INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 8 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 8 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-8-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL EXPANSION AND WHITE-COLLAR CRIME: EXAMINING FRAUD AND REGULATORY FAILURES IN INDIA'S HEALTHCARE SYSTEM

AUTHOR – NUR NAHAR AMIN, SYMBIOSIS LAW SCHOOL HYDERABAD

BEST CITATION – NUR NAHAR AMIN, DIGITAL EXPANSION AND WHITE-COLLAR CRIME: EXAMINING FRAUD AND REGULATORY FAILURES IN INDIA'S HEALTHCARE SYSTEM, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (8) OF 2026, PG. 426-433, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

White collar crime within the healthcare sector has become apparent as an outstanding governance concern in India as healthcare fraud is a serious issue, and when it is committed by customers, it becomes a more serious issue in India's healthcare system, which not only affects its stability but also efficiency and quality of services. Now there is an expansion of digital health records, government insurance schemes, private healthcare institutions, and even opportunities for activities that are fraudulent such as false insurance claims, manipulated medical bills, and there is an increase in unnecessary treatments. This study examines how fraud like this is common as it takes different forms and how it impacts healthcare institutions. However, there are government initiatives like Ayushman Bharat and the National Digital Health Mission which was introduced for the purpose to improve transparency and access and also existing preventive mechanisms still remain inadequate. The study suggests that advanced technologies such as Artificial Intelligence, Machine learning, and blockchain, and with these technologies, there are stronger regulatory frameworks, increased public awareness, and improved public-private collaboration which are essential in order to prevent fraud. Overall, the research emphasises the need for comprehensive policy reforms in order to ensure a more transparent, reliable, and sustainable healthcare system in India.

Keywords: White-Collar Crime, Healthcare Fraud, Digital Healthcare, Insurance Fraud, Artificial Intelligence

1. Introduction

Healthcare customer fraud has become a serious and is growing in India's healthcare system, which is affecting both its financial stability and daily functioning. In earlier times, fraud was limited because of the reason that healthcare services were smaller and mostly localised. However, as digital health records expanded, large insurance schemes, growth of the private healthcare sector, therefore created opportunities for fraud as well. The increase in healthcare fraud has disrupted trust among the patients, providers of healthcare and insurance companies. Even though there are legal provisions that exists in order to address fraud, there are times when they do not have a positive impact due to weak enforcement, outdated regulations, and a lack of specialised focus on healthcare related white-collar crimes. The Indian government has introduced several initiatives in order to improve in transparency and in reducing fraud. One of the major schemes is Ayushman Bharat Pradhan Mantri Jan Arogya Yojna (AB-PMJAY), which provides health insurance to economically weaker sections as the scheme uses Aadhar-based biometric authentication, digital e-cards, in order to prevent misuse or to take unwanted advantage of the scheme. The National Health Authority (NHA) manages works with regards of implementation by conducting audits and penalizes fraudulent entities. The Central Bureau

of Investigation (CBI) has also created a dedicated healthcare and Pharma fraud unit in order to investigate fraud that will be happening in public healthcare schemes. Furthermore, the National Digital Health Mission (NDHM) looks forward to digitize medical records and reduce data manipulation.

Despite this progress, several factors have been taken into consideration where progress has continued to allow healthcare fraud in India as the healthcare system is in pieces or complex where multiple stakeholders are involved such as hospitals, insurance companies, and patients, which created sectors where there are high possibilities of exploitation. Weak government regulation, unsuccessful enforcement and dependence on human intervention have limited the ability to respond to fraud productively.

Recent developments have shown that fraudulent activities are becoming more sophisticated, especially with the digitization of healthcare services. Fraud that involves Electronic Health Records (EHRs), identity theft, telemedicine platforms, and manipulation of insurance claims are also increasing. In order to address these challenges, advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML) are also growing to detect fraud and track anomalies. Moreover, blockchain technology is also being explored for creating secure and tamper-proof patient data systems, but there are some private sector organizations that are adopting biometric authentication, solutions of blockchains, weak government enforcement and the absence of cohesive policy development is becoming unsuccessful. There are gaps in implementation when healthcare services are compared with countries like the United States uses Medicare and Medicaid fraud detection programs, and European nations such as the UK and Germany have more strict government regulations and strong enforcement mechanisms as these countries use predictive analytics, data monitoring, and cross-sector cooperation for managing fraud more successfully.

