: Report' *BW BusinessWorld* (India, 05 December 2024) < https://www.businessworld.in/article/indias-deepfake-cases-up-550-losses-may-hit-rs-70000-cr-by-2024-report-541202#:~:text=Deepfake%20cases%20in%20India%20have%20surged%20by%20550,fraud%2C%20according%20to%20the%202024%20report%20by%20Pi-Labs> accessed 08 July, 2025

[6] Mirsky, Yisroel, et al. 'CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning' *28th USENIX Security Symposium (USENIX Security 19)*, 2019

WHY ARE MEDICAL DEEPFAKES ON THE NEWS?

This threat has garnered more attention from the public because of the rapidly rising number of cases. The most recent is the case of Dr. Trehan's digital doppelganger.[7] On December 23, 2024, Dr. Naresh Trehan, an acclaimed Cardiothoracic Vascular Surgeon and the Chairman of the Heart Institute of Medanta Hospitals, found that his likeness, voice, and reputation had been taken without permission. Deepfake videos, which had garnered more than 1.1 million views on Facebook, showed him endorsing questionable "natural remedies" for prostate problems and erectile dysfunction, areas far from his focus in cardiothoracic surgery. The videos not only displayed MEDANTA's trademarks, but also superimposed the face and voice of Dr. Trehan with the sole intention of misleading and misguiding the public at large about medical conditions relating to Urology and its cure without any certified medical data proving the same and infringing upon the rights and goodwill that have accrued in favor of the plaintiffs.[8] Visually, these trademarks become a sign of reliability, thereby instilling good faith and overshadowing any potential deepfake artifacts.[9]

This was not a hoax; it was a calculated fraud that took advantage of medical trust for profit and created serious public health risks. Trusted medical professionals are being cloned to peddle unverified treatments[10], targeting specific patients who have either limited to no knowledge of medicine, the aged victims, or those vulnerable ones who are anxious about their health.

Similarly, in the case of *Dr Devi Prasad Shetty v. Medicine Me & Ors.*[11] Dr. Shetty, a renowned cardiac surgeon, became the victim of deepfake, where the perpetrators were misusing his name, voice, likeness, and persona by producing fake videos on various social media platforms for commercial gain.[12] What the plaintiffs had alleged was that such can mislead the population into purchasing products and medicines or unverified and unsubstantiated health tips.

[7] *Global Health Limited & Anr. v. John Doe & Ors.*, CS(COMM) 6/2025, Order dated 08.01.2025, High Court of Delhi

[8] *Global Health Limited & Anr. v. John Doe & Ors.*, CS(COMM) 6/2025 [36]

[9] Arunima Rajan, 'Why Medical Deepfakes are the New Public Health Crisis' (Healthcare EXECUTIVE, 24 January, 2025) < https://www.healthcareexecutive.in/blog/deepfake > accessed 09 July 2025

[10] *Ibid*

[11] *Dr Devi Prasad Shetty v Medicine Me & Ors.*, (CS(COMM) 1053/2024)

[12] Bisman Kaur, Gaurangi Sharma, 'Delhi High Court takes strict approach to personality rights violation in healthcare industry amid spike in use of AI and deepfakes' (WTR, 13 February 2025) < https://www.worldtrademarkreview.com/article/delhi-high-court-takes-strict-approach-personality-rights-violation-in-healthcare-industry-amid-spike-in-use-of-ai-and-deepfakes > accessed 07 July 2025

MEDICAL DEEPFAKES: MORE THAN JUST MISINFORMATION

Medical deepfakes transcend mere misinformation. They threaten patient safety, healthcare trust, and legal responsibility. Unlike false claims or altered images, AI-generated synthetic fake doctor-patient interactions or changed diagnostic results can cause harmful medical decisions, fraudulent treatments, or misdiagnoses that can change lives. Dissemination of erroneous, incomplete, or even denialist information affects the health of the population. Legally, these deepfakes blur the lines of responsibility, challenging current laws on medical malpractice, and data integrity.

