January - June 2025 Volume 34 Issue 1

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW

Official Publication of Medicolegal Association of Maharashtra

MULTISPECIALITY, MULTIDISCIPLINARY, NATIONAL
PEER REVIEWED, OPEN ACCESS, MLAM (SOCIETY) JOURNAL
Indexed with Scopus (Elsevier)

Editorial Office Address
Department of Forensic Medicine & Toxicology, Third Floor, Library Building, Seth G S Medical College & KEM Hospital, Parel, Mumbai, Maharashtra, India. Pin-400 012. Email id: mlameditor@gmail.com Phone: 022-24107620 Mobile No. +91-9423016325.

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW
(Official Publication of Medicolegal Association of Maharashtra)
Email.id: mlameditor@gmail.com

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

Editorial

Cybercrime: Medicolegal Perspective

Ravindra B Deokar[a*], Sachin S Patil[b]

[a]Professor (Additional), Department of Forensic Medicine & Toxicology, Seth G S Medical college & KEM Hospital, Parel, Mumbai-400012. Orcid Id: 0000-0003-1539-1035.
[b]Professor (Additional), Department of Forensic Medicine & Toxicology, Lokmanya Tilak Municipal Medical college & LTMG Hospital, Sion, Mumbai-400022.

1. Introduction

Cybercrime refers to illegal activity carried with the use of computers or an internet, mainly targeting individuals, organisations, public or governments for financial gains, creating nuisance or causing harm to others with a wide range of malicious activities. Various main types of cybercrimes based on targets are against individuals (identity theft, cyberstalking, credit card fraud, etc.), against organisations (malware attacks, denial of service attacks, ransom ware) and against property (intellectual property theft, credit card theft). Cybercrime poses significant hurdles in terms of its detection, prevention and long term negative impact on the victim of such attacks.[1] There is big data at healthcare institution with personal sensitive information. The medicolegal perspective of cybercrime mainly includes legal and ethical challenges related to digitally committed crimes. There are main ethical concerns related to digital crimes involving hacking, unauthorised access and leakage of sensitive health data and consequent exploitation of the patients. The field is evolving and there is no appropriate defined processes to deal with the cases of digital abuse and hospital guidelines on reporting such incidences and how to secure the forensic evidence in such crimes.[2] In medicolegal context, cybercrime is the complex issue related to patient data privacy, telemedicine, accountability, hospital information management system (HIMS) and digital health records.[3]

The main key issues at healthcare institutions in cyber-attacks are defining legal liability, patient's data privacy and consent, establishing forensic evidence and the existing legal framework. Cybercrime at healthcare institutions may involves fraud, mischief, defamation and forgery of healthcare professionals and patients. Digital advancement leads to multiple challenges to law enforcement agencies, policymakers, and governments to deal with cybercrime cases.[4]

2. Various Medico-Legal Implications of Cybercrime at healthcare institutions

1. Patient Confidentiality: Patient's data should be protected from unauthorized access and data breach should be avoided by Healthcare providers.[5]
2. Informed Consent: There is need of valid informed consent of the patients after informing them about the risks and benefits of digital health services. They should be well aware of the implications of telemedicine and electronic health records.
3. Cyber Forensics unit at healthcare institution: There is need of specialised unit at healthcare institution under Forensic

How to cite this article: Deokar RB, Patil SS. Cybercrime: Medicolegal Perspective. J Forensic Med Sci Law. 2025;34(1):1-3. doi: 10.59988/jfmsl.vol.34issue1.1

***Corresponding author**: Dr Ravindra B Deokar, Professor (Additional), Department of Forensic Medicine, Seth G S Medical College & KEM Hospital, Mumbai, Maharashtra, India. Email: ravindradeokar@kem.edu (M)+91-9423016325.

***Article Info:* Received on:** 25.04.2025; **Accepted on:** 15.06.2025. doi: 10.59988/jfmsl.vol.34issue1.1

Medicine with trained cyber forensic experts who will collect and preserve the digital forensic evidence and facilitate appropriate investigation in cybercrimes at healthcare institution.

3. Various Cybercrime Challenges in Healthcare[4-6]

1. Data Breaches: The unauthorized access to digital records containing sensitive patient information at healthcare institution by various stakeholders lead to serious consequences such as identity theft and financial fraud.
2. Digital Health Records: To ensure the safety, security and integrity of electronic health records of patient is one of the crucial thing to uphold patient's trust and confidentiality.[7]
3. Telemedicine: Nowadays, there is rise of telemedicine. It is increasing the new risks of data interception and unauthorized access to patient's confidential information.

4. Legal Framework related to cybercrime

1. Information Technology Act, 2000: A legal framework for addressing cybercrimes in India is provided by this act. It covers hacking, data theft and unauthorized access to digital systems and computers.
2. The Digital Personal Data Protection Act 2023: It aims to safeguard individual privacy and permitting lawful data processing. It regulates the collection, storage and processing of personal data, including sensitive health information. In India, it is the prime comprehensive data protection law.
3. Bharatiya Nyaya Sanhita (BNS): The BNS complimentary to the IT Act, addressing various cybercrimes and providing penalties for offenses like Cyberstalking (BNS Section 78), Voyeurism (BNS section 77) and cyber frauds (BNS section 318 and 336).