2. Research questions

- Whether digitisation has transformed the nature and scope of white-collar crime in India's healthcare sector?
- Whether emerging forms of healthcare fraud in digital insurance systems and electronic health records are adequately addressed under existing legal frameworks?
- Whether current legal and regulatory mechanisms are sufficient to combat digitally enabled healthcare fraud?
- Whether stronger technological, institutional, and policy reforms are necessary to improve fraud detection and governance in India's digitising healthcare system?

3. Research objectives

- To examine whether digitisation has transformed the nature and scope of white-collar crime in India's healthcare sector.
- To analyse the various forms of healthcare fraud that is emerging within digital insurance schemes, electronic health records, and biometric authentication systems.
- To evaluate whether existing legal and regulatory frameworks are adequate to address digitally enabled healthcare fraud.
- To propose necessary legal, technological and institutional reforms to strengthen fraud and improve governance in India's digitising healthcare system.

4. Scope of research

This research is limited to examining whit- collar crime in India's digitising healthcare sector, particularly in relation to schemes. Moreover, it focuses on economic and financial offences. This study analyses the applicability of major legal frameworks in addressing digitally enabled healthcare fraud. Furthermore, a brief comparative reference with other countries is also included but the primary focus remains on the Indian Legal and regulatory context.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

5. Research Methodology

This research adopts a doctrinal method that is based on the study of relevant statutes, judicial decisions, and government policies related to healthcare fraud and digital governance in India. It examines laws such as the Indian Penal Code, Information Technology Act, Prevention of Corruption Act, and related frameworks. Furthermore, the study also uses secondary sources like academic articles and official reports for analysis. The approach is qualitative and focuses on legal interpretation and evaluation rather than empirical research.

6. Literature review

Author C.M. Selvamuthu & others in the Article titled "*Strengthening India's Healthcare System: Combating Fraud with Technology and Policy Reforms*"[531] examines how fraud in India's healthcare sector have a huge impact on its financial resources and service delivery as it highlights practices which includes false insurance claims, inflated medical bills, and misuse of government health schemes.

Author MingJian Tang & others in the Article titled "*Unsupervised Fraud Detection in Medicare Australia*"[532] examines how unsupervised machine learning techniques can be used to detect fraudulent activities in Medicare claims. The authors have focused on identifying unusual patterns in healthcare billing data without relying on labelled fraud cases.

Author Ronak Singh Bhangu in the article titled "*White collar crime in the medical field: A study in Indian perspective*"[533] mentions that particular number of doctors and hospitals are involved in dishonest practices for gaining more profit which includes charging more than necessary, suggesting treatments that are not required, providing fake medical certificates, being involved in illegal organ trade, or taking bribes from pharmaceutical companies.

Author Brian K. Payne in the Article titled "*White Collar Crime Cybercrime: White Collar Crime, Cybercrime, or both?*"[534] Examines whether cyber offences that is committed for the purpose of financial gains should be classified as traditional white-collar crimes, cybercrimes, or a combination of both. The study explains that white collar crime involves offences which are financially motivated and are non-violent in nature, as they are committed by professionals, but on the other hand, cybercrime involves offences which are committed through the medium of digital technology.

Journal review titled "*Fraud detection in healthcare claims using machine learning: A systematic review*"[535] by author Anli du Preez examines how machine learning is used in order to detect fraud in healthcare claims, as it finds that models like decision trees and random forests are used and have shown high accuracy. However, the authors have highlighted the problems related to limited labelled data, class imbalance, and lack of real-world testing.

7. Digitisation and transformation of white-collar crime in healthcare

Digitisation has changed the course of the healthcare sector as patient records can now be stored online, insurance claims are processed automatically, and verification is done through digital systems[536]. These changes were made in order to make healthcare faster and more transparent. With more accuracy, these digital systems have also created possibilities for white-collar crime because, earlier, fraud took place by changing paper records, but it has the ability to do so by tampering with the online systems, giving the opportunity or full access to