1. **Exploiting Critical Trust Asymmetry**: Patients naturally trust doctors and established healthcare institutions. Deepfakes bypass important scrutiny by imitating trusted sources with alarming accuracy. With the advent of deepfake videos and the fear of being crippled by any disease, patients struggle to differentiate legitimate information from misleading ones, thereby eroding the trust in healthcare sector.[13] This "veracity exploitation" is much more powerful than pretending to be a politician or celebrity.

2. **Direct Harm to the patient by:**
   - **Misleading and falsified treatments**: Patients might delay or skip evidence-based care for false, ineffective, or dangerous alternatives promoted through deepfakes. Deepfakes are often used to manipulate research data, influence unapproved clinical or drug approvals, and fake medical conditions, especially in cases of diseases like cancer. A 2019 study demonstrated that AI could be trained to create fake cancer nodules on CT scans of lungs, fooling both radiologists and AI-powered diagnostic software.[14]
   - **Uncertified Medical Products**: Promotion of contaminated drugs, unapproved medical devices, or harmful "alternative" therapies. For example, the use of deepfakes in telemedicine swindles. In the case of Prof. Jonathan Shaw, a well-known endocrinologist, stated that the deepfake video showed him talking about

[13] Frank Cutitta, 'The Deepfake and Social Engineering Arms Race in Healthcare' (DHInsights, 23 October, 2024) < https://www.dhinsights.org/news/the-deepfake-and-social-engineering-arms-race-in-healthcare > accessed 09 July 2025; *See also* Mika Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) TIMReview < https://www.timreview.ca/article/1282 > accessed 07 July 2025

[14] Mirsky, Yisroel, et al. "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning." *28th USENIX Security Symposium (USENIX Security 19)*, 2019

a fake medicine having TGA approval, which targeted primarily patients with Type-2 diabetes.[15]

- **Financial Exploitation**: Scams involving fake consultations, urgent payments for non-existent treatments, or selling worthless products at high prices.
- **Stealing Patient Data**: As the creation of deepfakes requires the collection of personal data (e.g., images from social media platforms) and because the deepfake itself is designed to possess identifiability as a key characteristic, they unmistakably qualify as a form of personal data.[16] Deepfakes are often used in phishing attacks to steal sensitive patient health data, such as cloning hospital helpline voices.[17]

3. **Exploiting Susceptible Vulnerability**: These deepfakes prey on individuals when they are most vulnerable—those facing serious illness, chronic conditions, or have limited medical knowledge[18]. Desperation clouds judgment, making victims less likely to question the authenticity of a "doctor's" urgent message.

4. **Erosion of Genuine Healthcare Trust**[19]: The rise of medical deepfakes creates a "crisis of authenticity," where patients may doubt genuine health communications from the authenticated ones. This doubt could lead them to hesitate in believing important public health warnings or treatment instructions.[20] This raise concerns as it can easily

[15] Becca Whitehead, 'Deepfake technology exploited a well known endocrinologist's trust and authority. Can the industry avoid deepfakes?' (InSightPlus, 05 May 2025) < https://insightplus.mja.com.au/2025/17/deepfake-technology-exploited-a-well-known-endocrinologists-trust-and-authority-can-the-industry-avoid-deepfakes/ > accessed 08 July 2025

[16] Saar Hoek Suzanne Metselaar, Corrette Ploem, et. al., 'Promising for patients or deeply disturbing? The ethical and legal aspects of deepfake therapy' (2025) 51 Journal of Medical Ethics, 481-486 < https://doi.org/10.1136/jme-2024-109985 > accessed 10 July 2025

[17] Mike Ruggio, 'The Evolving Threat of Deepfake Telemedicine Scams' (Insights TaylorDuma, 22 October 2024) < https://insights.taylorduma.com/post/102jkzn/the-evolving-threat-of-deepfake-telemedicine-scams > accessed 07 July 2025