5. Key issues of cybercrime at healthcare institution[7,8]

1. Patient's Data Privacy:
The protection of the sensitive patient's healthcare data is one of the most important role of healthcare provider. Healthcare institution must ensure legal compliance with data privacy laws. Organisation should protect the patient's valuable information from unauthorized access.
2. Informed Consent:
The patient should be informed about the risk associated with digital health services. There are chances of personal data compromise due to cyber threat challenges, patient's informed consent is important and patient's data should be protected from unauthorised access.
3. Data Tampering and Manipulation:
Health data can illegally modified by cybercriminals with use of artificial intelligence causing misdiagnoses and compromised treatments or other malicious outcomes that directly impact patient care.[9]
4. Erosion of Patient Trust:
In healthcare industry, Cyberattacks leading to loss of patient's confidence about the security of their personal confidential health information. This is causing a great fear and anxiety in patient leading to reluctance to share their crucial personal healthcare information.
5. Disruption of Medical Care:
As there is loss of patient's trust and data breach, there may be healthcare mis-management and wrong treatment. The emergency medical care may be directly hampered by sophisticated cyberattacks causing hindrance in the emergent healthcare delivery. This may affect patient's safety and security leading to endanger life.
6. Forensic Evidence collection experts/ Forensic nurse:
There is need of trained forensic nurse or staff having digital literacy to identify, collect, and preserve online forensic evidence in cybercrime. Such person should work with forensic cyber experts, meticulously document incidents. Such experts should able to provide trauma-informed care to victims.
7. Data Breaches:
Poor standardisation and unauthorized access to patient's sensitive information may lead to fraud, identity theft, and personal blackmail. Accidental or malicious insider threats to data privacy causing data security compromise, including selling patient data, leaking financial information, passwords or downloading malware have great impact on proper functioning of healthcare organisation.

8. Jurisdictional Issues:
   Cybercrimes are often transnational, creating complex jurisdictional challenges for investigations and prosecutions, requiring international cooperation.[10, 11]

6. Roles of Medical and Legal Professionals

1. **Healthcare Providers:**
   Healthcare professionals should aware of their duty to report cybersecurity incidents and facilitate investigations to prevent further harm ensuring accountability.
   Healthcare professionals should uphold ethical principles like patient autonomy and confidentiality. At cybersecurity threats, they have legal obligations to report the security-breach incident and cooperate with investigations.
2. **Lawmakers, policyholders and Government:**
   Lawmakers should evolve and update the laws addressing the emerging cybercrimes to ensure the admissibility of digital evidence. It need to strike a balance between individual privacy rights and law enforcement.

7. Conclusion and Recommendations:

Deceptive emails or messages forcing healthcare workers to reveal sensitive information or login credentials. In the era of advancement and artificial intelligence, such attacks are often enhanced and more effective to cause immediate damage to healthcare delivery system. There is need to implement best practices involving robust security measures including firewalls, encryption, controlled access to the digital record at healthcare institutions.

Healthcare professionals should be trained on data confidentiality importance, cybersecurity and maintenance of forensic evidence. There should be stringent monitoring and regular audits in healthcare to detect and prevent cybercrimes. There is a need of cross-disciplinary legal reforms with integrated legal models for dealing with cyber threats in the healthcare sector effectively.

To combat cybercrime effectively, there is need of comprehensive legislation to deal all aspects considering digital advancements. To enhance cybercrime investigation and prosecution, there is need to establish specialized cybercrime units and even the special forensic cyberunit may be established to deal with forensic evidence at the healthcare organisations. Educating people and creating public awareness about cyber risks and best practices is helpful for prevention.

Contribution ship of authors: All the authors have contributed equally.

References:

1. Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst. 2020; 44(5):98.
2. Wang L, Jones R. Big Data, Cybersecurity, and Challenges in Healthcare. 2019 Southeast Con; April 10-14; Huntsville, AL. 2019. pp. 1–6.
3. Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Inf Manag. 2015; 44(3):23–38.
4. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare Challenges in the Era of Cybersecurity. Health Secur. 2020; 18(3):228–31.
5. Perakslis ED. Cybersecurity in health care. N Engl J Med. 2014; 371(5):395–7.
6. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018; 20(5):e10059.
7. Langer G. Cybersecurity Issues in Healthcare Information Technology. J Digit Imaging.2017; 30(1):117–25.
8. Sendelj R, Ognjanovic I. Cybersecurity challenges in healthcare. Stud Health Technol Inform. 2022; 300 :190–202.
9. Deokar RB, Patil SS. Artificial Intelligence in Healthcare and Biomedical Research - Ethical aspects. J Forensic Med Sci Law. 2024; 33(1):1-4.
10. Gupta RR. Cyber security and cyber forensic. IP Int J Forensic Med Toxicol Sci. 2025; 9(4):122-3.
11. Prahladh S, Jacqueline VW, Naidoo D, Mistry T, Makgaba M, Olivier S, Baloyi V. Piloting and Evaluation by Forensic Pathology Registrars of a Mobile Application Created for Autopsy Reporting. J Forensic Med Sci Law. 2024; 33(2):27-36.