[531] " C.M. Selvamuthu , *Strengthening India's Healthcare System: Combating Fraud with Technology and Policy Reforms,* 14, JOURNAL OD PIONEERING MEDICAL SCIENCES, 92, (2025).
[532] MingJian Tang, B. Sumudu.U. Mendis, D. Wayne Murray, Yingsong Hu and Alison Sutinen, *Unsupervised Fraud Detection in Medicare Australia*, 1 21, CONFERENCES IN RESEARCH AND PRACTICCE IN INFORMATION TECHNOLOGY, 103, (2011).
[533] Ronak Singh Bhangu, *White collar crime in the medical field: A study in Indian perspective*, 6, INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS, 688, (2019)."
[534] "Brian K. Payne, *White Collar Crime Cybercrime: White Collar Crime, Cybercrime, or both?,* 19, CRIMINOLOGY, CRIMINAL JUSTICE, LAW & SOCIETY, 17, (2018).
[535] Anli Du Perez, *Fraud detection in healthcare claims using machine learning: A systematic review*, 160, ELSEVIER, 1, (2025)
[536] NATIONAL HEALTH AUTHORITY, Official Website Ayushman Bharat | PMJAY | National Health Authority, (last visited March 2, 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

steal the login details, health portals without permission, or to submit fake insurance claims by changing electronic data.

In Uttar Pradesh, some individuals under the Ayushman Bharat Scheme illegally accessed the health portal and changed Aadhar-linked details and used this access to submit false treatment claims to gain money fraudulently[537]. The police registered a case under the Indian Penal Code and the Information Technology Act, which shows that digital systems can be misused if there are no strong measures for security checks. The scale of this fraud was very large as in just a few weeks, more than 6,000 fake claims[538] worth nearly rupees 10 crore were processed which clearly shows that digital fraud can take place at a fast rate and on a large scale if compared to older methods. Therefore, digitisation has improved healthcare services, but it has also changed how white-collar crimes are committed.

8. Nature and Forms of Healthcare Fraud in India

In India, healthcare fraud has become more complex and widespread, especially when digital health governance is expanded through public insurance schemes like Ayushman Bharat Pradhan Mantri Jan Arogya Yojna. With the introduction of online health records and biometric verification, it has become easy to commit fraud at multiple stages, like patient registration and diagnosis to treatment and final insurance claim settlement. There are general methods where it involves hospitals, insurance agents, intermediaries, pharmaceutical companies and sometimes even beneficiaries as false patient entries, unnecessary treatments, inflated bills, and manipulated digital records[539]. Furthermore, because many stakeholders are already involved in the system and is highly interconnected, it becomes extremely difficult to detect the exact source of fraud and to make healthcare fraud a structured and multi-layered process instead of an isolated act. The following categories explain the forms of healthcare fraud in greater depth:

8.1. Insurance Fraud

Insurance fraud is the most elementary form of healthcare related white collar in India as it mainly arise under public schemes such as Ayushman Bharat Pradhan Mantri Jan Arogya Yojana (AB-PMJAY) as well as private health insurance policies. In this kind of fraud, hospitals or other stakeholders manipulate insurance claims for the purpose of receiving higher reimbursements and since large amounts of public money are involved, serious economic consequences are also generated.

Practices which include ghost patients (non-existent beneficiaries) in order to claim reimbursement, increase the actual cost of treatment on papers so that they can gain more profit than the real expense. Moreover, there are times when they ask for payment from more than one insurance company for the same treatment which is also called duplicate billing. Furthermore, they also hide the fact that a patient was already suffering from a disease before taking the policy and later present it as a new illness so that the insurance company will approve the claim. For example: A hospital has performed a minor surgery which has costed around twenty thousand rupees but submitted a claim of seventy-five thousand rupees, under a government scheme by falsely adding ICU charges and unnecessary diagnostic tests that were never done[540]. Therefore, practices like this lead to financial losses of public funds, increase insurance premiums in the private sector and insurance companies start investigating every claim more strictly. As a result, even honest and genuine patients have to face extra questioning, longer verification, and approval for their treatment gets delayed.

[537] THE TIMES OF INDIA, Over 6k fake med claims made in 39 hospitals across UPunder Ayushman Bharat | Lucknow News - The Times of India, (last visited March 2, 2026)."
[538] "MEDICAL DIALOGUES, Rs 10 Crore Ayushman Bharat Fraud in UP: Over 6000 fake claims approved, (last visited March 2, 2026).
[539] Zain Hamid & others, Healthcare Insurance Fraud Detection Using Data Mining, 112, BMC MEDICAL INFORMATICS AND DECISION MAKING, 1, (2024)."
[540] PRESS INFORMATION BUREAU, Home Page:Press Information Bureau, (last visited March 3, 2026).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

8.2. Medical Billing Manipulation

Medical billing manipulation refers to inflating and altering medical invoices in order to raise revenue and it has come to notice that it occurs in insured as well as in uninsured environments. The strategies are based on billing diagnostic tests that has never been done, prescribing costly branded medication rather than the less expensive ones or retaining patients in the hospital unnecessarily. Even in other instances, patients might be discharged with Intensive care services yet they were in the general ward. Another common method is referred to as unbundling where services that are supposed to exist as one payment are separated and charged separately which directly increases the overall number of payments.