[18] Shashank Agarwal, Sumeer Peta, Sriram Panyam, 'Deepfakes In Healthcare: Reviewing the Transformation Potential and its Challenges' (2024) 12(4) IJISAE, 3965-3970 <https://ijisae.org/index.php/IJISAE/article/view/6956/5866> accessed 05 July 2025; *See also* Jamshir Qureshi, Samina Khan, 'Artificial Intelligence (AI) Deepfakes in Healthcare Systems' (2024) <10.20944/preprints202402.0176.v1> accessed 05 July 2025

[19] Frank Cutitta, 'The Deepfake and Social Engineering Arms Race in Healthcare' (DHInsights, 23 October, 2024) < https://www.dhinsights.org/news/the-deepfake-and-social-engineering-arms-race-in-healthcare > accessed 09 July 2025

[20] Laura Fitzgerald, 'Understanding the Threat of Deepfakes in Healthcare' (Pindrop, 26 June 2025) < https://www.pindrop.com/article/threat-deepfakes-in-healthcare/ > accessed 10 July 2025

confuse people and put their health at serious risk.[21] Someone can easily record a fraudulent audio recording, making it sound like a healthcare professional is involved in unethical activities.[22]

5. **Velocity of Harm**: Health scams operate quickly and spread like wildfire. For example, a deepfake promoting a "limited-time cancer cure" can go viral in hours, reaching vulnerable populations before authorities get the time to respond, as seen in the case of Global Health Limited, where the deepfake video had received massive circulation, with 6400 likes and 1.1 million views.[23]

INDIAN LEGAL FRAMEWORK AGAINST MEDICAL DEEPFAKES

India's legal framework is struggling to tackle the growing threat of medical deepfakes. Current laws, including the IT Act (2000) and its amendments, make identity theft and data manipulation illegal (Sec. 66D, 66E), while the Digital Personal Data Protection Act (2023) holds people accountable for misusing health data. The legal framework to tackle deepfakes involves the following provisions:

1. **The Information Technology Act, 2000 (IT Act)[24]** remains the primary statute for dealing
    - **Section 66C (Identity Theft)**: Which criminalizes fraudulent use of electronic signatures, passwords, or "any other unique identification feature."
    - **Section 66D (Cheating by Personation)**: This section prosecutes individuals who use deception and personation to commit cheating.

2. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules")[25]**
    - **Rule 3(1)(b)**: Mandates intermediaries to take down and not to host, display, upload, modify, publish, transmit, store, update, or share any impersonation content via synthetic media after a complaint.

[21] https://pmc.ncbi.nlm.nih.gov/articles/PMC11503397/#B32-nursrep-14-00203
[22] *Ibid*
[23] *Global Health Limited & Anr. v. John Doe & Ors.*, CS(COMM) 6/2025 [33]
[24] The Information Technology Act, 2000, ACT NO. 21 OF 2000
[25] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

3. **Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954 (DMR Act)**[26]:

- **Section 4**: Provides for the prohibition of misleading advertisements relating to drugs, including:

  (a) directly or indirectly giving false impression regarding true character of the drug; or

  (b) making a false claim for the drug; or

  (c) is otherwise false or misleading in any material particular

  - **Section 5**: Lays down the prohibition of advertisement of magic remedies for treatment of certain diseases and disorders. Magic remedies, as defined under **Section 2(c)** means and includes a talisman, mantra, kavacha, and any other charm of any kind which is alleged to possess miraculous powers for or in the diagnosis, cure, mitigation, treatment or prevention of any disease in human beings or animals or for affecting or influencing in any way the structure or any organic function of the body of human beings or animals.