Taking the example of a patient who is admitted for dengue treatment may be kept in the hospital for days despite his medical stability which is not necessary. Laboratory tests will be conducted repeatedly without clear justification, automatically leading to a higher final bill. Now conduct like this will be charged with legal provisions under section 420 of the Indian Penal Code for cheating, and also under consumer protection laws for deficiency of service. However, many patients will avoid legal remedies due to limited awareness or financial constraints. As a result. Medical billing manipulation can lead to a reduction in trust in private healthcare institutions, and a shift will come to notice from patient-centred care toward revenue-driven practices.

8.3. Identity theft and biometric misuse

Aadhar-linked verification was created or introduced under the scheme of Ayushman Bharat Pradhan Mantri Jan Arogya Yojna, biometric authentication was designed to reduce fraud and to improve transparency in healthcare delivery. The use of fingerprints and Aadhar numbers was introduced for the purpose of ensuring that actual beneficiaries are getting proper benefit and to prevent duplicate or false claims. However, misuse of identity credentials has successfully created new loopholes within the system as there is a possibility that fraud can take place when a beneficiary's Aadhar number or biometric details are used without their knowledge in order to generate insurance claims. Whereas, in some cases, individuals who are not eligible can also apply for this benefit by using forged documents. With that, there is a matter of concern about middlemen collecting biometric data in rural areas and misusing it for false claims. Taking the example of a beneficiary who might discover one day that a costly surgery was claimed in their name, even though they never received such treatment.

Therefore, although biometric systems has the ability to increase accountability, there are still challenges that exits such as limited digital literacy, inadequate data protection safeguards[541], and weak monitoring mechanisms which directly increase the risk of misuse and with that come consequences which include violation of privacy rights, denial of benefits to genuine beneficiaries if their claim limit is exhausted because of fraudulent claims, and also reduces trust in public welfare schemes[542].

8.4. Pharmaceutical fraud

Pharmaceutical fraud involves unethical or illegal practices which include healthcare providers and pharmaceutical companies where doctors receive commissions, gifts, or other incentives for prescribing overpriced or high-cost medicines despite the fact that there already exist cheaper and equally effective alternatives[543]. With these, there are also other problems or concerns about overpricing of medicines that is beyond the limits of regulations, the circulation of counterfeit or

[541] "Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[542] WORLD HEALTH ORGANISATION, gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf, (last visited March 3, 2026).
[543] Jillian Kohler, Anaam Khan & Andrea Bowra, *Bribery and the Global Pharmaceutical Industry: An Exploration of Patterns and Penalties in the Organisation for Economic Cooperation and Development Reports*, JOURNAL OF LAW, MEDICINE & ETHICS, 1, (2026).

substandard drugs[544], and irregularities in the conduct or reporting of clinical trials. Taking the example of a doctor who has been prescribing an expensive antibiotic which is very well influenced by financial incentives rather than proper regulations, where public officials are involved and therefore such conduct falls under the Prevention of Corruption Act.[545] Moreover, it may fall within the scope of the Drugs and Cosmetics Act[546] and professional ethical regulations who are medical practitioners. Due to which there are consequences of increased healthcare expenses for patients, potential health risks from unsafe or low-quality medicines, and weakening of ethical standards inside the medical profession.

8.5. Digital Record Manipulation

After the digitisation of the healthcare services under the initiatives of the National Digital Health Mission, transparency and record management have improved. But it has also created new risks in regards with cyber enabled fraud. Now electronic Health Records (EHRs) can be tampered to show higher treatment costs so that hospitals can claim more insurance money. In some cases, digital records can be edited in order to hide mistakes or negligence in treatment and telemedicine records can be altered, moreover, hospital computer systems can be hacked to access or misuse patient data.

Taking the example of a patient who died because treatment was delayed and in order to hide such conduct, someone might change the digital records. Therefore, such actions can lead to punishment under the Information Technology Act, 2000 and other criminal laws related to forgery. The result of this type of fraud includes difficulty in proving medical negligence, financial loss to insurance companies and increases risk of cyber-attacks on healthcare institutions.

9. Legal and Regulatory Framework: Strengths and Limitations

9.1. Indian Penal Code, 1860 (BNS, 2023) and General Offences

The Indian Penal Code (IPC) consist general provisions for offences like cheating (section 420)[547], forgery (section 463-465)[548], and criminal breach of trust (section 405)[549] and these sections can be used in cases of healthcare fraud. However, these laws were introduced before when digital systems became very common and because of this, they do not directly deal with online fraud or manipulation related to cyber which makes it difficult in order to apply these traditional sections to complex digital healthcare scams.

9.2. Information technology act[550] and cyber offences

In *Anvar P.V. v. P.K. Basheer 2014*[551], that electronic evidence must comply with section 65B of the Evidence Act.

9.3. The Prevention of Corruption Act, 2018[552]

In *Subramanian Swamy v. Manmohan Singh 2012*[553], the court held that when a sanction is provided for prosecuting public servants in corruption cases, it must be decided within a reasonable time.

9.4. The Prevention of Money Laundering Act (PMLA), 2002

In *Vijay Madanlal Choudhary v. Union of Union 2022*[554], the Supreme Court upheld the validity of PMLA provisions and recognised money laundering as a grave economic offence. Moreover, this act allows authorities to investigate, attach, and confiscate such property and it also clearly mentions punishment which includes imprisonment and fines.

[544] WORLD HEALTH ORGANISATION, Substandard and falsified medical products, (last visited March 4, 2026).
[545] Prevention of Corruption (Amendment) Act, No. 16, Acts of Parliament, 2018 (India).
[546] Drugs and Cosmetics Act, No. 23, Acts of Parliament, 1940 (India)."
[547] "Indian Penal Code, 1860, §, 420, No. 45, Acts of Parliament, 1860 (India).
[548] Indian Penal Code, 1860, §, 463-465, No. 45, Acts of Parliament, 1860 (India).
[549] Indian Penal Code, 1860, §, 405, No. 45, Acts of Parliament, 1860 (India).
[550] Information Technology Act, No. 21, Acts of Parliament, 2000 (India)."
[551] "Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[552] Prevention of Corruption (Amendment) Act, No. 16, Acts of Parliament, 2018 (India).
[553] Subramanian Swamy v. Manmohan Singh, (2012) 3 SCC 64.
[554] Vijay Madanlal Choudhary v. Union of Union, (2022) 10 SCC 368.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

9.5. Fugitive Economic Offenders Act, 2018

The Fugitive Economic Offenders Act[555] was introduced in order to deal with individuals who commit major or large financial crimes and then leave India to avoid legal proceedings. Under this law, any person who commits an economic offence where rupees 100 crore or more is involved and refuses to return to India can be declared a "Fugitive Economic Offender". Once they are declared, their properties in India can be confiscated as can be seen in the case of *Vijay Mallya 2019*. Therefore, the purpose of this law is to prevent offenders from escaping justice and to ensure that they cannot benefit from their illegal actions.

9.6. The Central Vigilance Commission Act, 2003[556]

In the case of *Centre for Public Litigation v. Union of India 2011*[557], the Supreme Court quashed the appointment of P.J. Thomas as the Central Vigilance Commissioner on the ground that the High-Powered Committee had failed to properly consider the criminal case pending against him. The court held that people who are appointed in anti-corruption positions must have clean records and strong integrity and institutions like this should be trustworthy, independent, and transparent so that the public can have confidence in them.

10. Comparative perspective

In the **United States**, Medicare fraud is monitored through advanced data analytics that can detect unusual billing patterns automatically[558]. Furthermore, there are various advanced AI tools (e.g., IBM Watson Health, SAS Fraud Framework) are used in order to analyse large claim datasets.

Australia uses a system known as the Medicare Data Matching System where billing data from healthcare are compared and there are mandatory routine checks for unusual patterns or inconsistencies[559]. Artificial Intelligence have also advanced in audit tools that are used to monitor histories and flag abnormal behaviour[560]. Therefore, helping the authorities in detecting fraud before large amounts of money are lost.

Singapore operates with a centralised healthcare system which includes securing medical records systems with detailed audits and these systems record every access and modification that is made to patient data, making it easier to detect tampering[561]. Moreover, Singapore also uses centralised claims monitoring platforms that automatically check for duplicate submissions and unusual billing activity.