4. **Bharatiya Nyaya Sanhita (2023)[27] [formerly the Indian Penal Code, 1860]**

- **Section 66(2) (False Electronic Content with Intent to Harm)**: This section makes it illegal to create or share false or misleading information electronically if the intent is to cause injury, intimidation, or deceit.
- **Section 66(3) (Enhanced Punishment for Harm)**: If such content poses a danger to public health or safety, the punishment can increase to 5 years.
- **Section 354D (Fraudulent Digital Impersonation)**: This section addresses identity fraud through digital means, including deepfake impersonation of doctors or patients.
- **Section 306 (Defamation via Electronic Means)**: Using deepfakes to damage the reputation of medical professionals, such as fake videos of misconduct, may result in defamation charges.

[26] Drugs and Magic Remedies (Objectionable Advertisements) Act, 1954 (Act No. 21 of 1954), India

[27] The Bharatiya Nyaya Sanhita, 2023, Act No. 45 of 2023

THE LEGAL VOID: WHEN EXISTING LAWS MISDIAGNOSE THE ISSUE

The existing laws are more reactive than preventive. The proposed **Digital India Act**[28] aims to strengthen regulations, but gaps still exist. Who is responsible when a deepfake leads to wrongful treatment? Can courts use traditional defamation or medical malpractice laws for synthetic media? As India navigates this new area, it needs clearer legislation, similar to the EU's AI Act, to protect both healthcare integrity and patient lives. While Global Health sets an important precedent, raising awareness, it points out a serious issue:

1. **Lack of Specific Law against Deepfakes**

   India's current legal systems do not effectively address the unique challenges posed by deepfakes[29], especially medical deepfakes. They were built for a time when tangible evidence and human mistakes were the norm, but not for our current digital landscape filled with algorithmic deception. Sections on privacy violations under the IT Act do not consider the unique nature of deepfakes. Linking anonymous creators to specific victim losses is near-impossible, which makes it more difficult to trace back the perpetrator. The law was codified keeping in mind human perpetrators, and not AI-generated synthetic media. Even recent advisories from the Ministry of Electronics and IT about AI-generated content provide guidelines[30], but they lack enforcement mechanisms. Also, the law doesn't cover non-drug scams (e.g., devices, financial cons). The definition of "advertisement" struggles with synthetic social media posing as genuine endorsements. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002[31] remains silent on AI or any digital manipulation. Additionally, the laws address the aftermath of the harm already caused but provide little for prevention.

[28] Ministry of Electronics & IT, *MoS Rajeev Chandrasekhar to hold a Digital India Dialogues' session tomorrow in Mumbai on principles of Digital India Act* (Press Information Bureau, 22 May 2023)

[29] Deb Roy, Nilutpal. 'Rising Menace of Deepfakes with the Help Of AI: Legal Implications In India', Indian Journal of Integrated Research in Law (2024)

[30] Ministry of Electronics and Information Technology Cyber Law and Data Governance Group, Advisory No. 2(4)/2023-CyberLaws - 3 dated 15th Mar 2024

[31] Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (Published in Part III, Section 4 of the Gazette of India, dated 6th April, 2002)

2. Medical Malpractice and the "Standard of Care"

The foundation of medical malpractice law is the "standard of care."[32] This refers to the level of skill and caution that a reasonably careful healthcare provider in the same specialty would use in similar situations. But how does this standard apply if a doctor depends on a deepfake image? If a radiologist overlooks a tumor that was synthetically removed, are they negligent? The deepfake might appear so realistic that neither the human eye nor typical detection software can identify it. This makes it nearly impossible to prove a breach in the standard of care. On the other hand, if a doctor acts on a fake tumor, the resulting harm is not due to their medical judgment but from altered data. Medical photographs can be manipulated to add or remove indicators of health challenges to engage in insurance scams, sabotage ongoing investigations, execute terrorist acts, seek vengeance against others, or even commit murders.[33] The doctor becomes a victim while the patient suffers harm, creating a liability gap that leaves the injured patient without a clear way to seek compensation.