In the **United Kingdom**, the National Health Service has a Counter Fraud Authority that was set up to investigate healthcare fraud cases. These systems use predictive technology and specialised investigators[562] but compared to these models, India's system is still developing. There are some digital advancements that has taken place but the system does not always detect fraud immediately at the time when it is actually happening and there are many special teams that do not focus only on healthcare fraud.

11. Recommendations

11.1. Strengthening Technological Fraud Detection

The government should be using advanced technologies such as Artificial Intelligence, Machine Learning and predictive analytics in order to detect healthcare fraud as these technologies have the ability to analyse large amounts of data and to identify unusual billing

[555] Fugitive Economic Offenders Act, No. 17, Acts of Parliament, 2018 (India).
[556] The Central Vigilance Commission Act, 2003, No. 45 of 2003, Acts of Parliament, 2003 (India).
[557] Centre for Public Litigation v. Union of India, (2011) 4 S.C.C. 1 (India)."
[558] "Dorsa Farahmandazad, *ML-Driven Approaches to Combat Medicare Fraud: Advances in Class Imbalance Solutions, Feature Engineering, Adaptive Learning, and Business Impact*, ARXIV, 1, (2025).
[559] MingJian Tang, B. Sumudu.U. Mendis, D. Wayne Murray, Yingsong Hu and Alison Sutinen, *Unsupervised Fraud Detection in Medicare Australia*, 1 21, CONFERENCES IN RESEARCH AND PRACTICCE IN INFORMATION TECHNOLOGY, 103, (2011).
[560] Anli Du Preez, Sanmitra Bhattacharya, Peter Beling & Edward Bowen, *Fraud Detection in Healthcare Claims Using Machine Learning: A systematic Review*, 160, ELSEVIER, 1, (2025).
[561] MINISTRY OF HEALTH, SINGAPORE, Healthcare at a glance | Ministry of Health, (last visited Feb. 28, 2026).
[562] GOV.UK, NHS Counter Fraud Authority annual report and accounts 2023 to 2024 - GOV.UK, (last visited Jan. 1, 2026)."

patterns, duplicate insurance claims or suspicious activities.

11.2. Establishment of specialised healthcare fraud units

Special investigation units should be created in order to focus only on healthcare fraud and these units should include experts who will have full knowledge and understanding in both, the healthcare systems as well as in digital technologies.

11.3. Legal and Regulatory reforms

Existing laws such as the Indian Penal Code and the Information Technology Act mentions legal responsibility for fraud and cybercrime, but there is a possibility of not fully addressing the problem of modern digital healthcare fraud.

11.4. Enhancing Transparency and Institutional Accountability

Hospitals and healthcare institutions should follow strict rules when they participate in government healthcare schemes. Regular audits, monitoring of claims, and strict penalties for fraudulent activities can improve transparency. Moreover, holding healthcare providers responsible will reduce unethical practices and help in maintaining the trust in the healthcare system.

11.5. Public Awareness and Patient Education

There are people at large number who are not aware of their rights under healthcare schemes and due to which, they can be easily misled or exploited by hospitals or intermediaries. Campaigns for raising awareness and educational programmes can help patients understand their rights or benefits and encourage them to report any suspicious activities.

Conclusion

The digitisation of healthcare services in India has improves easy access, transparency in healthcare delivery but these developments have also created new opportunities for white-collar crime within the healthcare sector. Fraudulent practices like insurance fraud, medical billing manipulation, identity misuse, pharmaceutical corruption and digital record tampering show how digital systems can be exploited for financial gain. These activities not only cause financial losses to healthcare institutions and insurance providers but public loses their trust in healthcare services. Even though provisions like the Indian Penal Code, the Information Technology Act, Prevention of Money Laundering Act provide mechanisms for addressing fraud, challenges in implementing the gaps still exist. Government initiatives such as Ayushman Bharat Pradhan Mantri Jan Arogya Yojna and the National Digital Health Mission have improved transparency and digital governance but there is still a need for strict monitoring technologies to prevent emerging forms of digital fraud.

Therefore, addressing healthcare-related white-collar crime requires a combined approach which involves strict legal provisions, advanced technological monitoring systems, specialised investigation units, and greater public awareness. Moreover, implementation should be strong and adopting modern fraud detection technologies will be essential to ensure responsibility and to protect the integrity of India's digitising healthcare system.

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344