3. The Inadequacy of Data Protection Laws

Data privacy laws like the Digital Personal Data Protection Act, 2023 (DPDPA)[34] In India and the Digital Information Security in Healthcare Act, 2018[35] focused on regulating digital health data with strict security, consent, and accountability measures for protecting patient information. However, they focus on unauthorized access and disclosure rather than malicious changes or fabrications of data, which are the essence of a medical deepfake. These laws aim to prevent data breaches, but they do not address data integrity against sophisticated AI manipulation. While a hospital could be held responsible for a cybersecurity issue that allowed a deepfake into its system, this approach fails to tackle the creation and spread of the deepfake itself. Similarly, the 36-hour window **(Rule 3(2)(b))**[36] is too slow for addressing the medical harm and lacks proactive detection mandates.

[32] Peter Moffett, Gregory Moore, 'The Standard of Care: Legal History and Definitions: the Bad and Good News', 2011 Feb 12(1) PMC, 109–112 < https://pmc.ncbi.nlm.nih.gov/articles/PMC3088386/ > accessed 10 July 2025

[33] Shashank Agarwal, Sumeer Peta, Sriram Panyam, 'Deepfakes In Healthcare: Reviewing the Transformation Potential and its Challenges' (2024) 12(4) IJISAE, 3965-3970 <https://ijisae.org/index.php/IJISAE/article/view/6956/5866> accessed 05 July 2025

[34] Digital Personal Data Protection Act, No. 22 of 2023

[35] Digital Information Security in Healthcare Act (DISHA), 2018

[36] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

4. **Criminal Law: A Blunt Instrument**

Existing criminal laws are not sufficient to deal with this issue. The aforementioned laws require proving who the perpetrator is and their intention, which is extremely difficult when dealing with anonymous online actors and decentralized AI tools. The absence of mechanisms to authenticate evidence in most legal systems puts the onus on the defendant or opposing party to contest manipulation, potentially privatizing a pervasive problem.[37] They were not created to regulate the technology itself or to push for security standards that could prevent such fabrications in the first place.

5. **Jurisdiction Limits**

Cybercrimes involving deepfakes are often cross-border, requiring transnational legal actions. For instance, in Bharatiya Nyaya Sanhita (2023), the definition of a crime "within Bharat" related to cybercrimes involving deepfakes is unclear. Identifying the person behind these crimes is very difficult because there are no territorial limits. When multiple jurisdictions with different accountability and penalty laws are involved, the prosecution and enforcement process becomes even more complicated. It is particularly challenging to prosecute and enforce laws without clear legislation defining who is responsible. This includes the creator, the AI-model developer, the Healthcare Provider or the middleman hosting the deepfake content, especially when each one is located in a different country, each with its respective laws.

CONCLUSION

Medical deepfakes are not a threat just for the future; they are a current and growing danger that takes advantage of India's digital health surge and slow regulations. The impact of doing nothing shows up in lost lives, drained savings, and weakened trust in a healthcare system that is already stressed. The mix of synthetic media and healthcare creates tough questions about trust, safety, and ethics. Without focused legal action, we risk changing medicine from a field of healing into a space for deception.

Tackling this issue requires us to go beyond fixing old laws. It needs a complete rethink of trust, proof, and responsibility in a digital healthcare system. By changing the standard of care,

[37] Harshvardhan Mudgal, 'The deepfake dilemma: Detection and decree' (BarandBench, 18 November 2023) < https://www.barandbench.com/columns/deepfake-dilemma-detection-and-desirability > accessed 10 July 2025

enforcing a secure chain of trust for medical data, and establishing clear liability rules, we can start to strengthen our collective defense. The lies in medicine are a new and frightening threat, but if we act now with planning and determination, we can keep our trust in medicine based on a reality we can all verify, protecting the health and safety of future generations. To maintain the importance of medical evidence and the dignity of patients, the law needs to change. We must create a regulatory barrier that protects not just data but also the truth itself.